PAKISTAN

BANKING INFORMATION TECHNOLOGY
MODERNIZATION REVERSE TRADE MISSION

FEBRUARY 4 - 13 • 2013

WASHINGTON DC • NEW YORK • CALIFORNIA

TABLE OF CONTENTS

Itinerary

About USTDA

Delegation

Company Profiles

Banking Technology Policies and Practices

Reverse Trade Mission (RTM) Survey

Entertainment

CONTACT INFORMATION

The Business Council for International Understanding (BCIU)
1212 Avenue of the Americas, 10th Floor
New York, NY 10036
Tel: 212-490-0460
Fax: 212-697-8526

Ms. Tosha Wilkes
Senior Vice President
Email: t-wilkes@bciu.org

Ms. Nina Kundra
Director
Cell: 917-442-9682
Email: n-kundra@bciu.org

The U.S. Trade and Development Agency (USTDA)
1000 Wilson Blvd, Suite 1600
Arlington, VA 22209-3901
Tel: 703-875-4357
Fax: 703- 875-4009

Mr. Henry Steingass
Regional Director, South and Southeast Asia
Tel: 703-875-4357
Email: hsteingass@ustda.gov

Mr. Jacob Flewelling
Country Manager, Pakistan
Tel: 703-875-4357
Email: jflewelling@ustda.gov

PAKISTAN

BANKING INFORMATION TECHNOLOGY MODERNIZATION REVERSE TRADE MISSION

FEBRUARY 4 - 13 • 2013

WASHINGTON DC • NEW YORK • CALIFORNIA

ITINERARY AS OF FEBRUARY 1, 2013

February 2013						
Sunday	**Monday**	**Tuesday**	**Wednesday**	**Thursday**	**Friday**	**Saturday**
						2
						Arrive in Washington, D.C
3	**4**	**5**	**6**	**7**	**8**	**9**
Washington, D.C.	Washington, D.C.	Washington, D.C. Business Briefing	Washington, D.C. *Depart from Washington D.C. to New York*	New York City	New York City	New York City
10	**11**	**12**	**13**	**14**		
New York City	New York City *Depart from New York to San Francisco*	Silicon Valley, CA	Silicon Valley, CA	*Depart from San Francisco to Pakistan*		

Saturday, February 2, 2013	
Washington, D.C.	
10.30pm	Delegates arrive in Washington, D.C. (DCA) from Pakistan on American Airlines 2026 via Chicago/Abu Dhabi. Delegates are greeted by BCIU at airport.
11.30pm	Depart for Renaissance Mayflower Hotel, 1127 Connecticut Avenue Northwest, Washington, D.C. in Washington, D.C.
11.50pm	Delegates arrive in Washington, D.C. (DCA) from Pakistan on American Airlines 532 via Chicago/London. Delegates are greeted by BCIU at airport.
Sunday, February 3, 2013	
12.50am	Depart for Renaissance Mayflower Hotel, 1127 Connecticut Avenue Northwest, Washington, D.C. in Washington, D.C.
12.00pm	**BCIU Orientation Meeting and Luncheon,** Mayflower Hotel, Pennsylvania Room, Second Floor, 1127 Connecticut Avenue Northwest, Washington, D.C. in Washington, D.C.
Monday, February 4, 2013	
9.00am	**U.S. Department of the Treasury, Office of Technical Assistance** Meeting, 740 15th St NW. 4th Floor, Northwest, Washington, D.C.
11.00am	**IBM** Meeting and Lunch, 1301 K Street, Northwest, Washington, D.C.
2.00pm	**NACHA, the Electronic Payments Association** Meeting, Mayflower Hotel, Pennsylvania Room, Second Floor, 1127 Connecticut Avenue Northwest, Washington, D.C

PAKISTAN

BANKING INFORMATION TECHNOLOGY MODERNIZATION REVERSE TRADE MISSION

FEBRUARY 4 - 13 • 2013

WASHINGTON DC • NEW YORK • CALIFORNIA

Tuesday, February 5, 2013	
9.00am	**Experian** Meeting, Offices of DLA Piper, 500 Eighth Street, N.W., Washington, D.C.
11.30am	**MicroTech International, Inc.** Meeting and Lunch, 8330 Boone Boulevard Suite 600, Vienna, Virginia
2.00pm	**Unisys Corporation** Meeting, 11720 Plaza America Drive, Reston, Virginia
Wednesday, February 6, 2013	
9.00am	**Meet and Greet with The Honorable Leocadia Zak, Director, U.S. Trade and Development Agency**, 1000 Wilson Boulevard, Suite 1600, Arlington, Virginia
9.30am	**Banking ICT Finance and Policy Roundtable,** Offices of the U.S. Trade and Development Agency, 1000 Wilson Boulevard, Arlington, Virginia
	Mr. Henry Steingass, Regional Director, South and Southeast Asia, U.S. Trade and Development Agency
	Mr. Brian Sant Angelo, Senior Business Development Officer, Global Business Development, Export-Import Bank of the United States
	Mr. John Carlson, Executive Vice President, Banking Industry Technology Secretariat (BITS)
10.30am	**Mandiant Corporation** Meeting and Lunch, Offices of Offices of the U.S. Trade and Development Agency, 1000 Wilson Boulevard, Arlington, Virginia
1.00pm	**Federal Deposit Insurance Corporation (FDIC)** Meeting, 550 17th Street NW, Washington, DC
6.00pm	Delegation departs from Washington, D.C. (DCA) on Delta Airlines 5924 to New York, New York (LGA).
New York, NY	
6.50pm	Delegation arrives in New York, NY. Depart for W Union Square New York, 201 Park Avenue South, New York, New York.
Thursday, February 7, 2013	
10.00am	**SQN Banking Systems** Meeting, W Union Square, 201 Park Avenue South, New York, New York
1.00pm	**Oracle Corporation** Meeting and Lunch, 120 Park Avenue, New York, New York
6.00pm	Dinner with Oracle Corporation
Friday, February 8, 2013	
8.30am	**New York Stock Exchange (NYSE)**, 11 Wall Street, New York, New York
8.30am	Delegation arrives at the New York Stock Exchange (NYSE) and proceeds through security to conference room.
9.00am	Tour of the NYSE
9.30am	Observation of the Opening Bell Ceremony
9.45am	NYSE Technologies Meeting and Presentation

11.30am	**CA Technologies** Meeting and Lunch, 520 Madison Avenue (entrance on 53rd Street between Madison and 5th Avenue), New York, New York
3.30pm	**Society for Worldwide Interbank Financial Telecommunication (SWIFT)**Meeting, 7 Times Square, New York, New York
Saturday, February 9, 2013	
	Free time for site seeing & shopping in New York. Entertainment options provided in the delegate handbooks.
Sunday, February 10, 2013	
	Free time for site seeing & shopping in New York. Entertainment options provided in the delegate handbooks.
Monday, February 11, 2013	
9.00am	***Bloomberg Government,*** *731 Lexington Avenue, New York, New York, or* ***BNY Mellon,*** *101 Barclay Street, New York, New York*
11.00am	**MorphoTrust USA, Inc./ L-1 Identity Solutions Inc.,** Meeting and Lunch Ten Exchange Place, 18th Floor, Jersey City, New Jersey
5.00pm	Delegation departs from New York (JFK) on Delta 31 to San Francisco, California (SFO).
San Francisco, CA	
8.49pm	Delegation arrives in San Francisco, California. Depart for Sheraton Fisherman's Wharf, 2500 Mason Street, San Francisco, California.
Tuesday, February 12, 2013	
8.00am	**Visa/Paul Hastings LLP.,** Meeting and Breakfast, 55 Second Street, Twenty-Fourth Floor, San Francisco, California
10.30am	**Symantec Corporation** Meeting and Lunch, 350 Ellis Street, Mountain View, California
1.30pm	**Juniper Networks** Meeting, 1133 Innovation Way, Building A, Sunnyvale, California
Wednesday, February 13, 2013	
10.00am	**Informatica Corporation** Meeting and Lunch, 100 Cardinal Way, Redwood City, California
1.30pm	**EMC Corporation** Meeting, 2831 Mission College Boulevard, Santa Clara, California
Thursday, February 14, 2013	
10.45am	Delegates from Pakistan depart from San Francisco (SFO) on American Airlines Flight 892 via Chicago and Abu Dhabi.

Meetings in italics are pending company/executive schedule availability.

U. S. TRADE AND DEVELOPMENT AGENCY

USTDA in Pakistan

Since 1982, USTDA has sponsored and provided funding for 62 different project development and international business partnership activities in Pakistan. As a result of these efforts, over $264.5 million in U.S. exports have been generated in the energy, transportation, services, water, and human resources sectors. USTDA will continue to see significant growth of its program as it has begun implementing an expanded infrastructure initiative to support the Administration's priorities for results-oriented economic cooperation. This program emphasizes needs for infrastructure improvement in the energy, transportation, and food security sectors, and links Pakistani development interests with U.S. exports and companies offering project solutions. USTDA continues to work with USG agency partners, U.S. companies, and the government and private sectors of Pakistan in order to identify projects for funding consideration.

USTDA Activities by Sector

Energy

USTDA is providing grant funding in the amount of $462,520 for a feasibility study and pilot project for Warid Telecom, one of the major cellular service providers in Pakistan, to determine the viability of replacing diesel generators and lead acid batteries with methanol-based fuel cells and sodium batteries to power cell tower sites. This conversion will reduce the energy consumption of Warid Telecom and improve the reliability of mobile services for Warid's more than 18 million subscribers in Pakistan.

USTDA is providing a feasibility study grant in the amount of $769,000 to Pioneer Cement Limited (PCL), a large Pakistani cement manufacturer, to evaluate the viability of incorporating a 35-50 MW biomass-fired power plant, a waste heat recovery system, and energy efficiency upgrades at PCL's cement plant in Punjab province.

USTDA is providing a technical assistance grant in the amount of $924,290 to the Islamabad Electric Supply Company (IESCO) for a grid modernization assessment and pilot project in greater Islamabad to serve as the basis for the deployment of smart grid technologies. The TA includes a gap analysis of the present system infrastructure versus a suite of potential smart grid investments, and identifies an appropriate combination of technologies to upgrade the capabilities of IESCO's distribution system.

USTDA provided a grant in the amount of $510,475 to Karachi Electric Supply Company Limited for a feasibility study to determine the viability of an integrated Smart Grid system in Karachi to reduce electricity losses and improve the efficiency of utility operations.

USTDA provided grant funding in the amount of $289,125 to Packages Ltd. for a feasibility study to determine the best option to convert paper and agricultural wastes to energy at Packages' Bulleh Shah paper mill in Kasur, Punjab province, Pakistan. This paper mill would serve as an example of energy

self-generation in local communities at time when Pakistan is facing considerably large energy shortfalls nationwide.

USTDA provided grant funding in the amount of $299,896 to Educational Services (Private) Limited for a feasibility study to determine the technical, economic, and financial feasibility of installing solar photovoltaic (PV) power systems at hundreds of private schools in the Beaconhouse school system. In September 2011, a pilot project was installed at a school in Lahore, Pakistan. Data collection since the project's launch has demonstrated positive results regarding the energy production capacity of these solar PV systems.

Transportation

USTDA is funding a technical assistance activity in the amount of $628,000 with Premier Mercantile Services (Pvt.) Ltd., a private sector port and freight logistics operator, with an assessment of the infrastructure, operational, and business requirements of acquiring and operating a fleet of locomotives and wagons on the existing Karachi-Lahore Railway.

USTDA provided a grant in the amount of $933,273 to Mega & Forbes Group for a feasibility study and pilot project that assesses the viability and application of a Trade Information Gateway Real-Time Exchange (TIGRE) software solution for cargo movement operations in and around the main ports in Karachi, Pakistan.

USTDA funded a feasibility study in the amount of $864,002 to Pakistan International Airlines that will consider expanding a Maintenance, Repair, and Overhaul (MRO) Facility for PIA. The Study will develop a market assessment and business plan for PIA's expanded MRO facility, as well as the necessary technical requirements and cost estimates.

Information Technology

USTDA is funding a reverse trade mission (RTM) to assist officials from Pakistan's public and private sector commercial banks in upgrading their banking information technology systems, particularly relating to mobile and internet banking, anti-money laundering solutions, fraud analytics and customer relationship management solutions. The RTM will assist Pakistan's efforts to modernize its banking sector and broaden Pakistanis' access to financial services. USTDA envisions that the RTM, which will include time in Washington, D.C., New York City, and Silicon Valley, CA, will take place in February 2013.

Food Security/Cold Chain

USTDA provided grant funding in the amount of $392,328 to support a feasibility assessment for establishing a network of private sector cold storage facilities at within five geographical areas throughout Pakistan (Lahore, Karachi, Islamabad, Quetta, and Peshawar). The study will identify strategic locations for effective investment in the cold chain for a proposed twelve cold storage facilities, reducing perishable product loss. The $14-16 million prospective project would improve the post-harvest system by adding value and security to Pakistan's food systems and ultimately promoting greater private sector involvement in the country's most important sector.

U.S. Trade and Development Agency

Information and Communication Technology

The U.S. Trade and Development Agency (USTDA) helps companies create U.S. jobs through the export of U.S. goods and services for priority development projects in emerging economies. USTDA links U.S. businesses to export opportunities by funding project planning activities, pilot projects, and reverse trade missions while creating sustainable infrastructure and economic growth in partner countries.

USTDA Programs

USTDA promotes economic growth in emerging economies by facilitating the participation of U.S. businesses in the planning and execution of priority development projects in host countries. The Agency's objectives are to help build the infrastructure for trade, match U.S. technological expertise with overseas development needs, and help create lasting business partnerships between the United States and emerging market economies.

USTDA advances these objectives through its two key programs, the *International Business Partnership Program* and the *Project Development Program*.

USTDA's reverse trade missions (RTM) are the mainstay of its *International Business Partnership Program (IBPP)*. Created in 2010 in response to President Obama's National Export Initiative, the *IBPP* is USTDA's signature program for linking the U.S. private sector to foreign buyers. These visits are carefully planned to enable foreign decision-makers to meet with U.S. businesses and to observe the manufacture and demonstration of U.S. goods and services that can help them achieve their development goals. These RTMs also include meetings with financial institutions to observe financing options and technical and regulatory bodies that can assist with strengthening the project sponsor's technical capacity.

Through feasibility studies, technical assistance and pilot projects, USTDA's *Project Development Program* helps overseas project sponsors identify technological solutions and various sources of financing for priority infrastructure projects.

Through these programs, USTDA funds an array of activities that promote the procurement of U.S. information and communication technologies (ICT) and the development of ICT infrastructure projects in partner countries.

Success Story

Bringing broadband communications to Africa through the sale of more than $400 million in U.S. exports demonstrates USTDA's success in utilizing U.S. technologies and services to expand ICT infrastructure overseas. The Agency's investment in a regional ICT conference in Ghana and a reverse trade mission to the United States proved successful when a group of African ministers, traveling on the USTDA-funded RTM, convinced potential financiers that undersea fiber-optic cable connecting East Africa to the rest of the world could be commercially attractive. As a result, the SEACOM fiber optic cable network has revolutionized communications in Africa.

The Tyco Resolute laying cable along the eastern coast of Africa

Recent Activities

Egypt Forward: Partnering for Trade and Economic Growth

To demonstrate that Egypt is "open for business" as it transitions to a new governing structure, USTDA hosted Egypt: Forward, a two-day forum in Washington, DC followed by four sector-specific RTMs across the country. Over 50 Egyptian public and private sector delegates connected with hundreds of U.S. government and industry representatives. The Egyptian ICT officials, consisting of entrepreneurs as well as established businesspeople, discussed their country's needs given the transformative changes and learned about U.S. technological advances in e-government, cloud computing, data centers, and other solutions.

Kazakhstan Digital Broadcasting

U.S. businesses were given the opportunity to present digital TV solutions to a delegation from Kazakhstan during this reverse trade mission. The delegates visited U.S. facilities and met with leading U.S. companies and U.S. government agencies active in digital television broadcasting, including Harris Corporation, Broadcast Electronics, and Axcera. These visits included trips to Washington DC, Melbourne, FL, Quincy, IL, and Pittsburgh, PA.

Kenya Cybersecurity

USTDA hosted a delegation of senior Kenyan ICT decision makers in Washington, DC, and Silicon Valley, CA, to explore best practices and innovative cybersecurity technologies to protect Kenya's growing ICT infrastructure.

Vietnam Financial Information Management Modernization

Introducing a delegation from the State Bank of Vietnam to U.S. central bank operations best practices and the ICT systems used in the management and supervision of the sector was the goal of this USTDA-sponsored mission, which visited Washington D.C., New York, NY and Silicon Valley, CA. The RTM directly supported the Vietnamese government in developing a centralized and integrated ICT platform to include a data warehouse and core banking system, while simultaneously opening up business opportunities for U.S. ICT providers.

India Integrated Emergency Communications System Feasibility Study

This project partially funds a feasibility study for the Indian Ministry of Home Affairs (MHA) to establish an Integrated Emergency Communications System (IECS) and supporting infrastructure in Hyderabad. The MHA requested funding for a study to assess the current IECS communications architecture; analyze the operational, financial, and organizational aspects that would lead to a national IECS; and address the implications of project implementation focused on a pilot project in Hyderabad.

Brazil Data Center Feasibility Study

In order to facilitate communication between the agencies within the state of Rio de Janeiro, as well as improve their services, USTDA awarded a grant to the Rio de Janeiro IT Company (PRODERJ) for a feasibility study to develop an implementation plan for a new data center. The study will review the state's overall IT strategy, providing recommendations and standards to ensure that all future systems coordinate with the new data center.

Contact us for more information!
(703) 875-4357
www.ustda.gov

Paul Marin, Regional Director for Sub-Saharan Africa
Diana Rossiter, Director of Program Evaluation (Acting)
Michael DeRenzo, Country Manager for Southern Africa
Joshua Kaplan, Country Manager for the Middle East

USTDA: ICT by the Numbers

1/5

In fiscal year 2011 one-fifth of USTDA's activities focused on ICT sector development.

16

USTDA funded 16 new ICT-oriented activities in fiscal year 2011 that directly support the National Export Initiative.

50%

Half of all USTDA activities in sectors such as clean energy and transportation have significant ICT sub-components.

NEI NATIONAL EXPORT INITIATIVE

USTDA supports the NEI's mission as a member of the President's Export Promotion Cabinet

PROMOTING FINANCIAL SECTOR DEVELOPMENT

The U.S. Trade and Development Agency (USTDA) supports a wide range of banking and financial sector activities in low and middle-income countries that support the development of a modern infrastructure. USTDA has provided training and technical assistance on the development of primary and secondary mortgage markets, core banking and cash management systems, regulatory processes governing bank lending, bond issuances, and credit rating capability. The agency's grant-based assistance has been provided to ministries of finance, state and private banks, development and regulatory organizations, and municipalities. The following is an illustrative list of recent banking and financial sector projects that USTDA has supported:

Afghanistan: Telecommunication Development Fund – USTDA awarded a $404,500 grant to the Afghanistan Telecommunications Regulatory Authority for technical assistance on the utilization of the newly created Telecommunications Development Fund. The Fund was created to improve rural access and ensure that local and rural initiatives can properly integrate and inter-operate with systems at the district and national levels. The technical assistance will also examine mechanisms to incentivize existing operators and new entrants to participate in rural development opportunities. ASTRO Systems, Inc. of Bethesda, MD, is providing the assistance.

Azerbaijan: Capacity Building for State Oil Fund Phase II – USTDA is providing $855,075 to the State Oil Fund of Azerbaijan (SOFAZ) to review and refine asset management guidelines and polices and enhance asset and risk management capabilities. The assistance will strengthen financial management and promote better governance and transparency. Overture Financial Services of New York, NY, is providing the assistance.

Cameroon: Leasing Regulatory Framework - A $200,000 grant is funding technical assistance to the Government of Cameroon in drafting legislation for leasing operations, including the regulation of leasing companies. The grant will also assist in the implementation of new legislation. The International Finance Corporation (IFC) will manage the assistance.

China: Banking Sector Prudent Lending Practices – USTDA approved $325,282 for technical assistance to support a Banking Sector Prudent Lending Practices program for members of the Chinese banking community. The program introduced modern risk management practices with the goal of reducing China's portfolio of non-performing loans. The American Bankers Association was the contractor.

China: Shanghai Infrastructure Finance Advisory Services - USTDA provided a $498,500 technical assistance grant to evaluate options for the Shanghai Water Services Assets Operation and Development Company, Limited (SWAOD) to utilize corporate bonds to raise revenue for environmental projects. This assistance led to the issuance of a US$190 million bond to obtain long-term capital financing.

India: Tamil Nadu Sub-Sovereign Finance for Water and Sanitation Infrastructure – This $300,000 technical assistance grant to the Tamil Nadu Urban Infrastructure Financial Services, Ltd. developed the capacity of the Tamil Nadu Urban Development Fund (TNUDF) to issue and service bonds. This assistance was designed to give TNUDF the capacity to implement a revolving loan fund similar to that used in the United States to provide financing for water and sanitation infrastructure projects.

Indonesia: Integrated Financial Management Information System – USTDA funded an orientation visit to the United States for Indonesian officials responsible for implementing the $32 million World Bank-funded Integrated Financial Management Information System Project. The itinerary included site visits to municipal, state and Federal entities that utilize U.S. technologies for accounting and financial management activities.

Mexico: Financial Literacy Education Program – USTDA provided a $697,550 technical assistance grant to Banco del Ahorro Nacional y Servicios Financieros (BANSEFI) to develop a financial education training program for low-income Mexicans on the financial products and services that are available from Mexican financial institutions. The program will reach the "unbanked" Mexican population that does not currently use the formal banking sector. This project will help maximize the development impact of remittances, increase domestic savings, improve access to financial products, and strengthen Mexico's financial system.

Mexico: Financial Officer Training Program – USTDA provided a $847,109 technical assistance grant to provide an agricultural and rural bank officer training program for Financiera Rural (FR), a major financial lender to Mexico's agricultural and rural communities. This project aims to strengthen FR's capacity to assess creditworthiness and market risk. Implementation of this technical assistance furthers the goals of advancing the Mexican financial sector.

Mexico: Housing Finance Reform – USTDA provided a $250,000 technical assistance grant to help the Northwestern Mexican states of Sonora and Baja California Norte address the legal, institutional, and transactional reforms needed to facilitate a transparent housing securitization process, leading to the construction of low and middle-income housing.

Montenegro: Water Sector Revolving Investment Fund — USTDA provided $463,950 to the Montenegrin Ministry of Environmental Protection and Physical Planning for technical assistance (TA) to establish a revolving investment fund for the water sector. The TA analyzed the technical and economic feasibility of establishing such a fund for the Montenegrin water utilities to obtain necessary funds for operational maintenance and improvements. The International Association of Development Funds of Bethesda, MD, provided the assistance.

Nigeria: Stock Exchange Disaster Recovery Plan and Systems Backup – USTDA provided a $236,410 technical assistance grant to the Nigerian Stock Exchange for the development of an emergency response system that would involve the procurement of back-up software and hardware, and include plans for the establishment of a secure, secondary location in case of an emergency.

Nigeria: Polmaz Financial Structuring Technical Assistance – USTDA is funding a $470,000 grant to the Nigerian oil services firm Polmaz. This project will help Polmaz to prepare an Exim Bank guaranteed loan to support the purchase of three tug boats from the United States. This project will also create an innovative trade finance product that would allow a bank guarantee to be secured by a contract that a borrower has with a major oil company. Clifford Chance LLP was competitively selected to perform this technical assistance.

Philippines: DBM Financial Management System – USTDA is funding a $274,000 grant for technical assistance to help the Department of Budget and Management in the preparation of tender documents for the modernization and enhancement of its financial management system. Contractor selection is currently underway.

Regional South and Southeast Asia: SME Financing and Capacity Building Workshop – USTDA funded a regional two-day workshop on Small and Medium Enterprise (SME) Financing and Capacity Building in Bangkok, Thailand. The workshop featured disaster recovery programs and best practices for delivering assistance to Asian SMEs.

Regional Latin America and the Caribbean: IDB Equity Broker for Energy Projects – USTDA provided a $140,000 technical assistance grant to help the Inter-American Development Bank (IDB) more efficiently bridge the "equity gap" of financing energy sector projects in Central America. The technical assistance will provide for the services of a Broker who will perform an intermediary role between project developers and equity investors in order to expand the inventory of projects IDB can consider for financing.

Thailand: IT Systems Integration for BAAC – USTDA provided $186,326 to fund technical assistance on an IT Integration Project for the Bank of Agriculture and Agricultural Cooperatives (BAAC) in Thailand. This project investigated the technical and financial options for acquiring a Human Resource Management and Core Banking System. It also helped BAAC to improve its IT systems and provide more efficient and cost-effective services to its agricultural client base.

Vietnam: State Capital Investment Corporation IT System Project – This $453,400 feasibility study grant funded the development of detailed technical design and bidding documents for the IT infrastructure at the State Capital Investment Corporation in Vietnam. This project will allow the SCIC to carry out its mandate to improve the oversight, efficiency and reform of state-owned enterprises.

Vietnam: Hanoi Securities Trading Center Expansion Project – USTDA provided a $422,000 feasibility study grant for the development of a roadmap and detailed technical design for expanding the IT infrastructure at the Hanoi Securities Trading Center, which is managed by the State Securities Commission in Vietnam. This expansion would allow the HSTC to operate at a greater capacity and efficiency. An ADB/AFD loan will be used to finance this project for implementation.

For more information on USTDA's program in the Finance sector, please contact Geoff Jackson (East Asia), David Hester (Europe and Eurasia), Nathan Younge (Latin America and the Caribbean), Carl B. Kress (Middle East and North Africa), Henry Steingass (South and Southeast Asia), and Paul Marin (Sub-Saharan Africa) by telephone at (703) 875-4357.

Our Mission

The U.S. Trade and Development Agency (USTDA) helps companies create U.S. jobs through the export of U.S. goods and services for priority development projects in emerging economies.

Who We Are

USTDA is an independent federal agency that was created to promote U.S. private sector participation in international development projects.

What We Do

USTDA links U.S. businesses to export opportunities by funding project planning activities, pilot projects, and reverse trade missions while creating sustainable infrastructure and economic growth in partner countries.

The International Business Partnership Program

In support of the **National Export Initiative,** USTDA launched the **International Business Partnership Program** to connect international buyers with U.S. manufacturers and service providers in order to open new export markets and commercial opportunities around the world for American companies. Key activities include:

Reverse Trade Missions:
CONNECTING U.S. FIRMS WITH FOREIGN BUYERS

USTDA hosts **reverse trade missions** to bring foreign buyers to the United States, pending upcoming procurements, in order to observe the design, manufacture, and operation of U.S. products and services that can help them achieve their development goals. These strategically planned missions also present excellent opportunities for U.S. businesses to establish or enhance relationships with prospective overseas customers.

During FY 2010, USTDA-funded reverse trade missions and conferences connected more than 3,000 foreign buyers from 35+ countries with over 1,000 U.S. company representatives.

Conferences and Workshops:
MAKING CONNECTIONS

USTDA organizes **conferences and workshops worldwide** to connect U.S. firms with foreign project sponsors. These sector or region-specific events are designed to showcase U.S. goods, services and technology to foreign buyers. U.S. firms also have the opportunity to meet one-on-one with overseas project sponsors and other potential customers.

Training:
LEVELING THE PLAYING FIELD FOR U.S. FIRMS

In support of U.S. businesses, USTDA provides **training for foreign decision makers** to support the sale of U.S. equipment and services overseas. Training can take place in either the United States or a host country and typically focuses on technology or regulatory requirements in order to give project sponsors a better understanding of U.S. capabilities and expertise related to a procurement.

Supporting Small U.S. Businesses:
THE ENGINE OF OUR ECONOMY

USTDA draws extensively on the expertise of small consulting and engineering firms to provide a variety of services related to project definition and evaluation.

Many small businesses have expanded their markets through the international contacts made while working with USTDA. To further enhance its outreach to the small business community, USTDA partnered with the Small Business Administration (SBA). This increased engagement is raising the profile of small businesses with international buyers who may not have been familiar with the unique technologies and services small U.S. companies can provide.

More than 90% of contracts awarded by USTDA are performed by small businesses. Furthermore, over 40% of grants awarded to overseas project sponsors directly lead to contracts with U.S. small businesses.

Project Development Program

USTDA provides grants directly to overseas sponsors who, in turn, select U.S. companies to perform Agency-funded project development activities. An overseas sponsor is a local entity, public or private, with the decision-making authority and ability to implement a project. The Agency targets priority development projects that are most likely to utilize U.S. exports. While USTDA projects span a variety of sectors, many focus on clean energy and energy efficiency, transportation, information and communication technology, and the environment. Key activities include:

Feasibility Studies and Pilot Projects:
GETTING IT RIGHT FROM THE START

USTDA-funded and U.S.-led **feasibility studies** link foreign project sponsors with U.S. businesses at the critical early stage of project development when technology

(CONTINUED)

options and requirements are being defined. These studies evaluate the technical, financial, environmental, legal, and other critical aspects of infrastructure development projects.

In some cases, export opportunities depend on a demonstration of the U.S. seller's goods, services or technologies in the foreign buyer's setting. USTDA-funded **pilot projects** demonstrate the effectiveness of commercially proven U.S. solutions in location.

USTDA evaluates project proposals based upon the following criteria.

- *Significant export opportunities for U.S. manufactured products and services*
- *Developmental priority in the host country*
- *Strong likelihood of success securing implementation financing*

Technical Assistance:
PROVIDING NEEDED KNOW-HOW

USTDA advances economic development in partner countries by funding **technical assistance** that supports legal and regulatory reform related to commercial activities and infrastructure development, the establishment of industry standards, and other market-opening activities. These technical assistance programs facilitate favorable business and trade environments for U.S. goods and services.

Tell Me More About...

- **CONTRACT OPPORTUNITIES WITH USTDA:** Review procurement opportunities to work directly with the Agency at: ***www.ustda.gov/businessopps/ustdaopps.asp***
- **WORKING WITH GRANT RECIPIENTS:** Opportunities to work with overseas project sponsors on USTDA-funded activities are listed at: ***www.ustda.gov/businessopps/index.asp*** or the Federal Business Opportunities website at: ***www.fbo.gov***
- **OPPORTUNITIES FOR SMALL BUSINESSES:** Register on-line with the Agency's consultant database to be considered for small business designated solicitations: ***www.ustda.gov/consultantdb*** Small businesses should also sign up with the U.S. Government's Central Contractor Registration website at: ***www.ccr.gov***
- **USTDA'S EVENTS:** Check out our calendar to find an event in your sector or region of interest: ***www.ustda.gov/news/index.asp***

USTDA NEWS & INFORMATION: Sign up to receive USTDA's bi-weekly e-newsletter, which is the best source for information on upcoming procurements and events: *www.ustda.gov/pubs/news_information.asp*

- **CONTACTING USTDA'S PROGRAM STAFF:** If you already know where you would like to do business, contact USTDA's regional teams:
  - East Asia and Eurasia: ***East_Asia_Eurasia@ustda.gov***
  - Latin America and the Caribbean: ***LAC@ustda.gov***
  - Middle East, North Africa and Europe: ***MENA_Europe@ustda.gov***
  - South and Southeast Asia: ***South_Southeast_Asia@ustda.gov***
  - Sub-Saharan Africa: ***Africa@ustda.gov***

AN INTRODUCTION TO THE

U.S. TRADE AND DEVELOPMENT AGENCY

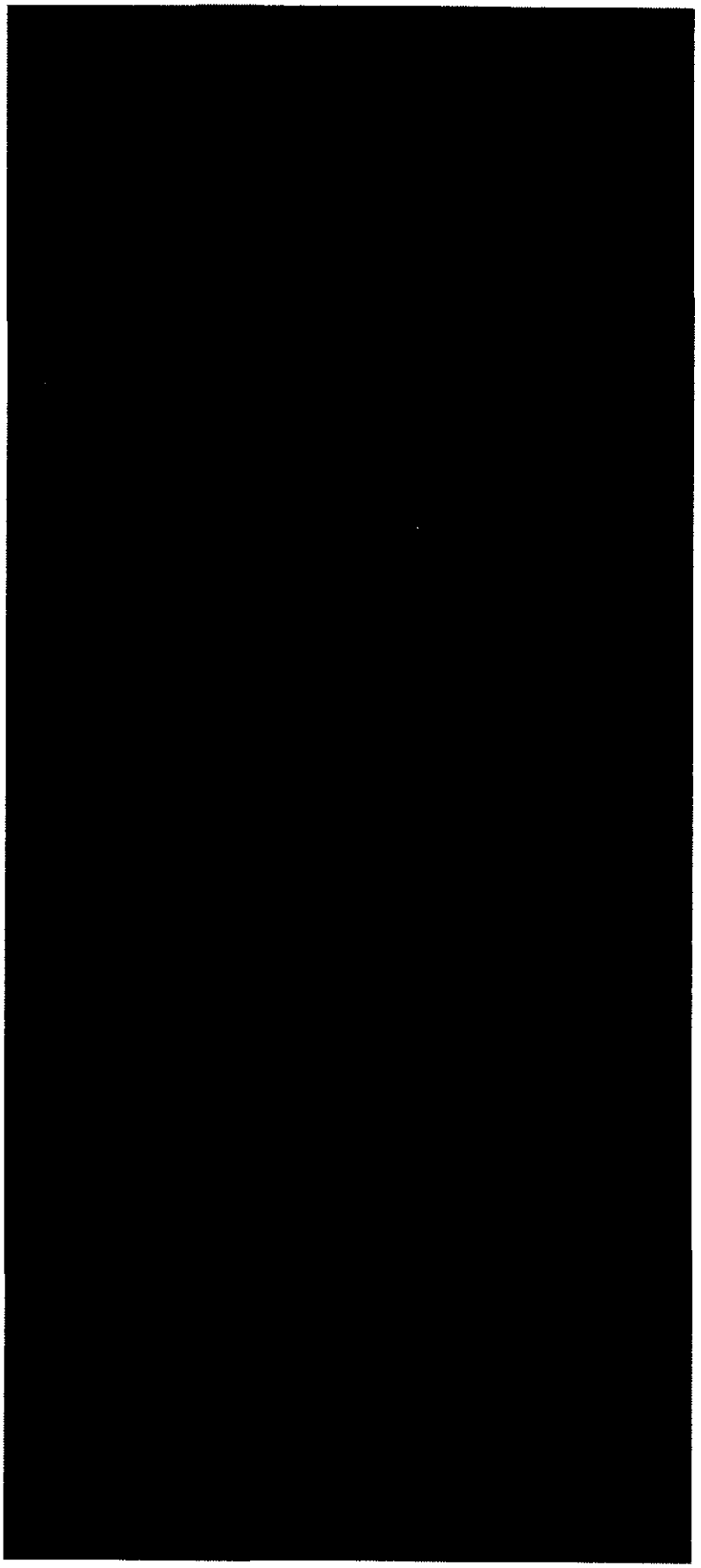
U.S. Trade and Development Agency
1000 Wilson Boulevard, Suite 1600
Arlington, Virginia 22209
Phone: 703.875.4357 • Fax: 703.875.4009
E-mail: info@ustda.gov
Website: www.ustda.gov

U.S. TRADE AND DEVELOPMENT AGENCY

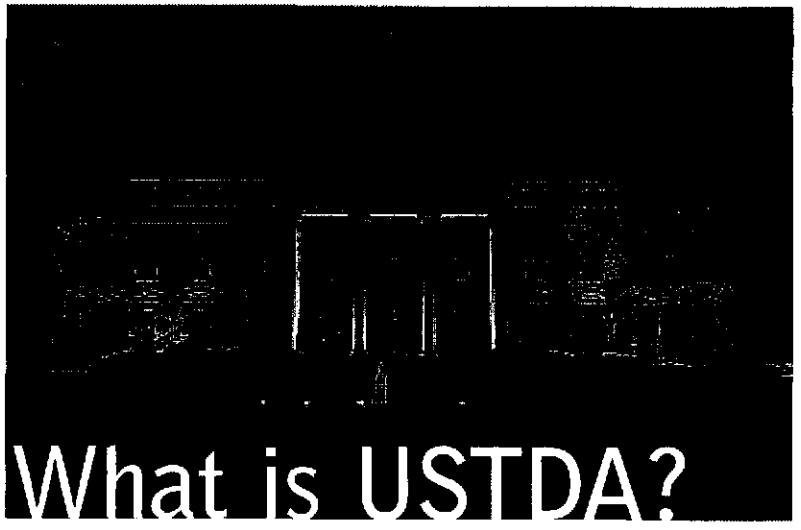
Project Sponsor Information

U.S. Trade and Development Agency
1000 Wilson Boulevard, Suite 1600
Arlington, Virginia 22209
Phone: 703.875.4357 • Fax: 703.875.4009
Website: www.ustda.gov

8/09



Recognizing that trade and private sector growth are catalysts for development, the U.S. Trade and Development Agency (USTDA) helps project sponsors in developing and middle-income countries to establish the infrastructure and environment necessary for economic growth to occur. By providing access to U.S. expertise in the planning and development of priority projects and capacity-building activities, USTDA facilitates partnerships between project sponsors and U.S. firms that contribute to the achievement of important development goals.



What is USTDA?

USTDA is an independent U.S. Government foreign assistance agency that is funded by the U.S. Congress.

What are USTDA's objectives?

Our aim is to advance economic development in developing and middle-income countries by providing foreign project sponsors with access to U.S. technology and expertise.

What types of projects does USTDA support?

USTDA provides grant funding for the planning of projects that support the development of modern infrastructure and an open trading system.

While USTDA activities span a wide variety of sectors, many focus on clean energy and power, transportation, information and communications technology, environmental infrastructure and services, and healthcare.

On what eligibility factors are USTDA grants based?

USTDA evaluates projects primarily based on:

- Their priority to the project sponsors and the countries where they are located and their likelihood of receiving implementation financing or, in the case of USTDA's trade capacity building work, advancing trade liberalization efforts; and
- Whether they offer mutual economic benefit for the host country and the United States, including opportunities for commercial cooperation with U.S. firms, thereby supporting U.S. jobs.

With whom does USTDA work?

USTDA provides grants directly to foreign project sponsors.

A foreign project sponsor is the local entity with the decision-making authority and ability to implement a project. The sponsor may be a government institution at the national, state/provincial, or local level, or it may be a local private sector company.

USTDA is open for business in more than 100 nations around the world.

What types of activities does USTDA support?

USTDA accomplishes its mission by funding: 1) trade capacity building and sector development; and 2) project definition and investment analysis.

Trade capacity building and sector development assistance supports the establishment of industry standards, rules and regulations, market liberalization and other policy reform. Project definition and investment analysis involves activities that support large capital investments related to overseas development.

Trade Capacity Building and Sector Development

SECTOR DEVELOPMENT TECHNICAL ASSISTANCE

USTDA provides technical assistance to help with the development of sector strategies, industry standards, and legal and regulatory regimes. This assistance helps to create a favorable business and trade environment. Transportation safety and security are particularly important sectors for USTDA's technical assistance work.

TRAINING

USTDA provides training for foreign decision-makers in economic sectors where there are opportunities for the sale of U.S. equipment and services. The training is normally focused on technology or regulatory issues and is designed to give project sponsors a better understanding of U.S. experience and capabilities. Training can be conducted in the United States and/or in the host country.

TRADE AND INDUSTRY ADVISORS

Foreign government entities may obtain USTDA grants for trade and industry advisors. These advisors are typically located in ministries or municipalities, where they can help with capacity building activities relevant to trade regulations, standards or the import of technology and additional expertise.

Project Definition and Investment Analysis

FEASIBILITY STUDIES

USTDA provides grants for overseas infrastructure project planning assistance, such as feasibility studies. These studies evaluate the technical, financial, environmental, legal, and other critical aspects of infrastructure development projects that are of interest to potential lenders and investors.

ORIENTATION VISITS

Orientation visits bring foreign project sponsors to the United States to observe the design, manufacture, demonstration and operation of U.S. products and services that can potentially help them to achieve their development goals.

WORKSHOPS AND CONFERENCES

USTDA organizes workshops, conferences and technical symposia worldwide. These events are sector or project oriented and connect overseas project sponsors with U.S. firms and entities that supply project finance, technology and industry expertise that may be useful in project implementation.

PROCUREMENT ASSISTANCE

To promote project transparency and integrity, USTDA provides grants to assist in the establishment and oversight of international project procurement activities. Support can take the form of developing appropriate bidding procedures, assisting in the evaluation of technical proposals, and identifying potential suppliers or bidders.

How is a project brought to USTDA for consideration?

If you are developing a project or initiative that you would like USTDA to consider for possible grant funding, you should begin by:

1. Contacting the appropriate USTDA Regional Director or Country Manager for your region (see *How Do I Contact USTDA?*); or,
2. Communicating with the commercial or economic officer, or USTDA representative, at the U.S. Embassy in your country.

To formally initiate USTDA consideration of a project, a project sponsor should direct a request to USTDA. In cases where a specific U.S. company has been identified as a partner or preferred supplier on the project, the U.S. company submits a separate, detailed proposal to USTDA. There is no set deadline for projects to be considered.

How does the approval process work?

USTDA's due diligence review of a proposal involves two steps. First, USTDA staff conducts an internal review to determine whether the proposal represents an appropriate opportunity for USTDA support. Second, proposals that satisfy this internal analysis are then independently assessed by USTDA-funded definitional mission and desk study consultants. Because of the high demand for USTDA funding, not all proposals that meet USTDA funding criteria can be supported.

How does the grant process work?

If USTDA approves funding, it signs a Grant Agreement with the foreign project sponsor (the Grantee). The Grantee then signs a contract with the U.S. company it has selected, usually on a competitive basis, to carry out the USTDA-funded activity. Both the Grant Agreement and the contract contain the terms of reference that outline the parameters of the activity.

What are the responsibilities of the Grantee?

The Grantee is responsible for managing the USTDA-funded activity, including the review of invoices, and providing some limited administrative support.

Who pays the U.S. contractor?

The Grant Agreement is signed by USTDA and the Grantee. The U.S. contractor works under its contract with the Grantee and submits its invoices to the Grantee. Once the Grantee is satisfied with the work product, the invoices are approved and forwarded to USTDA, which then pays the contractor directly.

Do USTDA Grants have to be repaid?

USTDA funds are grants, not loans. Grantees are not required to repay USTDA for the grants they receive.

How much money is available?

Each year, USTDA funds approximately 125 grant activities. The average USTDA grant is $400,000.

This 47.5 megawatt power plant was constructed in the Aydin-Germencik geothermal field in Turkey by the Gurmat Energy Investment and Trade Company, a private Turkish company, following the findings of a USTDA-funded feasibility study. The plant, which became operational in May 2009, is providing an important renewable energy source to further Turkey's economic growth.

Where is USTDA located?

USTDA is active in every region of the world. The agency is headquartered in the Washington, D.C. area, in Arlington, Virginia. In addition, USTDA has representatives in South Africa and Thailand to promote the agency's program throughout Sub-Saharan Africa and Asia.

What other U.S. Government Agencies can I contact?

- U.S. & Foreign Commercial Service
  www.usatrade.gov
- U.S. Department of State
  www.state.gov
- Office of the U.S. Trade Representative
  www.ustr.gov
- Overseas Private Investment Corporation
  www.opic.gov
- Export-Import Bank of the United States
  www.exim.gov
- U.S. Agency for International Development
  www.usaid.gov
- Millennium Challenge Corporation
  www.mcc.gov

HOW DO I CONTACT USTDA?

More information about USTDA is available at *www.ustda.gov*. General inquiries about USTDA's program can be made by calling (703) 875-4357, sending a fax to (703) 875-4009 or an e-mail to *info@ustda.gov*, or completing the Contact Form on USTDA's website.

To contact USTDA's program staff, send an e-mail to your region of interest:

- East Asia:
  East_Asia@ustda.gov
- Europe and Eurasia:
  Europe_Eurasia@ustda.gov
- Latin America and the Caribbean:
  LAC@ustda.gov
- Middle East and North Africa:
  MENA@ustda.gov
- South and Southeast Asia:
  South_Southeast_Asia@ustda.gov
- Sub-Saharan Africa:
  Africa@ustda.gov

MAKING GLOBAL LOCAL

U.S. TRADE AND DEVELOPMENT AGENCY

The U.S. Trade and Development Agency (USTDA) helps companies create U.S. jobs through the export of U.S. goods and services for priority development projects in emerging economies. USTDA links U.S. businesses to export opportunities by funding project planning activities, pilot projects, and reverse trade missions while creating sustainable infrastructure and economic growth in partner countries.

MAKING GLOBAL LOCAL

OVERVIEW

Making Global Local is an initiative designed to connect towns and cities across the country with USTDA's programs. By building strategic partnerships, USTDA and local business organizations can support the creation of high-paying jobs through the growth of U.S. exports.

If you are committed to this goal and have local market knowledge, we want to partner with you. By understanding the Agency's programs, partner organizations can help companies in their communities maximize the benefits of working with USTDA.

Over the past year, U.S. companies have increasingly targeted emerging economies as export destinations. Given its unique role, USTDA is perfectly positioned to support U.S. businesses interested in entering or expanding their presence in developing and middle-income countries.

The Agency's signature International Business Partnership Program brings foreign delegates on reverse trade missions to the United States pending upcoming procurements. While in the U.S., the delegations observe the design, manufacture and operation of U.S. products and services that can help them achieve their development goals. Last year alone, USTDA supported 50 reverse trade missions that connected more than 600 foreign delegates with over 1,000 U.S. company representatives across the country.

Foreign buyers explore U.S. equipment on a USTDA-sponsored reverse trade mission.

PARTNER ORGANIZATIONS

Examples of partner organizations include:

- State, county, and city governmental entities
- Local non-profit economic development organizations
- Small Business Development Centers
- District Export Councils
- World Trade Centers
- Academic institutions

Benefits of becoming a Making Global Local partner organization include:

- Recognition as a Making Global Local partner organization on USTDA's website
- Direct delivery of USTDA news & events
- Access to a network of regional and industry experts to speak at events
- Opportunity to co-host USTDA roundtables
- Support for joint marketing and outreach campaigns

JOIN US!

Interested in becoming a Making Global Local partner organization? Contact us to learn how USTDA's programs can expand export sales in your community. We look forward to working with you!

Leila Aridi Afas
Director for Export Promotion
(703) 875-4357
lafas@ustda.gov

Christine Campigotto
Public Affairs Specialist
(703) 875-4357
ccampigotto@ustda.gov

VISIT US ON THE WEB: WWW.USTDA.GOV

USTDA supports the NEI's mission as a member of the President's Export Promotion Cabinet.

NEI NATIONAL EXPORT INITIATIVE www.export.gov

DELEGATION LIST

MR. KHURRAM GUL AGHA
GROUP HEAD, OPERATIONS & TECHNOLOGY
NIB BANK

MR. SYED BASIT ALY
DIRECTOR OF INTERNATIONAL COORDINATION
FINANCIAL MONITORING UNIT (FMU)
GOVERNMENT OF PAKISTAN

MR. INAYAT HUSSAIN
EXECUTIVE DIRECTOR, OPERATIONS GROUP
INFORMATION SYSTEMS & TECHNOLOGY
DEPARTMENT
STATE BANK OF PAKISTAN

MR. MOHIB HASSAN KHAN
CHIEF INFORMATION OFFICER
BANK AL-HABIB

MR. IMTIAZ MAHMOOD
EXECUTIVE VICE PRESIDENT (EVP)
HEAD OF INFORMATION TECHNOLOGY (IT)
MCB BANK LIMITED

MR. YOUSUF NASIR
HEAD OF INFORMATION TECHNOLOGY
UNITED BANK, LTD.

MR. ARIF SAEED
HEAD OF INFORMATION TECHNOLOGY AND RISK MANAGEMENT
ADAMJEE INSURANCE COMPANY LTD.

MR. TARIQ SAYEED
SENIOR COMMERCIAL SPECIALIST
U.S. COMMERCIAL SERVICE
U.S. EMBASSY ISLAMABAD

MR. IMTIAZ AHMAD SHEIKH
CHIEF INFORMATION OFFICER
ASKARI BANK

MR. SABAH UZ ZAMAN
CHIEF INFORMATION OFFICER
STATE BANK OF PAKISTAN (SBP)

MR. KHURRAM GUL AGHA
GROUP HEAD, OPERATIONS AND INFORMATION TECHNOLOGY (CIO)
NIB BANK

Khurram Gul Agha has served as the Group Head for Operations and Information Technology of NIB Bank since April of 2012. In this role, Mr. Agha is responsible for the revitalization of the Operations and Information Technology departments, all back-office operational functions, and centralization of operations for Corporate, Consumer, Trade, Treasury, Retail banking and ADC services. Mr. Agha manages a team of more than 1200 employees.

Prior to this role, Mr. Agha has served as the Group Head for Transactional Banking and IT with NIB Bank from 2010 until April 2012; Country Head for Pakistan at Firstdata from August 2008 to June 2010; the Executive Vice-President of the Cash Management, Financial Institutions and Home Remittances Cell at United Bank Limited from August 2003 to August 2008; Country Product Manager of Pakistan for Citibank N.A. from September 2002 to July 2003; Country Technology Officer for Pakistan for Citibank from October 1999 to September 2002; Electronic Banking Implementation Head for Citibank Pakistan from June 1998 to October 1999; Country Technology Head for TCS (Private) Limited from February 1997 to June 1998; Senior Manager for Technology with TCS (Private) Limited from December 1994 to January 1997; and Technology Manager for Pakistan Technologies (Private) Limited from March 1994 to November 1994.

Mr. Agha completed O-Levels through Cambridge University in 1984 and earned a Bachelor of Computer Science and Mathematics from the State University of New York – Binghamton in 1993.

MR. SYED BASIT ALY
DIRECTOR OF INTERNATIONAL COORDINATION
FINANCIAL MONITORING UNIT (FMU)
GOVERNMENT OF PAKISTAN

Syed Basit Aly has served as the Director of the Financial Monitoring Unit for the Government of Pakistan's Finance Division since March of 2011.

Prior to this role, Mr. Aly has served as Director of Strategic Planning and the Governor's Office for the State Bank of Pakistan from 2010 through March of 2011; Principal Staff Officer to the Governor for the State Bank of Pakistan from April 2003 to 2010; Section Officer in the Ministry of Finance for the Government of Pakistan from 2001 to 2003; and Assistant Commissioner within various subdivisions in Baluchistan from 1997 to 2001.

Mr. Aly has earned a Bachelor of Sciences in Electrical Engineering from the University of Engineering and Technology in Lahore, and a Master of Arts in Development Economics from Williams College. He has also completed numerous training programs throughout the world.

MR. INAYAT HUSSAIN
EXECUTIVE DIRECTOR, OPERATIONS GROUP
INFORMATION SYSTEMS AND TECHNOLOGY DEPARTMENT (ISTD)
STATE BANK OF PAKISTAN (SBP)

Inayat Hussain has served as the Executive Director for the Operations Group in the Information Systems and Technology Department (ISTD) of the State Bank of Pakistan (SBP) since September 2012. In this capacity, Mr. Hussain oversees a number of projects aimed at upgrading the Bank's existing IT infrastructure. He additionally represents the SBP as a Director on the board of the Pakistan Institute for Corporate Governance (PICG) and the International Islamic Market (IIFM), Bahrain.

Prior to this role, Mr. Hussain served in a number of positions at SBP, including the Executive Director of the Banking Policy and Regulations Group from September 2009 until April 2010, and again from June 2010 until September 2012. He was also the Executive Director of the Banking Supervision Group from April 2010 until June 2010; Director of the Banking Inspection Department from September 2006 until September 2009; Divisional Head of the Banking Regulations Division in the Banking Policy Department from January 2001 until September 2006; Assistant Director for SBP's World Bank Consultancy Project from August 1997 until January 2001; and Inspecting Officer for the Banking Inspection Department/Non-Banking Financial Institutions Regulation and Supervision Department from May 1993 until August 1997. Mr. Hussain has additionally served on a number of committees and task forces, such as the Corporate Rehabilitation Legislation Committee in 2009, as well as various Committees, Sub-Committees and Consultative Groups for the Securities and Exchange Commission of Pakistan (SECP).

Mr. Hussain is a Diplomaed Associate of the Institute of Bankers in Pakistan (DAIBP), and has earned a Master of Business Administration in Finance. He is a certified Associate Cost and Management Accountant (ACMA), Financial Risk Manager (FRM), and Chartered Financial Analyst (CFA).

MR. IMTIAZ MAHMOOD
EXECUTIVE VICE-PRESIDENT
HEAD OF INFORMATION TECHNOLOGY
MCB BANK LIMITED

Imtiaz Mahmood has served as Executive Vice-President and Head of Information Technology for MCB Bank Limited since July of 2012. In this role, Mr. Mahmood is responsible for the IT Operations, Enterprise Infrastructure, IT Software Solutions, IT Service Management, Information Security, and Business Technology and Project Management Divisions within the Bank, including IT finance, administration, human resources and procurement functions.

Prior to his current role, Mr. Mahmood served as MCB's Executive Vice President and Head of the IT Strategy & Capacity Planning Division from March 2012 through June 2012; Senior Vice President and Head of the newly created IT/IS Audit Division from January 2009 to March 2012; Vice President and Team Leader for the IT/IS Audit Department from January 2008 to December 2008; and Assistant Vice President and Senior Manager for the IT/IS Audit Department from March 2007 to December 2007. Prior to joining MCB Bank, Mr. Mahmood managed the IT Department at the Pakistan Credit Rating Agency Limited (PACRA) from April 1997 to March 2007.

Mr. Mahmood earned a Bachelor of Science in Mathematics and Physics from the Government Islamia College Civil Lines in Lahore, Pakistan in 1993. He has also received a Post-Graduate Diploma in Computer Engineering and Electronics (PGD-CEE) from the National Institute of Computer Engineering & Electronics, Lahore (Al-Khair University Lahore) in 1994, a Master of Business Administration (MBA) in Banking and Finance from the Syed Ali Hajvery University Lahore in 1996, a Master of Computer Sciences from the Institute of Computer Sciences ICS-NKFACT, Lahore's Executive Program in 2000, and an Advanced Diploma in Network Engineering (ADNE) from the National Engineers Training Services (NETS), Lahore in 2003. Additionally, Mr. Mahmood has also received a number of certifications in a range of information technology areas, from cyber forensics to cybercrimes to information systems auditing.

MR. YOUSUF NASIR
CHIEF INFORMATION OFFICER
UNITED BANK LIMITED (UBL)

Yousuf Nasir has served as Chief Information Officer of United Bank Limited (UBL) since April 2011. In this role, Mr. Nasir is responsible for all aspects of strategic IT planning, implementation and support worldwide.

Prior to his position with UBL, Mr. Nasir served as Chief Information Officer and Advisor for Strategy, PMO & Business Development at Arwen Technologies from March 2010 to March 2011; CIO for Bank al-Bilad, Kingdom of Saudi Arabia from January 2008 to February 2010; CIO for Habib Bank Limited (HBL) from February 2006 to January 2008; Vice-President for the Technology Division of Retail and Investment Banking of JPMorgan Chase from January 1994 to 2006; Senior Systems Engineer for Corporate Technology Services at Unisys from January 1993 through January 1994; and Network Engineer for Cuisenaire Company of America from January 1990 to January 1993.

Mr. Nasir earned a Bachelor of Sciences in Electrical Engineering from the N.E.D. University of Engineering and Technology in 1989 and a Master of Sciences in Electrical Engineering from the New Jersey Institute of Technology in 1991.

MR. ARIF SAEED

HEAD OF INFORMATION TECHNOLOGY AND RISK MANAGEMENT

ADAMJEE INSURANCE

Arif Saeed has served as the Head of Information Technology and Risk Management of Adamjee Insurance since January of 2011. In this role, Mr. Saeed is charged with the implementation of the Enterprise Risk Management Project, has prepared the Information Technology (IT) Operational Risk Management Plan and Disaster Recovery Plan, and ensures data security at all levels of the organization.

Prior to leading Adamjee's IT and Risk Management arm, Mr. Saeed was the Senior Vice President and Head of Projects at Atlas Bank Limited from 2008 to 2010; Manager of Product Support and Development at the National Bank of Fujairah (UAE) from 2006 to 2007; Head of the Banking and Financial Services Solutions segment of IMTAC Technologies, LLC of Dubai in 2006; Vice President of the Risk Management Group of the National Bank of Pakistan from 2003 to 2006; Globus/T-24 Project Manager of the State Bank of Pakistan (Central Bank) from 2001 to 2003; Director of AZM Computer Services (Pvt) Limited from 1999 to 2001; Business Analyst for First Chicago NBD Corporation from 1996 to 1999; and Assistant Manager with Adamjee from 1991 to 1994.

Mr. Saeed earned a Master of Sciences in Statistics from the University of Karachi in 1990, and a Master of Sciences in Business Administration from Boston University in 1998. His specialties include Risk Management, Information Technology, and Project Management.

MR. TARIQ SAYEED
SENIOR COMMERCIAL SPECIALIST
U.S. COMMERCIAL SERVICE
U.S. EMBASSY ISLAMABAD, PAKISTAN

Tariq Sayeed has served as Senior Commercial Specialist with the U.S. Commercial Service at the U.S. Embassy in Islamabad, Pakistan since March 1989. In this role, Mr. Sayeed reports on trade and regulatory matters that may impact trade between the U.S. and Pakistan. He also supports U.S. Trade Missions and other U.S. agencies, such as the U.S. Trade Development Agency (USTDA), Export-Import Bank of the United States and the Overseas Private Investment Corporation (OPIC) in developing projects in Pakistan.

Prior to this role, Mr. Sayeed served as the Audio-Visual Program Manager for the U.S. Information Service (ISIS) at American Consulate General Karachi from September 1986 to March 1989, and as Assistant Manager for Advertising and Public Relations for Jaffer Brothers Limited (JBL) from March 1985 to October 1986.

Mr. Sayeed earned a Bachelor of Sciences in Journalism and Advertising from Southern Illinois University in 1982 and a Master of Arts in Journalism and Public Relations from Northern Illinois University in May 1984.

MR. IMTIAZ AHAMD SHEIKH
SENIOR EXECUTIVE VICE PRESIDENT
ASKARI BANK

Imtiaz Ahmad Sheikh has served as the Senior Executive Vice President of the Technology Division of Askari Bank since June of 2012.

Mr. Sheikh possesses 31 years of diversified experience of managing versatile technology platforms. He has successfully established and effectively managed the IT setups of banks and organizations in Pakistan and overseas. Migration & Integration of legacy Banking Systems to Centralized Banking Systems, setting up of Data Centers and successful management of IT projects are hallmark of his professional competence.

Mr. Sheikh was the Chief Information Officer of Bank Alfalah Limited from 2007 to 2012. Prior to this role, he worked as Executive Vice President for the Information Technology Division of NIB Bank (Formerly PICIC Commercial Bank), a position in which he held for five years. Mr. Sheikh has also served as the Chief Operating Officer of io-2-io (Pvt) Ltd. and Vice President of Standard Chartered Bank (Formerly Union Bank).

Mr. Sheikh started his Career as Assistant Director Water and Power Development Authority (WAPDA) Pakistan in 1982 and was promoted as Deputy Director in 1987. He was associated with Electricity Corporation Riyadh (Saudi Arabia), USAID, GTZ and CIDA on deputation from WAPDA, where he completed various IT projects/assignments of critical importance.

Mr. Sheikh has earned a Master of Sciences in Computer Science from the University of Engineering and Technology, Lahore, Pakistan.

MR. SABAH UZ ZAMAN

CHIEF INFORMATION OFFICER (CIO)

STATE BANK OF PAKISTAN (SBP)

Sabah Uz Zaman has served as the Chief Information Officer of the State Bank of Pakistan since August of 2005. In this capacity, he has managed implementation of information technology systems and their sustained operations for the State Bank and its subsidiaries. Mr. Zaman has additionally restructured the IT department to merge the project teams with operational teams, a move for which he has received praise from the World Bank. He manages a team of approximately 120 employees with the assistance of two Deputy CIOs.

Prior to this role, Mr. Zaman served as the Local Integration and Assurance Manager (LIAM) for the Shell Corporation's Middle East-South Asia Cluster (MESA), managing the region of India, Pakistan, Dubai, Oman, Saudi Arabia and Yemen. He also served as a Systems and Applications Manager for Shell Pakistan from March 2001 until December 2004; JDE Team Member with Shell Services International from October 1998 until March 2001; and Methods Analyst and Systems Officer with Pakistan Burmah Shell (later Shell Pakistan) from August 1986 until January 1997.

Mr. Zaman earned his Master of Sciences in Physics from Karachi University in 1983. He is fluent in both English and Urdu.

U.S. DEPARTMENT OF THE TREASURY

The U.S. Department of Treasury is the executive agency responsible for promoting economic prosperity and ensuring the financial security of the United States. The Department is responsible for a wide range of activities such as advising the President on economic and financial issues, encouraging sustainable economic growth, and fostering improved governance in financial institutions. The Department of the Treasury operates and maintains systems that are critical to the nation's financial infrastructure, such as the production of coin and currency, the disbursement of payments to the American public, revenue collection, and the borrowing of funds necessary to run the federal government. The Department works with other federal agencies, foreign governments, and international financial institutions to encourage global economic growth, raise standards of living, and to the extent possible, predict and prevent economic and financial crises. The Treasury Department also performs a critical and far-reaching role in enhancing national security by implementing economic sanctions against foreign threats to the U.S., identifying and targeting the financial support networks of national security threats, and improving the safeguards of their financial systems.

The Department of the Treasury is organized into two major components the Departmental offices and the operating bureaus. The Departmental Offices are primarily responsible for the formulation of policy and management of the Department as a whole, while the operating bureaus carry out the specific operations assigned to the Department. Their bureaus make up 98% of the Treasury work force. The basic functions of the Department of the Treasury include:

* Managing Federal finances;
* Collecting taxes, duties and monies paid to and due to the U.S. and paying all bills of the U.S.;
* Currency and coinage;
* Managing Government accounts and the public debt;
* Supervising national banks and thrift institutions;
* Advising on domestic and international financial, monetary, economic, trade and tax policy;
* Enforcing Federal finance and tax laws;
* Investigating and prosecuting tax evaders, counterfeiters, and forgers.

The delegation will meet with the Office of Technical Assistance (OTA) whose core mission is to develop strong financial sectors and sound public financial management in countries where assistance is needed and there is a strong commitment to reform. Government financial management in all countries performs a dual function separate and unique from other executive activities – laying down a framework for national economic growth on one hand, and providing fiscal governance on the other. These responsibilities, when well executed, create the pre-conditions for stability and sustainable progress.

IBM

IBM's Institute for Electronic Government (IEG) was founded in 1995 as a resource for public sector leaders worldwide in electronic government. The IEG focuses on issues, which include public policy as it relates to technology strategy and execution, economic development and education, online citizen and business services, and e-democracy. As the public sector has worked to transform itself, the IEG has expanded its efforts to demonstrate best practices and leadership for the public sector as a whole.

The IEG includes a briefing center, which is utilized to deliver customized programs and events for government, banking and healthcare organizations. This facility houses demonstrations on innovation in the Public Sector, featuring modules of best practices, leading edge solutions, technology and case studies. Here, best practices are placed in the context of benefits to citizens, the economy and society. Over fifty thousand leaders (including Prime Ministers, Presidents and other high-level dignitaries) from over one hundred twenty countries have visited the facility since its opening.

IBM will highlight their successful banking architecture programs implemented around the world. In March 2010, IBM acquired Initiate Systems, a leading provider of customer-centric master data management and Enterprise Master Person Index (EMPI) software and services for the on-demand enterprise. Initiate Systems enables customer-focused business strategies by providing customer and patient data to people and systems in real time.

With Initiate Systems, banks can:

* Capture complete, accurate, real-time views of customer or patient data
* Improve patient safety and care efforts
* Help organizations comply with new regulations and privacy concerns
* Have a scalable solution to grow with future business

By enabling accurate data linking in real time, Initiate delivers the right data at the right time to all critical touch points. Initiate's proven experience makes it uniquely qualified to enable organization's strategic initiatives to increase revenue and efficiency while reducing operating costs and risks.

Mobile banking and payments solutions

Enable faster, less expensive, safer and more accessible mobile banking and payments

Highlights

- Enables new revenue sources while helping to reduce up-front costs with a security-rich platform for mobile transactions
- Allows cross-industry interoperability and collaboration through the Mobile Money Cloud and Trusted Service Manager platforms
- Facilitates responsiveness to changing market and regulatory demands through cloud delivery and analytics

Mobile banking and payments solutions from IBM can help you capitalize on the shift and growth of mobile-payments users and accelerate customer adoption. You need a low-cost platform that can handle high volumes of transactions and requires minimal up-front capital expenditures. You also need a trusted platform that can deal effectively with the multiple stakeholders involved in the mobile commerce ecosystem. Further, you want to reduce operational risk and improve responsiveness to changing customer and regulatory requirements.

Mobile banking and payments solutions from IBM can provide a comprehensive platform to help enable new revenue sources for banks, retailers and communications service providers. Leveraging cloud technology, we help enable faster, less expensive, safer and more accessible mobile banking and payments services. Our broad, interoperable mobile payments solutions can help lower operational costs and better align your income from mobile transactions with operating costs. A robust, security-rich platform can handle high volumes of transactions, enhance responsiveness and help enable distribution networks through a shared infrastructure.

Helping you find new revenue sources and reduce up-front costs

By helping you monetize transactions with a security-rich and easy-to-use mobile payments service, we can help you exploit the revenue opportunities created by the accelerated use of mobile technologies in developed and emerging markets. Our highly scalable platform requires minimal up-front investments and can deliver a safer mobile banking experience to help you reach the increasing numbers of users leveraging their mobiles devices to interact with banks, merchants and each other.

Helping improve interoperability and collaboration

A highly interoperable cloud solution can easily interconnect multiple stakeholders and support the business functions performed by participants. In developed markets, the Trusted Service Manager deals in an equitable manner with multiple parties, as well as provides a security-rich platform to manage identity, personal data and product lifecycle. In emerging markets, the Mobile Money Cloud can enable the replacement of cash transactions using mobile devices and also facilitate value-added services like transaction flagging for fraud detection. These two platforms can hide the technical and operational complexities of establishing a mobile payments ecosystem with minimal up-front investments.

Facilitating responsiveness to market and regulatory demands

Extensive data analytics capabilities can help you detect fraud and deploy anti-money laundering solutions on the network to help you manage your compliance requirements. Predictive analysis enables you to understand customer behavior, so you can improve your responsiveness to changing customer demands while building trust and adoption. With payments processed on one system, data collection for regulatory reporting can also be greatly simplified.

Why IBM?

Our extensive experience in the communications, banking and retail industries makes IBM uniquely suited to provide an end-to-end solution for cross-industry platforms. We offer comprehensive project management skills and experience gained from numerous successful client engagements worldwide. You can also leverage IBM Research technology and expertise in the field of data analytics, cloud computing and authentication (biometrics) to further monetize mobile commerce opportunities.

For more information

To learn more about mobile banking and payments solutions, please contact your IBM marketing representative or visit the following website: [illegible]

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: [illegible]

© Copyright IBM Corporation 2011

IBM Global Services
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
December 2011

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corporation in the United States, other countries or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at [illegible]

Other company, product or service names may be trademarks or service marks of others. References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

Please Recycle

BKS03009-USEN-02

Accelerating more flexible and efficient processing

Highlights

- Adopt a progressive approach to renovating the enterprise payments infrastructure
- Leverage "best-of-the-best" solution components from leading application providers
- Speed implementation with best practices and payments-specific solution accelerators
- Lower near-term cost, shorten time to value, and reduce transformation risk

The payments industry is the backbone of our global economy, enabling billions of financial transactions each day. The global marketplace looks to financial institutions to provide secure, fast and reliable payments processes. However, as payments operations have expanded to meet the needs of an evolving global economy, many have become fragmented, complex, inflexible and costly to maintain.

Banks today face tighter margins and greater pressure on fees. Global regulation and standardization initiatives are increasing the need for change. And while technology has enabled greater connectivity in payments, settlement systems and exchanges, these advances have also opened the door to new competitors. These market pressures are changing the way banks must operate.

A more streamlined payments infrastructure is required. However, large scale transformation efforts are often costly, risky and slow to generate a return on investment. Today, banks need a better approach that enables them to transform their payments infrastructure over time, project by project, leveraging the assets they already have and driving value along the way. Now banks can build a technology roadmap to meet these needs with the IBM Banking Industry Framework for payments and securities.

The IBM Banking Industry Framework provides a software platform with prebuilt payments-specific software extensions, solution accelerators and best practices to help you significantly speed time ro value in implementing solutions. It provides an approach for a progressive, managed, business-driven transformation of your payments and securities processing infrastructure.

As you prioritize your business needs, you have a choice in how to get started. Along with a selection of applications from leading independent software vendors (ISVs), the framework supports your transformation journey with payments and securities projects in the following solution areas:

Corporate services. *Support corporate customers with greater transparency and market-driven integration of cash management, liquidity, and trade services.*

Digital payments conversion. *Transform paper-based transactions with electronic processing.*

Payments process efficiency. *Create federated, enterprise processing for all payments and securities applications, reducing costs while improving efficiency.*

Retail payments. *Move from proprietary and aging systems to more flexible, supportable and available retail payments systems that are adaptable to changing market conditions.*

Regulatory compliance. *Transform your payments and securities processing to support regulatory standards such as SEPA and ensure compliance.*

SWIFTNet modernization. *Modernize your back-end applications to SWIFTNet services with a single window into industry-standard processing services.*

A framework approach delivers benefits quickly to your payments infrastructure. With improved monitoring and tracking of payments through the process, you can better manage your business processing, improve customer service, and enable transaction auditing transparency. By moving to dynamic process ronting, you gain the flexibility to change processes as yonr business needs change, further reducing costly manual intervention in processes. With better risk and security management, you can feel confident in the security of your payments processes each time a change is made or you integrate with a third party. Plus, as you simplify and create a more flexible infrastructure, you can integrate with enterprise risk management, core banking and customer-facing processes.

IBM is a global leader in financial services. Financial institutions around the world are using an industry framework approach to simplify their technology infrastructure. IBM can help you get on the path to greater agility, whether you're just starting out, seeking to optimize your existing infrastructure or somewhere in between. Talk to your IBM representative today about conducting a Business Value Assessment to identify ways to get started.

- A predefined design and flow for your processes and data
- A single window to SWIFTNet services and reliable processing of high volume messages and files
- Assets to help you build an enterprise payments hub that provides integrated high-level service performance through transaction-level visibility to payments
- Transformation of payments and securities message data to industry standards
- Efficient XML data management to industry standards
- Service-oriented architecture (SOA)-based services reference templates to help you develop payments business services faster
- Best practice business and technical implementation patterns for service-oriented architecture-based payments solutions

A major European bank needed greater payments systems flexibility and data accessibility to comply with European Central Bank regulations—and to improve its ability to identify and intercept payments associated with known terrorists.

IBM proposed a comprehensive solution to integrate new SWIFT messaging services into the bank's payments infrastructure. By acting to replace its rigid, point-to-point financial messaging infrastructure with a flexible, hub-based architecture based on tools from the Banking Industry Framework, the bank is now in step with broader trends in the banking industry. It is differentiating itself as one of the more agile players in the industry while reducing integration-related IT costs and time to deploy new capabilities. At the same time it has improved its ability to offer global banking services, increased customer satisfaction and distinguished itself through new payments-related services that drive revenues.

NACHA, THE ELECTRONIC PAYMENTS ASSOCIATION

NACHA administers the Automated Clearing House (ACH) Network, which is a secure electronic network designed to directly transfer funds and data from one depository institution account to another. The network facilitates global commerce by serving as a safe and efficient payment system accessible by more than 14,000 financial institutions. This results in more than 19 billion ACH payments during the year 2009. NACHA develops operating rules and business practices for the ACH Network and for electronic payments in various areas. These areas include internet commerce; electronic bill; invoice presentment and payment (EBPP, EIPP); e-checks and financial electronic data interchange (EDI); among others.

NACHA has several functions, including serving as the rule-making body for the ACH Network and other payment systems; facilitating the development of new payment applications; identifying and implementing risk management initiatives; providing and supporting education programs; instituting and monitoring the quality controls in the payments system to improve member communications; and responding to regulatory and government relations issues relating to market electronic payment services.

ACH is a batch-oriented processing system for electronic network financial transactions. A batch-oriented processing system allows for large volumes of credit and debit to be processed in periodic batches, rather than in real time. ACH credit transfers include direct deposit payroll and vendor payments, while their direct debit transfers include consumer payments on insurance premiums, mortgage loans and other kinds of bills. Debit transfers also include new applications such as the Point-of-Purchase (POP) check conversion pilot program sponsored by NACHA. Virtually all of the 14,000 depository financial institutions in the U.S. are linked to the ACH network.

The Federal Reserve Banks are collectively the nation's largest automated clearinghouse operator. In 2005, they processed 60% of commercial interbank ACH transactions. The Electronic Payments Network (EPN), the only private sector ACH operator in the U.S., processed the remaining 40%. FedACH is the Federal Reserve's (Fed) centralized application software used to process ACH transactions.

NACHA
The Electronic Payments Association®
13450 Sunrise Valley Drive • Suite 100 • Herndon, VA 20171
Phone: 703-561-1100 • Fax: 703-787-0996
eMail: info@nacha.org
www.nacha.org

November 5, 2012

BY EMAIL: regs.comments@federalreserve.gov

Rovert deV. Frierson
Secretary, Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

Re: FR 3066a, b, c, and d; OMB control number: 7100-TBA

Dear Secretary Frierson:

NACHA – The Electronic Payments Association[1] respectfully submits this response to the Request for Comment regarding Proposed Agency Information Collection Activities (RFC) issued by the Board of Governors of the Federal Reserve System. The RFC requests comment on proposed information collection activities (surveys) and specifically (a) whether the proposed collection of information is necessary for the proper performance of the Federal Reserve's functions, including whether the information has practical utility; (b) the accuracy of the Federal Reserve's estimate of the burden of the proposed information collection, including the validity of the methodology and assumptions used; (c) ways to enhance the quality, utility, and clarity of the information to be collected; (d) ways to minimize the burden of information collection on respondents, including through the use of automated collection techniques or other forms of information technology; and (e) estimates of capital or start up costs and costs of operation, maintenance, and purchase of services to provide information. These surveys would be designed to collect information needed to support the Federal Reserve System's role in the retail payments system.

[1] NACHA manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data. The ACH Network serves as a safe, secure, reliable network for direct consumer, business, and government payments, and annually facilitates billions of payments. The ACH Network is governed by the *NACHA Operating Rules*, authored by NACHA, which guide risk management and create certainty for all participants.

NACHA, a not-for-profit organization, helps manage the ACH Network through its board of directors, staff, and various committees. NACHA represents nearly 11,000 financial institutions via 17 regional payments associations and direct membership. Through its industry councils and forums, NACHA brings together payments system stakeholders from all types of organizations to enable innovation that strengthens the industry with creative payment solutions.

NACHA's specific comments are limited to (a) *Whether the proposed collection of information is necessary for the proper performance of the Federal Reserve's functions, including whether the information has practical utility.*

NACHA General Comments.

The ACH Network is the direct payment Network, enabling the direct movement of money and information from one bank account to another. In this regard, the ACH Network plays an important role in the payments landscape, serving as a safe, efficient, high-quality and ubiquitous payments system that enables billions of Direct Deposit via ACH and Direct Payment via ACH payments annually.

The Federal Reserve's triennial payments study serves as a benchmark for the payments industry and provides data that is otherwise unavailable. This unique information identifies industry trends and shapes new opportunities. As such, NACHA has used the information collected from previous surveys to support strategic planning for the ACH Network, and in working with the industry to support payments innovation.

NACHA views the proposed collection of information as consistent with and central to the Federal Reserve's functions as they relate to the promotion of the safety and efficiency of the domestic payments system, which is integral to the national economy. The information that is collected and publicly shared by the Federal Reserve is used in whole or in part by diverse parties in the private and public sectors that have an interest in the continued use and development of solutions that leverage the domestic payments system in a safe and efficient manner. Organizations including financial institutions, processors and solutions providers, end-users, payment network administrators and other stakeholders rely on the output to understand and monitor trends, establish benchmarks, educate users, and inform risk management, product and network strategies.

With the broad reliance on the information, the veracity of the data and the credibility of the party responsible for its collection, analysis and dissemination are critical. Given the Federal Reserve's unique role in the domestic payments system, relationship with entities that utilize it, and demonstrated proficiency and reputation in this regard, NACHA supports the Federal Reserve activities as proposed in FR 3066a, b, c, and d. NACHA does not believe respondents would find the information collection burdensome. In addition, costs to provide such information should be *deminimus*.

With respect to the ACH Network, NACHA supports the requesting respondents to report the number and value of ACH volumes into subcategories to identify interbank ACH payments and help avoid double counting correspondent ACH volumes. This would give a more accurate picture of volume of transactions flowing through the Network.

* * *

If I can be of further assistance, please do not hesitate to contact me at (703) 561-3943 or bsullivan@nacha.org.

Sincerely,

/S/

William D. Sullivan
Senior Director & Group Manager
Government & Industry Relations

EXPERIAN

Experian is the leading global information services company, providing data and analytical tools to clients in more than 90 countries. The company helps businesses manage credit risk, prevent fraud, target marketing offers and automate decision making. Experian also works with local banks and financial institutions in countries without an existing credit bureau.

The company maintains a comprehensive information security program that contains administrative, technical and physical safeguards. These safeguards are designed to ensure the security, confidentiality and integrity of information. In addition, the safeguards protect against any threats or hazards to security.

Experian provides two key services to financial institutions. First, they seek to better understand risk associated with consumer loans. Data, including payment information, is collected from banks and given to credit bureaus. These bureaus process and re-pass the data to the banks to further analyze consumer behavior with other financial institutions to understand consumer behavior and evaluate risk.

Experian also manipulates data and model statistics to better understand risk behavior. This information is entered into complex databases, allowing for automated decisions. These credit and/or banks scores, assist financial institutions manage their financial relationships with businesses and consumers.

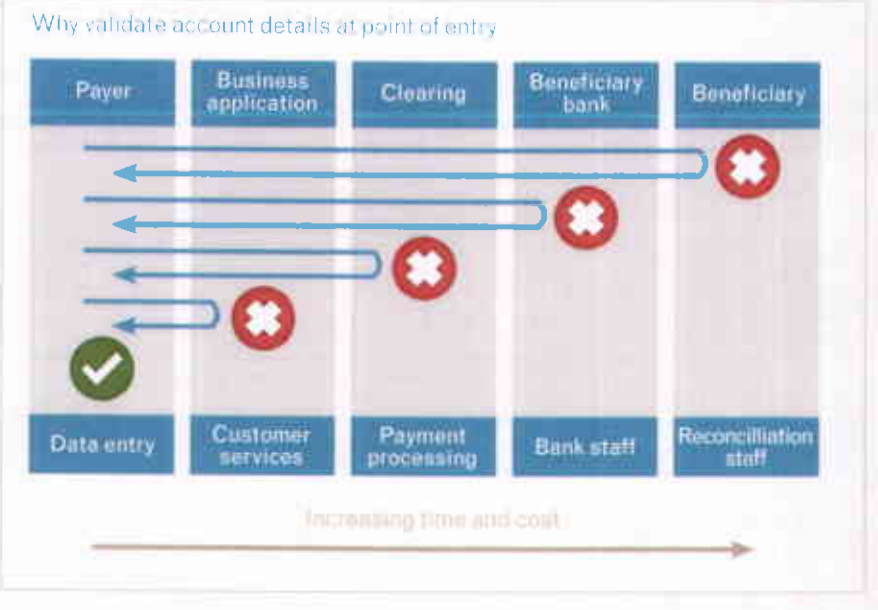
5 ways to make sure your payments get straight through

An Experian Payments guide

Experian™
Payments

5 ways to make sure your payments get straight through

1. Get customer details right at the point of sign-up



2. Reduce the risk of fraudulent payments

By confirming that bank account details are correct and that the account actually belongs to your customer you can be sure that the account you are making a payment to, or collecting a payment from, is genuine. This minimises the risk of fraudulent payments being processed. This is even more pertinent since the introduction of UK Faster Payments as payments can now be sent in 15 seconds and cannot be revoked.

3. Remove paper-based processes

By reducing paper based processes that take up unnecessary time and resource you can reduce delays in the customer sign-up process, and improve customer take-on rates. Also manual rekeying of data wastes valuable time and is open to error, causing payment delays and rejections. By reducing the amount of paper-chasing in the process, you can free up staff time, and remove inefficient manual steps.

4. Consolidate disparate payment systems

By consolidating all your back office payment submissions into one fast secure file for both your Faster Payments and Bacstel-IP submissions you'll optimise payment routing and ensure efficient, Straight-Through-Processing of your payments.

5. Automate your payments process

By automating some, or all, of your collections and payments processes you will minimise the need for manual intervention which can be prone to human error, and cost you valuable time and resource. Automation also provides a full audit trail: making staff more accountable resulting in fewer mistakes, fewer delays and reduces the cost of rejected payments.

Summary

Whether you collect customer payment details in-store, over the telephone or via your website Experian Payments can enable Straight-Through-Processing of your payments and help to:

1. prove that your bank account data is correct at the point of capture to minimise rejections and delays.
2. confirm whether the account details you is given actually belong to your customer to reduce the risk of fraudulent payments.
3. remove paper-based processes which are prone to errors and cause payment delays.
4. consolidate payments from multiple applications and submit automatically to payment services such as BACS and Faster Payments to ensure your payments are routed efficiently.
5. automate all, or part, of your payments process, removing the need for unnecessary human intervention which can lead to errors.

Let Experian Payments help you to maximise the efficiency of your payments systems and processes to ensure secure, Straight-Through-Processing of your payments.

"Since implementation, Bank Wizard has reduced administration costs and payment processing times and dramatically improved the efficiency of our payments function. The confidence we now have in terms of the accuracy of our payments has enabled us to introduce a refund service via Bacs, once again improving the service we are able to provide to our constituents."

Claire Blunden,
ICT Systems Support Officer
Basingtoke and Deane Borough Council

MICROTECH

MicroTech, a Service-Disabled Veteran-Owned Business (SDVOB), is a prime contractor on over 100 Federal projects and holds more than 25 procurement vehicles, offering access to 2500 vendors and over a million technology products and services across the government. MicroTech is also certified by the National Minority Supplier Development Council (NMSDC).

MicroTech offers technology services, network systems integration, unified communications & collaboration, product solutions, cloud computing, cyber security, mobility and social media solutions to commercial enterprises, as well as the public sector — managing over half-a-million tech users daily.

With further industry adoption of Cloud Computing, data storage solutions are evolving, however all have the same needs — redundant regulated power, high bandwidth Internet connections, physical and network security, as well as 24x7x365 monitoring and full technical support.

MicroTech can help banks acquire the latest smartphones and other mobile communications devices and design enterprise client and mobile computing architecture to meet these challenges. The company's experience as a leading integrator of advanced technology in large enterprises can benefit your organization by providing cost-effective and rapid deployment of efficient systems.

Unified Communications & Collaboration

MicroTech
Taking Technology Further...®

What is MicroTech UCC?

The Unified Solution to Your Disparate Messaging, Voice, Video and Web Communications

Map Your Communications Journey

It's time to leave behind the outdated, unsecured, non-compatible systems and embrace what your business needs to secure messaging, accelerate communications, and stay competitive:

Then: Primitive, slow Web-based e-mail

NOW: Secure "real-time" multimediacapable e-mail/ calendaring, text messaging, Web 2.0 Social Media

Then: Unsecure, public shareware Instant Messaging (IM)

NOW: Instant e-Presence detection drives business applications across the supply chain

Then: Traditional old-school analog phone

NOW: Software-powered global VoIP and Smart Phone capabilities

Then: Sporadic, unreliable, unsecure Web conferencing

NOW: Enterprise-class, online secure business collaboration

Then: Siloed Video Conferencing room systems

NOW: Immersive High-Definition (HD) Telepresence solutions that leverage multiple technologies to facilitate fast and effective decision making

"Many companies have messaging by voice and e-mail, but when they are integrated [through Unified Communications], a user can 'see' voicemails and have e-mails read aloud...deliver[ing] increased productivity and efficiency, and greater customer satisfaction." – Industry Week

Modern business technology offers a myriad of ways to stay in touch: Instant Messaging, e-mail, Voice over Broadband, Smart Phone, Video Conferencing –- the list continues to grow. Unfortunately, many of the communication applications that have become essential to doing business are not compatible with your legacy technology or easily integrated. And how can you keep up with the latest versions or new technology?

MicroTech Unified Communications & Collaboration

To combat the challenge of disparate communication systems, businesses are turning toward MicroTech's Unified Communications & Collaboration (UCC) solutions to improve message response time, secure proprietary exchanges, and to more effectively communicate with remote offices and an increasingly mobile workforce.

Customized—Vendor Neutral—Scalable

Every organization has unique requirements and limitations; there is no one-size-fits-all when it comes to a UCC solution. Award-winning technology integrator, MicroTech, offers a customized, scalable vendor-neutral solution that is just right for you. Our expert team of certified engineers and developers will review your existing technology, listen to your needs, and design and install a viable, secure solution that meets your mission requirements.

Communication Challenges

Technological innovation and enhanced communications have offered a new set of challenges for today's workforce:

Technology Overload

Potentially indispensible technologies like VoIP, video and Web conferencing, instant messaging, and e-mail are sometimes not easily integrated

Distributed Customers, Mobile Workforce

Non-integrated communication systems lead to delays in decision making, increased travel, and a slow response to customer needs

Fragmented IT Infrastructure

Piecemeal communication networks comprised of a variety of unsecure teleconferencing systems, PBX exchanges, free add-on instant messaging, and other distribution technologies tie up IT departments and leave your network vulnerable

CONTENT MANAGEMENT AND WORKFLOW

Benefits of MicroTech Unified Communications & Collaboration:

- Improves knowledge management
- Increases worker productivity
- Enables faster decision making
- Provides across-the-network communications security
- Reduces costs and energy consumption
- Creates better relationships across functional groups

Gain A Competitive Advantage

Cut costs by simplifying your IT administration and communications infrastructure with a Unified Communication & Collaboration solution from MicroTech:

- Integrate into existing infrastructure
- Eliminate parallel investments in PC / Telephony technologies
- Replace third-party solutions with security, compliance, automatic updates
- Complement onsite software with hosted services
- Use single identity for easier administration
- Streamline deployment with modular, flexible set up
- Centralize management security and control

MicroTech is one of the top innovative companies in the world and offers Unified Communications & Collaboration, Technology Services, Network Systems Integration, Product Solutions, Cloud Computing, Cyber Security, Mobility, and Social Media Solutions to leading commercial enterprises, as well as the public sector.

MicroTech Procurement Vehicles

MicroTech is a Prime Contractor on prominent contract vehicles:

- GSA Schedule 70/58-I/874 MOBIS
- GSA 8(a) STARS II
- NASA SEWP IV
- Navy SeaPort-e
- Army AMCOM EXPRESS
- Army ITS-SB
- Army OPTARSS II
- Army APC2
- FAA SAVES
- FAA eFAST
- FBI IT Triple S
- JTC/SIL ITECS Equipment (AMCOM)
- SEWP DFAS CUPA
- SEWP USDA CUPA
- USCG VTC BPA
- USMC VTC BPA

UCC Strategic Partners

CHRISTIE · POLYCOM · AMX · LifeSize · Vidyo · CRESTRON · Jupiter · GlobalMed · AMD · ForTheRecord · VBrick

MicroTech
Taking Technology Further.®

MicroTech Unified Communications & Collaboration
UCC@MICROTECH.NET | 8330 Boone Boulevard Suite 600; Vienna, VA | 703-891-1073
Follow MicroTechBUZZ on Twitter | Like MicroTech on Facebook
WWW.MICROTECH.NET

UNISYS

imagine it. done.

UNISYS CORPORATION

Unisys is a worldwide information technology company that provides a portfolio of IT services, software, and technology that solves critical problems for clients. The company specializes in helping clients secure their operations, increase the efficiency and utilization of their data centers, enhance support to their end users and constituents, and modernize their enterprise applications. To provide these services and solutions, they bring together offerings and capabilities in outsourcing services, systems integration and consulting services, infrastructure services, maintenance services, and high-end server technology. With approximately 22,500 employees, Unisys serves commercial organizations and government agencies throughout the world.

Unisys has recently switched to Dovetail technology to support their Open Payments Platform (OPP). Dovetail's solution forms the payment hub for OPP, alongside solutions from Oracle for reporting and business intelligence, OPP is intended to be based on a Service Oriented Architecture (SOA) and J2EE, with Unisys settling on a buy versus build route at an early stage. Unisys' OPP is being positioned for banks wanting to migrate from their disparate legacy platforms. By virtue of supporting both high and low volume payments, the Dovetail platform is ideal for a phased migration by product and/or country, onto a single architecture.

In addition, Unisys released an updated version of its Urbis universal banking system and migrated the solution from Unix to the Microsoft .NET development platform in 2012. According to the company, this enables faster implementation, lower total cost of ownership and better integration with financial institutions' existing systems.

The Unisys Urbis solution comprises 27 modules supporting mission-critical banking operations, including retail, treasury, private banking, back office operations, risk management and trading. Unisys has enhanced the Urbis core banking solution to help customers differentiate themselves in all areas of banking, from private banking to trading. The updated solution incorporates one centralised database for all product data; and updates of account, balance, settlement and position information, as well as risk exposure updates, in real-time. Urbis also features centralized customer records, along with comprehensive analytical and reporting capabilities.

UNISYS
imagine it. done.

ORACLE

white paper

Benefits of Payments Business Intelligence

insight.

Preface

Imagine having the insight to make the right decisions on payment fees, consolidation and outsourcing strategies, and payment products that result in the best bottom line results for your banks' payments business. Critical to making the best decisions is visibility into the volumes, costs, revenue, and trends across a consolidated view of the enterprise payments business. A payments data warehouse with business intelligence and analytic reports provides the visibility necessary to make the best payment business decisions.

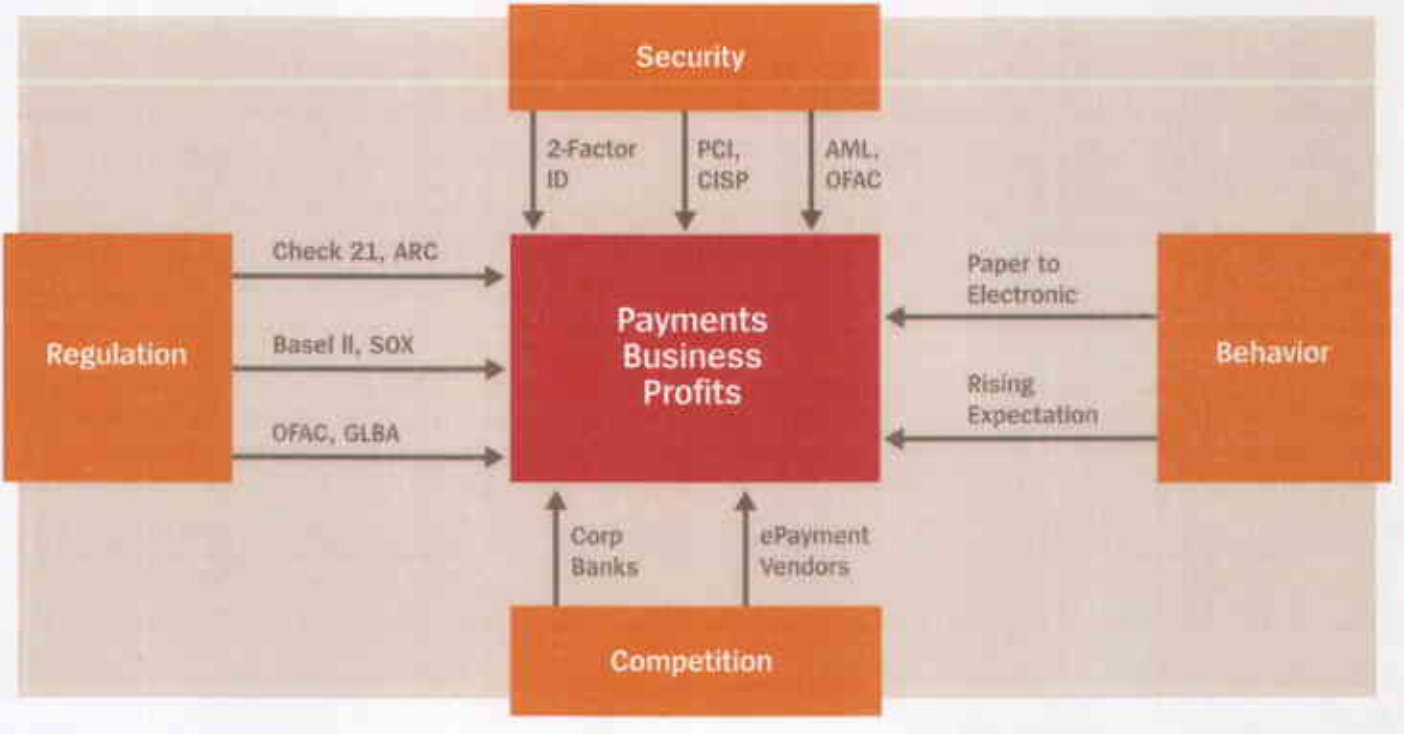
The Financial Insights' report *Enterprise Payments – Assessing the Concept*, states that "Banks are increasingly focusing on their payments infrastructure as an under managed and underutilized resource that is ultimately responsible for up to 40% of their revenues." Clearly anything responsible for this much of a bank's revenue warrants attention.

Forces Driving the Payments Market

Your customers expect the same level of speed, service and visibility when they make or receive payments as when they ship or receive packages. Specifically, they expect money to be transferred quickly and securely, and to know when, where and how it is being transferred. At the same time, banks must meet new payment and data security regulations, including Check 21, NACHA rules promoting check conversion to ACH, Single European Payment Area (SEPA) and Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET) while reducing the time and cost of payments processing. Fortunately, many of these new regulations have removed restrictions and opened the door for faster, better, smoother payments processing.

Additionally, a host of competitive and technology trends such as volume shifts and electronification makes enterprise payments an even more complex challenge and threatens overall profitability. For many banking innovators and leaders success starts with the right enterprise payments strategy, one that drives clear visibility into interconnected processes and costs across payment silos – from payment capture to cross-border payments, from check truncation to anti-money laundering.

Payments Business Pressures



A critical early step towards an enterprise payments strategy is an understanding of your payments business. Modeling and monitoring changes in payment volumes and associated fee revenue and processing costs provide insight into the bottom line for your payments business. As the March 2006 Gartner report *Payment Hubs Are the First Step in the Evolution of the Banking Payment Business* states, "One of the first tasks of the new generation of payment architectures is to achieve a better use of the information generated by payments and other transactional activity." According to the same report, "Companies are reproaching their banks for a lack of transparency in the pricing of their payment services."

What Executives Should Know

Most banks think that they know their payments business. They must since it may represent as much as 40% of their revenues, right? But do bank executives really know their payments business across the enterprise? Are they aware of how it is performing and transforming at any point in time, and are they ready to make informed decisions? BITS is the Technology Group for The Financial Services Roundtable. At a BITS forum, Webb Edwards, Wells Fargo's EVP overseeing technology operations, communications systems and payments strategies at the time, stated that bank executives should be able to answer these questions about their payments business:

- If asked for a consolidated view of how payments fall to the bottom line of my company is it available and would it be accurate?
- If two or more of my businesses had a conflict about payment direction, would I know it and would I have the ability to make a direction call based on financial facts?
- Who can sit down with me and describe our payment core competencies and how do they fit into our business strategies?
- Who is examining our existing infrastructure and planning our strategies for maintaining or growing fee income at existing or improved margins?
- What measurement and incentive systems need to be changed to build collaborative decision making across the enterprise?

How can bank executives gain insight into their payments business and make decision based on financial facts? According to the July 2005 Financial Insights report, *How to Get to the Promised Land: Alternative Pathways to Enterprise Payments,* "The simplest solution, creating a 'payments council' or 'payment czar', will not succeed unless it is accompanied by real authority over the payment silos and their budgets. Creating a single payments database for management and reporting purposes is a positive step forward, in that it can be turned into a product as well."

Several leading banks have recognized the need to better understand their payment business and address improvements in it holistically. A leading bank in the Southeast U.S. formed a Payments Think Tank with the following goals:

- Bring senior level managers together to form a comprehensive, cohesive view of issues surrounding the payments systems
- Eliminate further erosion of financial institution's control of the payment systems

The benefits gained from Unisys and Oracle Payments Business Intelligence Accelerator is greater insight into your payments business to enable business decisions that drive revenue growth as well as improved business agility, lower costs, and reduced risk and liability.

- Ensure the bank is addressing payment system issues in a holistic fashion rather than a product-by-product basis
- Develop an understanding of the economics of various payment types at the bank
- Determine ways to maximize the profitability of payments at the bank
- Continuously measure and document the costs, revenues, and service quality of payments and compare findings to available Industry data

This bank also had some questions that they felt bank executive must be able to answer about their payments business including:

- Can you gather all the required data for each payment type? (cost, revenues, quality, timeliness, productivity, etc.)?
- Do you know how clients use your payment products and services?
- Do you understand your banks' core payment competencies, core products, and how market/client process changes will affect them?
- Does your CEO truly know the importance of Payments?

So, how do bank executives achieve visibility into their payments business? According to the Financial Insights July 2005 report, *"A Key Element of Enterprise Payment Solutions: Reporting and Analytics*, this consists of databases and reporting systems optimized for the following purposes: transaction monitoring and alerts, liquidity management, management reporting and analysis, and customer inquiry."

Solutions for Payments Business Intelligence

To drive the best decisions for their bank, bank executives need to get better payments business intelligence to make informed business decisions. Because various payment types such as check, ACH, Wire Transfer, Credit Card, Debit Card, and Stored Value Cards have evolved over time as independent silos, it is very rare that a bank has an integrated, accurate, and continuous view of their payment business. As a consequence, they don't know how their decision may affect the business.

In a recent example at a top 10 U.S. bank, the checking account statements being mailed to customers included statement stuffers from the various payment silos. One encouraged the customer to adopt online bill payment. Another promoted direct account debit for bills. A third offered bill payment on the bank-issued credit card. All advertisements implicitly discouraged bill payment by check. Such conflicting silo-driven advertisement is confusing to customers and demonstrates a lack of payment insight on what is best for the bank's payments business and its customers.

Start by Collecting Payment Data in a Common Place

Most payment data is collected in the payment silos today. There are payment silos for retail checks, corporate checks, ACH, Domestic Wire Transfer, International Wire Transfer, Credit Card, Debit Card, and emerging Stored Value Cards. Any reports or analytics are typically at a point in time on the payment data for the payment silo.

Yes, you may be able to get transaction counts, monetary totals, and research individual transactions, but you cannot analyze cost and revenue factors associated with the transactions to determine profitability. You can't see volume and profitability trends by payment type over time, by geography, or by customer type. You can't perform customer segment payment profitability analysis across all payment types. Why? Because the payments data is collected and reported in silos, and there is little cost, revenue, region, or client data associated with the payment transactions.

Implement a Payments Data Warehouse

A payments data warehouse that collects all payment transaction data for all payment types over time can provide the start of the solution. It needs to include more than just the payment transaction. Dimensions such as the payment origination point, processing method, associated cost and revenue with the transactions at that point in time and in that regional location need to be included. The client segment, region and client identifier need to be recorded. A secure audit trail of all processing steps for the payment needs to be recorded.

Unisys and Oracle have collaborated to apply Oracle Data Warehouse and Business Intelligence tools to create a payments data warehouse with payments business analytics that provides a solution. Oracle's Data Warehouse Builder automates the process of building and populating a Data Warehouse.

Oracle's Data Warehouse includes Extract, Translate, and Load (ETL) tools to populate the payment data warehouse from the payment silos and cost/revenue accounting systems. The data warehouse can be implemented to store large amounts of data from the multiple payment types over time, and include dimensions such as the geographic region, customer segment, and processing method. The ETL tools enable rule-based automated capture and process flow from the legacy data sources.

Oracle Data Warehouse and Business Intelligence Platform
Complete and Integrated

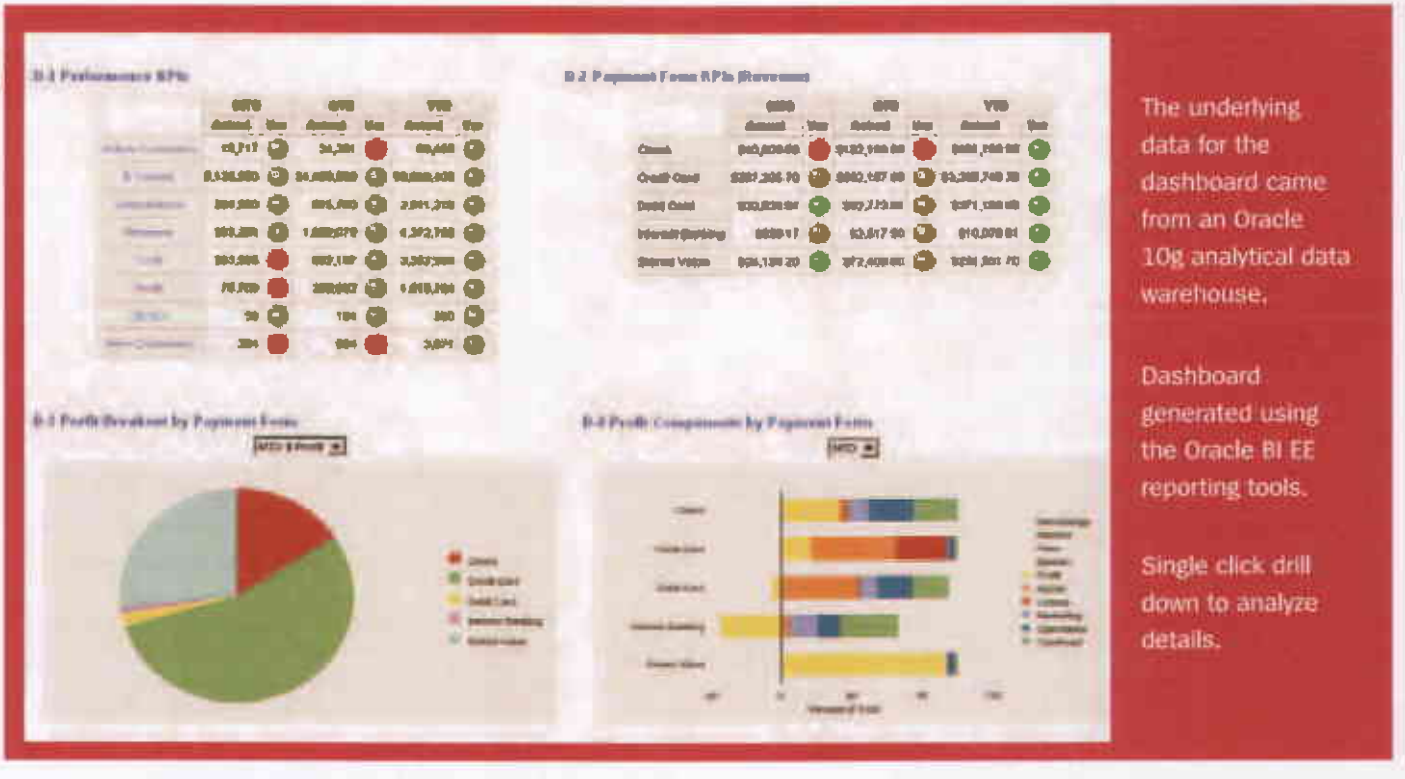
Maintain Privacy and Security of Payment Data

Maintaining the privacy and security of client payment data and enforcing authorized access is essential, especially with data from multiple payment types now consolidated in one database. New regulations such as SB1386 and industry imperatives like VISA's Cardholder Information Protection Program increase the obligations to protect sensitive client and payment data and corresponding penalties for not doing so. The Oracle Data Warehouse includes transparent data encryption features to keep data secure. Role based access control, change control, and audit trails can be used to ensure that only authorized access is provided to the data.

Extracting Business Intelligence from Payment Data

Once payment transaction data and associated client and business data are stored in a common data warehouse, the stage is set to create business intelligence reports and a payments business dashboard. Unisys has applied the Oracle Business Intelligence (BI) tools to create a payments business dashboard and a base set of business intelligence reports from the payments data warehouse. The Oracle BI tools include capabilities to automate the data warehouse discovery process. Graphical BI tools are used to produce dashboards, graphs, and reports that can be integrated with web portals, spreadsheets, and enterprise reporting tools.

Payments Business Intelligence Accelerator
Payments KPI Dashboard



The underlying data for the dashboard came from an Oracle 10g analytical data warehouse.

Dashboard generated using the Oracle BI EE reporting tools.

Single click drill down to analyze details.

Ad hoc payment research queries are supported. Dashboards, reports and graph displays can be updated in real-time to reflect the current state of the payments data. Trend reports can be produced by time, region, customer segment, and payment processing type. Best of all, the tools make it flexible enough to produce new payments reports in hours to meet new payments business intelligence needs.

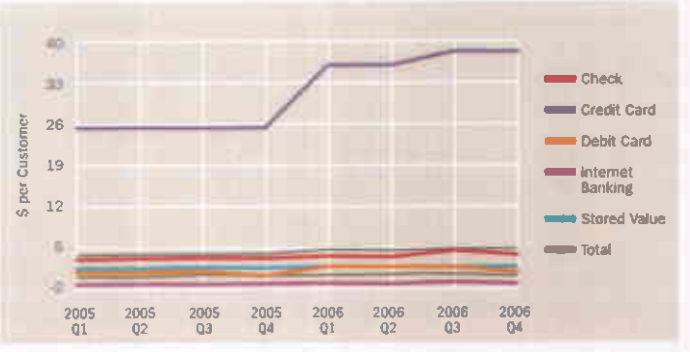
Payments Insight to Improve Business

The payments business intelligence reports and analytics should be available at any point in time and should operate on a holistic and up-to-date view of all of the payments data. The reports and payments dashboard should provide the intelligence necessary to make informed decisions on the payments business based on financial facts such as:

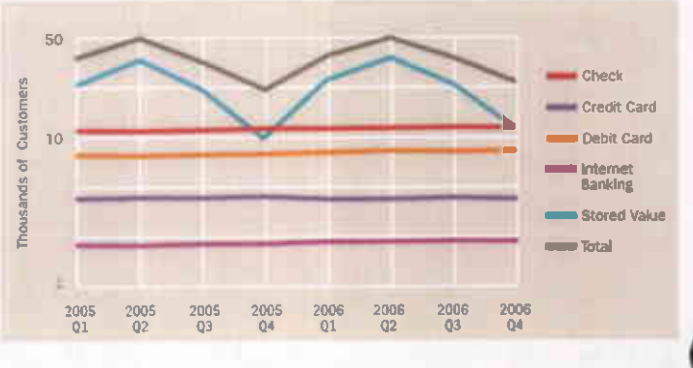
- Customer usage trends including the volume, channels used (branch, online, mail, ATM, VRU, Phone), type of payment (Check, ACH, Debit, Credit, Wire, Account-to-account, International versus Domestic), and average payment value by type and channel
- Fees/revenue by channel, payment type, and processing method
- Costs by channel, payment type, and processing method (e.g. checks processed as paper, converted to ACH, processed as Image Replacement Documents (IRDs) or images)
- Average payment processing time by channel and payment type
- Customer satisfaction by channel and payment type
- Periodically updating dashboard of payment incoming, processing, and outgoing item and $ volumes
- Analytics and trends such as most profitable customer segments, geographies and payment types used by customer segments

Payment Trends Dashboard

D-5 Quarterly Profit Trend by Payment Form

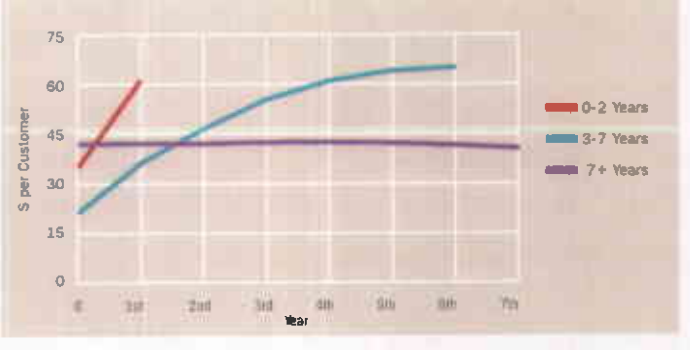


D-6 Active Customer Trend by Payment Form

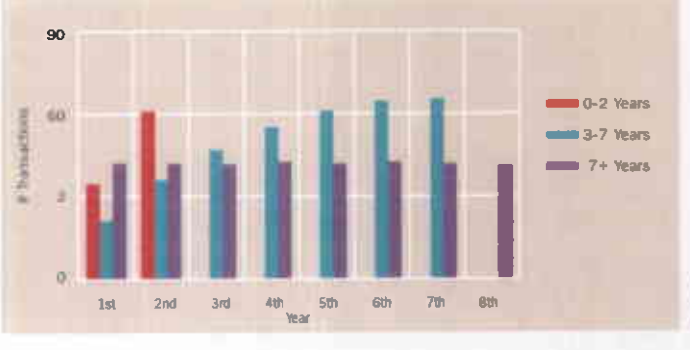


Payment Trends by Customer Segment

D-7 Profitability Over Time by Start Cohort



D-8 Transactions Over Time by Start Cohort



There are many more business intelligence reports possible once the Data Warehouse is established. Some of the desired reports mentioned by banks include:

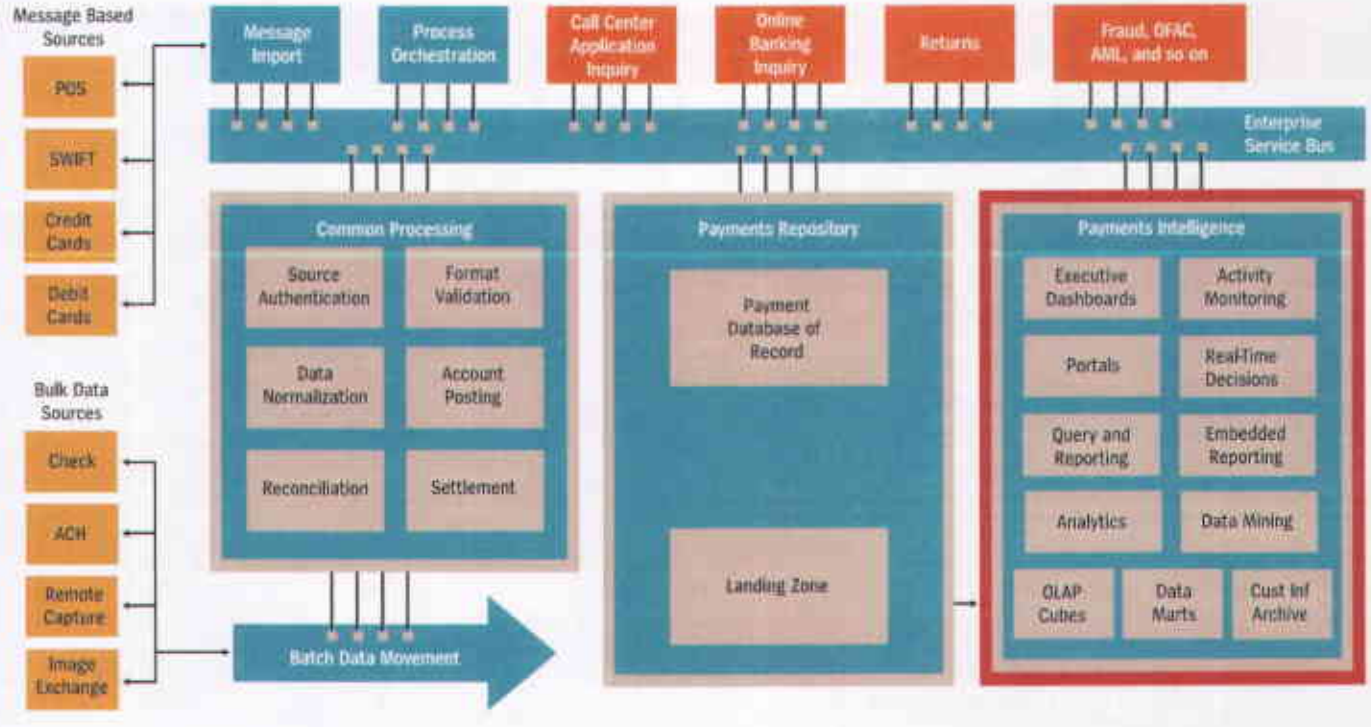
- Payment $ volume by payment type by quarter, average transaction $ amount by type
- Revenue/profit by payment type by quarter, number of payment transactions per DDA account by transaction type per month
- Payment volumes by type and by line of business (retail, small business, wholesale)
- Check processing trends of paper versus IRD, versus image exchange, and versus ARC clearing
- Profitability of card transactions by merchant, by SIC code by quarter, profitability of merchants by geographic region by quarter

Actions to Improve the Payments Business Bottom Line

The payments business is transforming. Consumer payment behaviors are changing. Consumers are writing fewer checks, instead they are paying bills online, transferring money from the U.S. to India, China, and Mexico, and expecting timely, visible, and low cost payments. Existing competitors, such as First Data Corporation, Western Union, and MoneyGram are getting stronger as the volume of electronic payments increases.

New competitors, such as Paypal and Walmart are emerging. Corporations are expecting intelligent, visible, and timely payments at a fair price – they are not expecting fees to make payments within their own corporation. After trying for years to get a full-service bank, Walmart scaled back its ambitions last summer and asked regulators for permission to simply process electronic payments. The goal is to save money by cutting out third-party payment processors.

Payments Business Intelligence is an Integral Part of an Enterprise Payments Strategy



"Payment hubs are the first step in the evolution of the banking payment business."

Source: Gartner, March 2006

Regulations are changing the payments landscape and the payment mix is impacting revenues. Debit card transactions are replacing checks and putting non-sufficient funds fees from checks at risk of declining. Check 21 permits checks to be processed as images, and ARC allows checks to be converted to ACH, changing the cost dynamics. SEPA requires fees for domestic and international payments within the Eurozone to be the same.

One thing is clear: if banks do not make the right decisions to adapt to the transforming payments market, the payments business mainstay of their revenue and profits will be a risk. So what is a bank to do? As described in this paper, a critical first step is to implement a payments data warehouse across the enterprise and create business intelligence reports and analytics that provide continuous visibility into the payments business.

In addition to implementing a robust, enterprise-wide payments warehouse with business intelligence to guide informed payments business decisions, banks must adapt the organization and processes to respond to the transforming payments markets. Some recommendations include:

- Charter and empower an enterprise-wide payments steering committee with CEO sponsorship
- Adjust internal accounting, payment product siloed organizations, and compensation structure to support an enterprise payments business
- Begin consolidating infrastructure, process, and labor redundancies across payment silos
- Design and evolve your payment infrastructure around a hub based on a business component architecture, including services and events
- Expose the newfound visibility of payments processing to customers for payment tracking
- Make payment fees transparent to customers and commensurate with the cost and value of the service

Unisys and Oracle Payments Business Intelligence Accelerator

The Unisys and Oracle Payments Business Intelligence Accelerator provides business analytics based on a payments data warehouse. The solution enables consolidation of customer and payments data from multiple sources including payment transactions, customer information, cost and revenue data. The data warehouse supports reporting and analysis for payment business performance, customer profitability, and risk management. Pre-defined business intelligence reports, and tools to easily produce additional reports and analytics, are included with the solution. The benefit gained from Unisys and Oracle Payments Business Intelligence Accelerator is greater insight into your payments business to enable business decisions that drive revenue growth as well as improved business agility, lower costs, and reduced risk and liability.

The payments business intelligence reports and analytics should be available at any point in time and should operate on a holistic and up-to-date view of all of the payments data.

EXPORT-IMPORT BANK OF THE UNITED STATES

The Export-Import Bank of the United States (Ex-Im Bank) is the official export credit agency of the United States. Ex-Im Bank's mission is to assist in financing the export of U.S. goods and services to international markets. Ex-Im Bank provides U.S. exporters and lenders with a variety of short-term (generally up to 180 days) export credit insurance policies, allowing them to extend credit terms to international buyers with minimal risk. This is often more cost effective than bank financing or letters of credit.

The Export-Import Bank of the United States (Ex-Im Bank) now offers financing support in the short-and medium-term to the private sector in Pakistan, in addition to being fully available for short-, medium- and long-term transactions in the public sector. Under project financing structures, lenders depend on the proceeds from the project for repayment and do not rely on recourse to foreign governments, financial institutions or established corporations. Ex-Im Bank's Project Finance Program helps U.S. exporters compete in new international growth industries such as private power, telecommunications and other infrastructure sectors. Ex-Im Bank enables the U.S. exporter to offer a more attractive comprehensive financing package to purchasers.

PAKISTAN

BANKING INFORMATION TECHNOLOGY
MODERNIZATION REVERSE TRADE MISSION

FEBRUARY 4 - 13 • 2013

WASHINGTON DC • NEW YORK • CALIFORNIA

BANKING INDUSTRY TECHNOLOGY SECRETARIAT (BITS)

The Financial Services Roundtable represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Roundtable member companies provide fuel for America's economic engine, accounting directly for $92.7 trillion in managed assets, $1.2 trillion in revenue, and 2.3 million jobs. The Banking Industry Technology Secretariat (BITS), the Roundtable's technology policy division, addresses issues at the intersection of financial services, technology and public policy, where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. BITS works to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions.

BITS provides intellectual capital and addresses emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. The organization also facilitates cooperation between the financial services industry and other sectors of the nation's critical infrastructure, government organizations, industry associations and technology providers to identify problems and develop solutions.

The BITS Software Assurance Framework represents a set of common practices within financial services firms to improve software security for customer- and employee-facing applications. This framework leverages the maturity of software assurance controls that were adopted by financial services firms in recent years and is intended to provide guidance and serve as a reference tool for financial services firms interested in improving software security controls and practices.

BITS

FINANCIAL SERVICES
ROUNDTABLE

BITS Projects

FRAUD

- Mortgage Fraud Reduction
- Payment Card Fraud
- Prepaid Access Card Fraud
- Remote Channel Fraud

REGULATION

- Various regulatory issues

SECURITY

- Cloud Computing
- Cyber Operational Resiliency Review (CORR)
- Email Security
- Malware Reduction
- Mobile Financial Services Security Assessment
- Security Awareness and Education
- Social Media

SPECIAL INTEREST GROUPS

- Cybersecurity Legislation
- Data Governance and Quality
- Mobile Financial Services
- R&D
- Vendor Management

THE FINANCIAL SERVICES ROUNDTABLE
Financing America's Economy

BITS
FINANCIAL SERVICES ROUNDTABLE

ROUNDTABLE MEMBER COMPANIES

COMPANY	CITY
Allianz Life Insurance Company of North America	Minneapolis, MN
The Allstate Corporation	Northbrook, IL
Ally Financial Inc. (GMAC)	Detroit, MI
American Express Company	New York, NY
American Honda Finance Corporation	Torrance, CA
Ameriprise Financial, Inc.	Minneapolis, MN
Ares Capital Corporation (Allied Capital)	New York, NY
Associated Banc-Corp	Green Bay, WI
Assurant, Inc.	New York, NY
Aviva USA	West Des Moines, IA
AXA Financial, Inc.	New York, NY
BancorpSouth, Inc.	Tupelo, MS
BancWest Corporation (First Hawaiian Bank)	Honolulu, HI
Bank of America Corporation	Charlotte, NC
Bank of Hawaii Corporation	Honolulu, HI
Barclays	New York, NY
BB&T Corporation	Winston-Salem, NC
BBVA Compass	Birmingham, AL
BlackRock, Inc.	New York, NY
BMO Financial Corp.	Chicago, IL
BNY Mellon Corporation	New York, NY
Brown & Brown Insurance	Daytona Beach, FL
Capital One Financial Corporation	McLean, VA
Caterpillar Financial Services Corporation	Nashville, TN
The Charles Schwab Corporation	San Francisco, CA
The Chubb Corporation	Warren, NJ
CIT Group, Inc.	New York, NY
Citigroup Inc.	New York, NY
City National Corporation	Los Angeles, CA
Comerica Incorporated	Dallas, TX
Commerce Bancshares, Inc.	Kansas City, MO
Discover Financial Services	Riverwoods, IL
E*TRADE Financial Corporation	New York, NY
Edward Jones	St. Louis, MO
Fidelity Investments	Boston, MA
Fifth Third Bancorp	Cincinnati, OH
First Horizon National Corporation	Omaha, NE
First Niagara Financial Group, Inc.	Buffalo, NY
First Republic Bank	San Francisco, CA
Ford Motor Credit Company	Dearborn, MI
Fulton Financial Corporation	Lancaster, PA
General Electric Company	Norfolk, VA
Genworth Financial	Richmond, VA
Hancock Holding Company (Whitney Holding Corporation)	Gulfport, MS

COMPANY	CITY
The Hanover Insurance Group, Inc.	Worcester, MA
The Hartford	Hartford, CT
HSBC USA, Inc.	New York, NY
Huntington Bancshares Incorporated	Columbus, OH
IBERIABANK Corporation	Lafayettte, LA
ING U.S.	Atlanta, GA
John Deere Financial Services, Inc.	Johnston, IA
John Hancock Financial Services, Inc.	Boston, MA
JPMorgan Chase & Co.	New York, NY
KeyCorp	Cleveland, OH
Liberty Mutual Holding Company, Inc.	Boston, MA
Lincoln National Corporation	Radnor, PA
LPL Financial	San Diego/Boston
M&T Bank Corporation	Buffalo, NY
MasterCard Worldwide	Purchase, NY
Mutual of Omaha Insurance Company	Omaha, NE
Nationwide	Columbus, OH
New York Life Insurance Company	New York, NY
Northern Trust Corporation	Chicago, IL
People's United Bank	Bridgeport, CT
The PNC Financial Services Group, Inc.	Pittsburgh, PA
Popular, Inc.	Hato Rey, PR
Principal Financial Group	Des Moines, IA
The Private Bank	Chicago, IL
Protective Life Corporation	Birmingham, AL
Prudential Financial, Inc.	Newark, NJ
Putnam Investments	Boston, MA
Raymond James Financial, Inc.	St. Petersburg, FL
RBC Capital Markets	New York, NY
RBS Americas (Citizens Financial Group)	Providence, RI
Regions Financial Corporation	Birmingham, AL
RenaissanceRe Holdings Ltd.	Pembroke, Bermuda
Sallie Mae, Inc.	Newark, DE
Sovereign (Banco Santander)	Boston, MA
State Farm Insurance Companies	Bloomington, IL
State Street Corporation	Boston, MA
SunTrust Banks, Inc.	Atlanta, GA
Swiss Reinsurance America Corporation	Zurich/Armonk, NY
Synovus	Columbus, GA
TD Bank	Portland, ME
Toyota Financial Services	Torrance, CA
Transamerica	Baltimore, MD
Trustmark Corporation	Jackson, MS
TSYS	Columbus, GA
Union Bank (Bank of Tokyo Mitsubishi, UFJ)	San Francisco, CA
United Bankshares, Inc.	Parkersburg, WV
Unum	Chattanooga, TN
U.S. Bancorp	Minneapolis, MN
Visa Inc.	San Francisco, CA

COMPANY	CITY
Webster Financial Corporation	Waterbury, CT
Wells Fargo & Company	San Francisco, CA
Western & Southern Financial Group	Cincinnati, OH
Zions Bancorporation	Salt Lake City, UT

*97 Roundtable Member Companies as of August 2, 2012.

FINANCIAL AFFILIATE ORGANIZATIONS

ORGANIZATION	CITY
American Bankers Association (ABA)	Washington, D.C.
Canadian Bankers Association (CBA)	Toronto, Canada
Canadian Payments Association (CPA)	Ottawa, Canada
Center for Information Policy Leadership (CIPL)	Washington, DC
Chilean Association of Banks and Financial Institutions (ABIF)	Vitacura, Chile
The Clearing House	New York, NY
Credit Union National Association (CUNA)	Washington, D.C.
The Depository Trust & Clearing Corporation (DTCC)	New York, NY
Early Warning Services	Scottsdale, AZ
East West Bank	Pasadena, CA
SWACHA	Dallas, TX
USAA	San Antonio, TX

*12 Financial Affiliate Members as of September 13, 2012.

INDUSTRY AFFILIATE ORGANIZATIONS

ORGANIZATION	CITY
Federal Reserve Bank of Boston	Boston, MA
Intuit	Mountain View, CA
Microsoft	Redmond, WA
Silver Tail Systems	Palo Alto, CA

*4 Industry Affiliate Members as of September 12, 2012.

MANDIANT CORPORATION

Mandiant offers enterprise and government organizations the critical intelligence, technology, products and services to fight today's advanced threats head-on. Mandiant's people and product approach to incident response differentiates the company from any other firm and has contributed to the company's dramatic growth over seven years. Mandiant's elite force of incident responders and forensic investigators bring to each breach investigation a unique blend of technical and investigative experience and offer leading incident response, malware analysis and incident response program development.

Mandiant is investing significantly in the delivery of next-generation threat detection and response through MCIRT, the Mandiant Computer Incident Response Team. MCIRT combines Mandiant's experience in advanced threat detection and response, exposure to diverse threat intelligence, revolutionary technology, and some of the best incident responders in the business. This combination provides customers with effective incident insight – from host to network – along with actionable intelligence.

The implementation of best practices to reduce response time and a return to normal business operations saves money, time and reputation damage. Mandiant customers are better prepared to tackle advanced threats and any resulting breaches through better intelligence sharing and effective execution of incident response and forensic best practices.

Mandiant offers a complete portfolio of vulnerability assessment services that allow organizations to identify critical security vulnerabilities that attackers could exploit. These services help organizations improve their existing security posture to reduce the risk of a successful attack.

MANDIANT

Mandiant Intelligent Response®

You've seen the headlines. Today's threat actors are savvy, sophisticated, and relentless. They target human vulnerabilities to slip through your preventive defenses. When they do, Mandiant Intelligent Response (MIR®) is the weapon that gives your team a decisive advantage over the adversary, revealing their every move and penetrating their attempts to stay hidden.

When attackers get through, Mandiant Intelligent Response® equips you to respond immediately and thoroughly to stop them before they complete their mission.

Mandiant Intelligent Response scales your most qualified security expert to investigate thousands of endpoints and scope the impact of an incident.

PRODUCT OVERVIEW

Are you compromised? How did the attacker get in? What systems are involved? Mandiant Intelligent Response lets you answer these questions so you can respond immediately and keep advanced attackers from achieving their objective in your systems.

Sweep Endpoints for Evidence of Compromise
Sweeps all of your endpoints for evidence of compromise including malware, general malware behaviors and non-malware attacker tactics.

Remotely Investigate Any Endpoint
Gets the data needed for investigation securely over the network, without having to wait for access to be granted or exposing administrative credentials to an attacker in control of a system. Collect images and full live response or ask for only the exact data you need.

Access Mandiant's Intel & Create Your Own
Utilizes Mandiant's latest Indicators of Compromise (IOC) library based on our experience on the front lines; you can create your own IOCs as well.

Triage Alerts With Automated Host Interrogation
Automatically collect info and analyze suspicious systems based on alerts generated by your SIEM, ticketing system or other applications.

HIGHLIGHTS

Unlike other host-based tools, Mandiant was specifically designed to detect and respond to advanced attacker activity.

- **Speed & Scale**
  Designed to rapidly sweep thousands of endpoints at once while other tools are optimized to deep dive one machine at a time.
- **Finds More Than Malware**
  Identifies attacker behavior in addition to malware so you can uncover what attackers are doing – not just their tools.
- **OpenIOC Support**
  Supports the XML-based OpenIOC standard so you can create, edit and share your own Indicators of Compromise.
- **Agent-Based Data Collection**
  Lightweight, non-intrusive agent enables remote data collection without impacting end user functionality.
- **Memory Forensics**
  Analyze live memory without downloading memory images to uncover malware that hides from normal tools.

Mandiant Intelligent Response®

As soon as you detect a compromise, MIR® allows your team to scale and rapidly investigate thousands of endpoints to determine what systems are compromised and what the attackers are after.

PRODUCT CAPABILITIES

The Mandiant Intelligent Response appliance finds evidence of compromise and forensic artifacts on your endpoints left behind by attacker activity. With MIR you can rapidly sweep tens of thousands of endpoints using Mandiant's latest intelligence about advanced attacker activity.

OpenIOC Support

- Investigate with your own custom indicators or with those shared by others using the OpenIOC standard.
- Access Mandiant's proprietary library of Indicators of Compromise (IOC) and develop your own custom indicators using the OpenIOC format.

Response-Focused Forensics

- Hybrid disk / memory forensics perform analysis impossible with conventional tools.

Targeted Data Acquisition at Scale

- Intelligent filtering capabilities in the agent return only the data you need.
- Find answers to forensic questions on thousands of hosts at a time.

Rapid Live Response

- Pre-deployed agents provide immediate, full remote forensic access to any system.
- On-host analysis enables full investigation over slow WAN links without waiting for memory or disk image downloads.

Integration With Other Products

- Works with Mandiant Redline™ to point users to the best-hidden malicious processes.
- Integrates with other detection systems to automate triage of hosts with suspicious activity.

HOW IT WORKS

MIR's "secret sauce" is the unique combination of Mandiant-based intelligence (gathered from all of our incident response consulting work done worldwide) and your own intelligence working together to search for evidence of compromise.

MIR agents are first deployed to all of your endpoints and are controlled via the Mandiant Console.

The MIR controller is armed initially with Mandiant Indicators of Compromise (IOCs) to do the initial sweep of every host in your environment.

Suspicious hosts are flagged for investigation and you are able to add your own IOCs and continue to sweep your entire environment in order to confirm the scope of the attack, identify all compromised hosts, and move quickly and effectively towards containment and remediation.

CASE STUDY

Mandiant Intelligent Response® Thwarts a Bank Heist

Event: A mid-size bank with over $1 billion in assets received two alerts of a potential problem on their network. The first alert was from a Federal law enforcement agency which had received a tip that the bank was targeted. The second alert came from customers who noticed irregular activity in their accounts.

Action: MIR was deployed, collecting data from over 550 systems in their enterprise within three hours.

Remediation: The bank was able to quickly determine which systems had been compromised, what data had been stolen, and even identify dormant malware left behind by the attackers. The information enabled the bank to ensure that the attackers were extricated from their enterprise and normal operations could resume.

MANDIANT®

Mandiant's products and services protect the world's most valuable data every day from targeted attacks. Our unique combination of intelligence, experience and technology equip organizations to detect, respond and contain attackers before they reach their objective.

TEL +1 (703) 683-3141 TOLL FREE (800) 647-7020 2318 MILL ROAD #500, ALEXANDRIA, VA 22314 WWW.MANDIANT.COM

MANDIANT

Vulnerability Assessments

Mandiant offers a full range of application and infrastructure vulnerability assessments designed to identify and evaluate security vulnerabilities and recommend risk mitigation strategies.

OVERVIEW

An enterprise must maintain a robust and attack-resilient infrastructure in order to successfully defend against cyber attacks. Mandiant offers a complete portfolio of vulnerability assessment services that allow organizations to identify critical security vulnerabilities that attackers could exploit. These services help organizations improve their existing security posture while reducing the risk of a successful attack.

MANDIANT'S APROACH

Mandiant's methodology and tools are adapted to suit each client's environment and objectives. Depending on the scope of the engagement, each application and infrastructure assessment can draw on a range of techniques that assess people, process, and technology:

People: Mandiant has utilized social engineering techniques including phone-based, USB drops and email phishing attacks to collect sensitive information such as user credentials, network information and passwords. Sometimes these activities involve spoofed web sites, help desk impersonations and implanting benign "malcode" that phones home.

Process: Mandiant has used a range of activities to identify policy and procedure deficiencies. This has included conducting compliance gap assessments against standards such as BS7799, ISO 27002, Sarbanes-Oxley and HIPAA. Mandiant has also conducted PCI audits and software development lifecycle assessments.

Technology: Mandiant has conducted penetration tests and performed assessments across all major platforms including mobile devices, virtualized environments, SCADA environments, cloud deployments and traditional enterprise applications.

Actionable Recommendations

Mandiant provides clients with actionable recommendations. All findings are rated based upon their risk, the probability of exploitation and the potential business impact. This allows clients to focus their efforts on addressing issues that matter the most.

THE MANDIANT DIFFERENCE

Real-World Experience
Mandiant consultants gather real-world attacker techniques observed during incident response engagements and continuously update the tools and methodologies so that they reflect the most current threat environment.

Client-Specific Assessments
Mandiant designs each assessment to meet the unique needs of each client. Assessments go well beyond commercially or publicly available vulnerability scanning tools. They mirror the tactics, techniques, and procedures attackers use as they attempt to gain access to the client's environments.

Knowledge of Attacker Tools
Mandiant has a dedicated team of malware reverse engineers that research the latest exploits and tools that attackers utilize. This research enables Mandiant to identify the vulnerabilities and weaknesses that attackers are most likely to exploit when penetrating a client's network.

Knowledge of Attack Groups
Mandiant has performed hundreds of investigations of successful attacks. Its consultants have extensive knowledge about the attack vectors used by advanced threat actors and how attacks can differ by threat actor.

Vulnerability Assessments

Mandiant offers a full range of application and infrastructure vulnerability assessments designed to identify and evaluate security vulnerabilities and recommend mitigation strategies.

ASESSMENT SERVICES

Mandiant has led hundreds of complex computer intrusion investigations and has amassed a wealth of information on how attackers breach organizations, what type of data they seek, and how they steal this data. Armed with this knowledge, Mandiant helps organizations of all sizes and across all industries improve their security posture and reduce the risk of a security incident.

Infrastructure Security

Mandiant has performed hundreds of external and internal infrastructure security assessments and identified thousands of critical vulnerabilities which exposed enterprises to external and internal attacks. Mandiant's services include:

- External network vulnerability assessments & penetration tests
- Internal network vulnerability assessments
- Network architecture reviews
- Device configuration reviews (host & network)
- Wireless security assessments
- VoIP security assessments
- Active directory reviews
- Social engineering and physical penetration tests
- Insider threat assessments
- Custom services as requested

Application Security

Testing applications at regular intervals, especially after important changes have been made to an application, is critical in order to maintain an attacker-resilient web presence. Mandiant has developed an extensive portfolio of application security assessments including:

- Web and client-server application security assessments
- Mobile application assessments
- Source code reviews for common programing languages
- Software development lifecycle (SDLC) reviews
- Application architecture assessments
- Custom services as requested

UNIQUE EXPERIENCE

Mandiant's specialized skills and experience have enabled it to identify and assess security vulnerabilities in some of the most complicated and mission critical environments:

- **Mobile Device Assessments**
  Mandiant has performed mobile device assessments for some of the largest telecommunication carriers in the world. This work has included handset reviews, mobile device web site assessments and data center compliance assessments for the infrastructure that supports third party applications running on carrier networks.
- **Web Applications**
  Mandiant has conducted reviews of large and complex custom web applications that consist of hundreds of dynamic pages and custom authentication mechanisms in highly fault tolerant configurations.
- **Social Engineering**
  Mandiant has performed social engineering engagements in which phishing emails have been sent to hundreds of client employees and encouraged to load modules onto their systems that report back to Mandiant servers. Mandiant has then summarized results for management to determine where the greatest need for security awareness education exists.
- **Security Policies**
  In one case Mandiant evaluated the incident response capabilities of a European country. This involved working with the National Police, Ministry of Justice, the National Forensics Bureau and the European Union to understand current capabilities, identify their needs and develop a plan for instituting more rigorous and modern tools, processes and practices.

MANDIANT

Mandiant's products and services protect the world's most valuable data every day from targeted attacks. Our unique combination of intelligence, experience and technology equips organizations to detect, respond and contain attackers before they reach their objective.

TEL +1 (703) 683-3141 TOLL FREE (800) 647-7020 WASHINGTON NEW YORK LOS ANGELES SAN FRANCISCO WWW.MANDIANT.COM

©2010 Mandiant Corporation. All rights reserved.

FEDERAL DEPOSIT INSURANCE CORPORATION

FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

The Federal Deposit Insurance Corporation (FDIC) is a Congress-created independent agency designed to maintain the stability and confidence in the nation's banking system. The agency does this by insuring consumer deposits and reviewing the soundness of financial institutions. The agency has many divisions such as IT, legal and supervision. The FDIC insures deposits of up to $250,000 per depositor, per insured bank, for each account ownership category at approximately 9,000 banks and savings associations nationwide. The two primary functions of the FDIC are to examine banks and resolve failures of banks/savings associations in the least costly manner. Both functions are dependent on data and analytics. The FDIC follows the guidance of the Government Paperwork Reduction Act, overarching federal e-government initiatives and the Clinger-Cohen Act. The latter act stipulates that all agencies adopt an IT architecture that enables business transformation. Since the FDIC was merged with the Resolution Trust Corporation in 1996, the number of employees was reduced from 23,000 to 4,700.

The FDIC spent seven years centralizing and rationalizing their infrastructure and applications. The agency was left with more than 360 stovepipe applications. These applications were optimized around workgroup needs, not enterprise business needs. Many applications also had their own stovepipe view of the data and that redundancy made data consistency and integrity an even greater challenge. Furthermore, many of these applications were developed by contractors or consultants who brought in their own architectures, databases, development methodologies and tools. This technical diversity increased complexity costs and made integration between applications difficult. The FDIC's initial enterprise architecture (EA) objectives were to streamline the IT environment and reduce the stovepipes so it could reduce costs and improve alignment.

The Structure Information Management System (SIMS) is the corporate database of the FDIC. SIMS maintains current and historical non-financial data for all institutions. The database also offers institution-specific demographic data, including a complete set of information on merger or consolidation transactions. All bank data is stored in a database known as the Corporate Business Information System (CBIS). This database is a registry of all U.S. banks with whom the FDIC is associated. CBIS is a repository for data collected from banks and other agencies. Consequently, the database knows how much money a bank has, including assets and number of operating branches. Another database, the Research Information Disk, mainly works with current statistics to predict future trends in order to make predictive forecasts. These databases are combined into one large database known as the Core Data Registry (CDR).

SQN Banking Systems

SQN Banking Systems was founded in 1983 and is headquartered in Rancocas, NJ. SQN claims to be the largest provider of signature verification and integrated check fraud prevention software for financial institutions of all sizes in the U.S. Their customer base of over 500 installations includes eight of the top ten U.S. banks and 70% of the top thirty U.S. banks.

SQN Banking Systems delivers innovative check fraud solutions that make large, mid-tier and community banks more competitive and more profitable. Browse our site to learn more about how SQN can assist your bank in detecting fraud with workflow, image fraud analysis, signature verification, transaction fraud analysis, official check verification, safe deposit management and conversion services.

SQN SENTRY Applications
Monitor - Finds potential deposit fraud by creating customer profiles and automatically comparing them with every deposit and other credit.

Detect - Finds potential check fraud by creating customer profiles and automatically comparing them with every "on-us" check.
Exception - Integrates check fraud suspects, signature comparison suspects, DDA exceptions, stop payment suspects, check images, signature images, and document images in an easy-to-use workflow that uses one screen.
SigCheck - Unique signature comparison engine that analyzes signatures and produces a confidence factor from 0 to 100.

Signature - Centralized database that stores and displays authorized signatures for your back office and branch operation. Online signatures can be used for a variety of applications such as signature verification and comparison, exception item processing, and batch file review.

Safe - PC based application that manages your entire safe deposit box operation. The database includes information unique to each authorized user, such as signature, photo, and payment status.
Batch Review - PC based application that works with leading check imaging systems to provide check images and authorized signatures for approval on one screen.

Don't let fraud affect your bottom line.

Check fraud continues to have a major impact on financial institutions. According to the Kobi Security Media Group, 65% of banks reported check fraud losses last year. You need solutions that help you find fraudulent checks before an item gets paid. Once the money is gone, it is much harder to recover.

Let SQN Banking Systems protect you.

SQN Banking Systems has been in the fraud prevention business since 1983. Our customers catch up to 91% of fraud attempts before suffering a loss. We offer a comprehensive line of powerful applications to combat check fraud and streamline payment processing operations. Each application can work independently or as part of a complete system that compares signatures, check images, behavioral patterns in deposits and credits, official checks and safe deposit management.

Take control of fraud with the protection you need.

For more than 25 years, SQN Banking Systems has provided the essential ingredients for integrated fraud detection and process improvement products for the financial industry. The SENTRY suite includes software designed to help you prevent fraud and offer a more secure environment for your customers. Take a look at the protection we can offer you.

WORKFLOW SOFTWARE Give your operations the opportunity to make critical pay/no pay decisions quickly and effectively. This software will help you make informed payment decisions and prevent fraud losses, and allow you to allocate resources as efficiently as possible.

IMAGE FRAUD ANALYSIS identifies potential fraud on check images with a powerful engine that automatically compares "on-us" check images to recognized data in customer profiles. The system can be used with various styles of check stock, check sizes and design types, as well as IRDs.

SIGNATURE VERIFICATION Automatically review signatures from incoming "on-us" checks to detect forgeries. Reduce check fraud and improve customer service by enabling bank personnel to visually compare signatures at the Teller Line and in the Back Office.

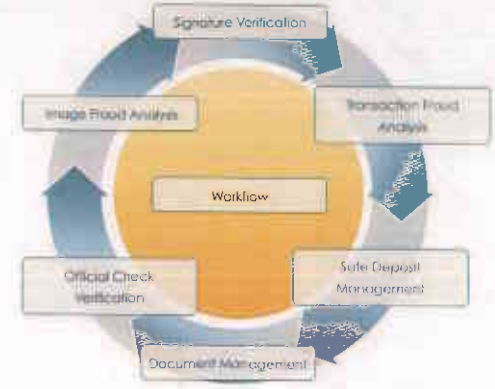
TRANSACTION FRAUD ANALYSIS Reduce your fraud risk by quickly identifying and placing holds on potentially fraudulent checks, credits and deposits before the item is paid. This system is scalable, customizable and parameter-driven, allowing for maximum flexibility in preventing check and deposit fraud.

OFFICIAL CHECK VERIFICATION Stop fraud before a check is cashed with instant validation at the Teller line or Back Office. SQN Banking Systems offers image-survivable security features printed directly on official and bank checks.

SAFE DEPOSIT MANAGEMENT Manage your entire safe deposit operation including customer signatures, photographs, rental agreements and billing information. A signature pad allows customers to sign in, documenting each visit. The system can print invoices and late notices or create a file for centralized billing.

DOCUMENT MANAGEMENT Electronically capture, store and manage every paper report, application file, and email in order to increase your organization's operational efficiencies.

CONVERSION SERVICES SQN Banking Systems can offer you a variety of proven, efficient ways to convert your data. Our expert staff has the skills and resources to quickly convert your paper-based signatures and other documents into an electronic format.



Get to know SQN Banking Systems.

In 1983 SQN revolutionized check fraud detection with the introduction of the first PC-based signature verification system. Since then, we've developed a comprehensive line of software products crucial to overcoming the growing problem of check fraud losses. And in an increasingly competitive banking world, we're helping our clients stay ahead of the curve with exceptionally efficient process improvement software.

SQN Banking Systems delivers innovative solutions that make large, mid-tier and community banks more competitive and more profitable – and ultimately, more secure against fraud.

SQN Banking Systems

ORACLE®

ORACLE CORPORATION

Oracle Corporation is the world's leading supplier of software for information management, and the world's largest independent software company. With annual revenues of more than $14+ billion, the company offers its database, tools and application products, along with related consulting, education, and support services, in more than 145 countries around the world. Oracle is the first software company to develop and deploy 100 percent internet-enabled enterprise software across its entire product line: database, server, enterprise business applications, and application development and decision support tools. Oracle acquired PeopleSoft and Siebel companies and continues to deploy and support those product lines.

Oracle has broadened its offerings for the financial services industry with the acquisition of Sun, a leading provider of standards-based computing systems, service, and storage. Oracle's Sun solutions have helped financial institutions gain operational flexibility and scalability, and improve service levels for many years. Banks around the world rely on Oracle to help them streamline business processes, meet increasing regulatory compliance demands, and improve cost efficiency, while providing greater value to customers. Now, with the combined strengths of Oracle Financial Services, Oracle E-Business Suite, Siebel, and PeopleSoft, Oracle PartnerNetwork provides the broadest functionality for helping banks securely grow their businesses and optimize performance.

Hardware and Software
Engineered to Work Together

Oracle Financial Services Analytical Applications

Features and Benefits

Features

- Industry-leading analytical methods
- Integration of risk, performance management, customer insight, and financial compliance
- Shared data model and applications architecture
- Enterprise class scalability

Benefits

- Actively incorporate risk into decision making
- Achieve a consistent view of performance
- Promote a transparent risk management culture
- Deliver actionable customer, business line, and product profitability insight
- Deliver pervasive intelligence

In today's turbulent markets, financial institutions require a better understanding of their risk-return, while strengthening competitive advantage and enhancing long-term customer value. Oracle Financial Services Analytical Applications enable financial institutions to measure and meet risk adjusted performance objectives, cultivate a risk management culture through transparency, lower the costs of compliance and regulation, and improve insight into customer behavior.

Enterprise Performance Management

To help financial institutions grow, manage risk, and optimize shareholder value, Oracle delivers a comprehensive, integrated suite of financial services analytical applications for enterprise performance management, including profitability management, funds transfer pricing, pricing management, and balance sheet planning. Now more than ever, financial institutions, their regulators, and shareholders are focused on the need to measure and meet risk-adjusted performance objectives, price products to reflect their true risk, and better understand how the institution is impacted by threats to liquidity, capital adequacy, and exposure to market rate volatility.

Enterprise Risk Management

Enterprise risk management solutions span all areas of risk, including credit, market, operational, liquidity, fixed asset, business and reputation risk, enabling institutions to manage all their risk and provide necessary feeds for compliance-based reporting. The capabilities of Oracle Financial Services for risk management help financial institutions address compliance issues such as Basel II that demand a close operational synergy between finance and risk functions.

Financial Crime and Compliance Management

Oracle Financial Services for Financial Crime and Compliance Management surrounds both the risk and compliance "point" solutions. It provides an end-to-end financial crime and compliance solution that leverages a comprehensive data model and robust dashboard functionality. The framework facilitates a transparent view of all crime and compliance related activities across the enterprise, allowing senior management to identify and mitigate any operational inefficiencies that might potentially increase noncompliance risks or the overall cost of compliance.

Related Products

- Oracle Financial Services Funds Transfer Pricing
- Oracle Financial Services Pricing Management, Funds Transfer Pricing Component
- Oracle Financial Services Profitability Management
- Oracle Financial Services Profitability Analytics
- Oracle Financial Services Balance Sheet Planning
- Oracle Financial Services Asset Liability Management
- Oracle Financial Services Analytical Applications Infrastructure
- Oracle Financial Services Basel II
- Oracle Financial Services ICAAP
- Oracle Financial Services Operational Risk
- Oracle Financial Anti-Money Laundering
- Oracle Financial Services Fraud

Customer Insight

Evaluating customer value is becoming tougher. Customer relationships are becoming more complex, involving several bank personnel, and have extended time periods. Increasingly, banks are customizing and personalizing products and services. While decisions are becoming riskier, time windows available for decision and action are becoming smaller. Such real-world scenarios mandate timely and comprehensive decision support. Oracle's Customer Insight solutions deliver targeted and actionable customer analysis that help financial institutions make quick decisions in a rapidly evolving marketplace.

Integrated Business Intelligence

Oracle's Financial Services Analytical Applications have corresponding Business Intelligence applications that deliver pre-packaged reporting, dashboarding and analysis capabilities, pre-integrated with the underlying applications. Role-based content is delivered across the enterprise at a significantly low cost of ownership. These applications leverage Oracle Business Intelligence Enterprise Edition (OBIEE), Oracle's market-leading BI platform. OBIEE provides a common reporting and analysis interface across the entire suite.

Integrated and Best of Breed

Oracle's next generation suite of Financial Services Analytical Applications is based on the merged capabilities of Oracle Financial Services Applications (OFSA), PeopleSoft Enterprise Performance Management (EPM), and Hyperion applications. The applications are built upon a shared analytical infrastructure consisting of a unified financial services data model, shared analytical computations and the industry-leading Oracle Business Intelligence platform, thereby ensuring consistency and an increased ROI by efficiently re-using components across applications. Additional solution components can be added without the significant cost associated with stand-alone applications.

Summary

In these uncertain times, the financial services industry will continue to be fiercely competitive, highly regulated, and more scrutinized than ever. Having the proper information available to make the right decisions that align with the business is now more important than ever. Oracle has led the marketplace for financial services analytical applications for over fifteen years, because of its comprehensiveness, scale, technology foundation, and industry insight. We remain committed to developing solutions that take advantage of advances in our technology leadership, and reflect the new challenges our customers face now and in the years to come.

CONTACT US

For more information, please call +1.800.ORACLE1 or visit www.oracle.com

ORACLE

Copyright © 2011 Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark licensed through X/Open Company, Ltd. 0611

Hardware and Software
Engineered to Work Together

Oracle Banking Platform

Enabling Transformation of Retail Banking

ORACLE

The banking industry is undergoing unprecedented change. Banks are challenged to enhance the customer experience while simultaneously reducing operational costs, better managing risk, and improving shareholder returns in a difficult regulatory climate.

To meet today's massive business change agenda, banks need modern and agile technology, but most are encumbered by aging systems that are rapidly approaching obsolescence. At a time when banks must transform their business models, they are also confronting the need to fundamentally transform their IT platforms.

Oracle Banking Platform has been designed to help banks progressively transform their business models by

- "Industrializing" business processes, driving productivity improvements across both front and back offices and reducing operating costs
- Enabling top-line revenue growth and new distribution strategies
- Moving customer centricity from an aspiration to a reality by putting the customer at the heart of the business model
- Enabling business innovation

"Industrializing" Banking

As both banks and customers simultaneously reduce risk, the net effect is a shrinking balance sheet and reduced income. When coupled with regulatory requirements to increase capital and reduce leverage, this places considerable downward pressure on returns. To adjust to this "new economics of banking," banks must re-engineer their operations to dramatically reduce costs.

Oracle Banking Platform enables banks to streamline and automate their business processes, enable back-office consolidation (for example, by creating "service hubs") and creative sourcing strategies (for example, by "in-sourcing" third-party servicing volumes), and reduce operating costs. Another key platform capability is role-based processing, which limits users' access to only those system functions required to fulfill their individual roles. This both addresses banks' needs to improve policy and process compliance and reduce the costs arising from exception management.

FACT: Oracle Banking Platform leverages the world's most successful applications footprint for banking, underpinned by industry leading Oracle Fusion Middleware to reduce IT complexity and total cost of technology ownership

"For us, the real advantage of Oracle Banking Platform is to have one platform, fully integrated, that is multichannel, multibrand, and multicurrency."

Gavin Slater
Group Executive
Group Business Services
National Australia Bank

Driving Top-Line Revenue Growth

To achieve acceptable returns on shareholder equity, banks must drive top-line revenue growth and generate more revenue from the existing cost base. Oracle Banking Platform has been designed to specifically enable revenue growth through

- "Multiproduct" origination capabilities that improve cross-selling effectiveness and result in an increase in products per customer
- Comprehensive pricing strategies that recognize the total value of the customer relationship
- Fee-based revenue optimization with fee waivers managed within delegation
- New distribution models that leverage Oracle Banking Platform's "multientity/ multibrand" architecture, enabling multiple brands to be supported within a single instance of the platform

Placing the Customer at the Heart of the Business Model

Customer centricity is something that every retail bank aspires to, but something that almost every bank falls short of achieving.

Breaking down silos and putting the customer at the heart of the business model is fundamental to delivering the customer experience that banks aspire to. Achieving this aspiration requires that banks put the customer at the heart of the IT architecture. Oracle Banking Platform exploits Oracle's world-class "customer hub" to incorporate customer relationship data into business process rules and fundamentally change the customer experience.

For example, in the traditional account-centric model, an insufficient-funds scenario typically results in the withdrawal being declined and a fee charged regardless of the value of the customer relationship. Oracle Banking Platform enables the bank to apply more-sophisticated treatment strategies. By creating a range of responses from highly automated to "high touch," the bank both recognizes customer relationship value and adheres to the bank's risk appetite, allowing the bank to optimize the outcome for both the customer and the bank.

Enabling Innovation

For many banks, the complexity of their business and IT architectures constrains innovation. Stories of taking 12 months or more to launch new products or make comparatively simple changes are commonplace. By leveraging a tier 1 banking platform architecture, Oracle Banking Platform enables business analysts to configure process

rules, product definitions, and a variety of other system parameters, enhancing business responsiveness and innovation. The paradigm shift from modifying code to configuring rules and parameters reduces IT effort and creates business agility.

Modern Banking Requires Modern Systems

With banks increasingly encumbered by complex, aging, and obsolete banking platforms, technology modernization is critical to future business success

For many banks, the problems are broadly the same:

- Highly efficient account processing platforms that are not easily modified for more customer-focused business models and distribution strategies
- Inability to deliver a consistent cross-channel customer experience, largely a consequence of different channels being implemented as discrete technology stacks with little commonality in architecture and design
- Protracted cycle times for implementation of new capabilities that affect new channel capability, new product development, or innovation in general
- Incredibly complex application portfolios that reflect years of best-of-breed purchase decisions at the component level and have resulted in massive integration complexity
- Limited or no practical upgrade paths for heavily customized vendor solutions and in-house developed legacy banking platforms

The decision to execute a technology modernization strategy is a decision to address fundamental issues in a bank's IT platforms, but with a view to enabling transformational business outcomes.

Oracle Banking Platform is a truly modern architecture that delivers

- The benefits of a 2010 design and the latest technological advances
- A native service-oriented architecture with key services externalized, enabling banks to either use Oracle's enterprise-class capabilities or integrate with their existing corporate systems leveraging world-class Oracle Fusion Middleware
- An enterprise-class security architecture covering bank staff, customers, and third parties
- A fully "multi-multi"-capable solution that supports multiple brands, entities, currencies, languages, and time zones within a single operating instance of the platform
- A platform designed and engineered for large bank scale, sophistication, and performance that reduces the bank's total cost of ownership of technology

"A key reason for choosing Oracle Banking Platform was the integrated stack, which over time will give us a very low total cost of ownership."

Christine Burdett
Executive Program Director
NextGen Program
National Australia Bank

Enabling Progressive Transformation

Oracle Banking Platform enables multiple sequencing options depending on individual banks' requirements. Most importantly, it enables banks to progressively transform their business and IT operating models by

- Addressing technology obsolescence risks
- Progressively enabling new business capabilities and realizing benefits
- Removing technology complexity and reducing the total cost of ownership of technology

Executing a complex transformational program can be expected to take a number of years and will need to be sequenced to reflect the bank's

- Short- and near-term priorities and longer-range business strategies
- Available options for unraveling existing business and technology complexity
- Ability to successfully execute, absorb change, and realize benefits

Oracle Banking Platform provides banks with the flexibility to address immediate issues while progressively realizing increased benefits from an expansive Oracle application footprint preintegrated by Oracle and engineered on a standard technology stack.

Oracle Banking Platform: Changing the Game in Banking

For decades, Oracle technology and applications have set the standard for enterprise information management—enabling modern businesses to do more, know more, and grow more quickly. Oracle provides the highest level of performance, business intelligence, flexibility, security, and scalability—at the lowest total cost of ownership.

With Oracle Banking Platform, banks get a comprehensive, preintegrated solution that enables them to take the complexity and cost out of technology and redirect investment from simply keeping the lights on to executing a strategic transformation of their business.

ORACLE
FINANCIAL SERVICES

INFORMATION CONNECTED

Comprehensive, Integrated Solutions for Islamic Banking

Oracle FLEXCUBE Islamic Banking

ORACLE

Grow Your Business with the Most Complete Solution for Islamic Banking

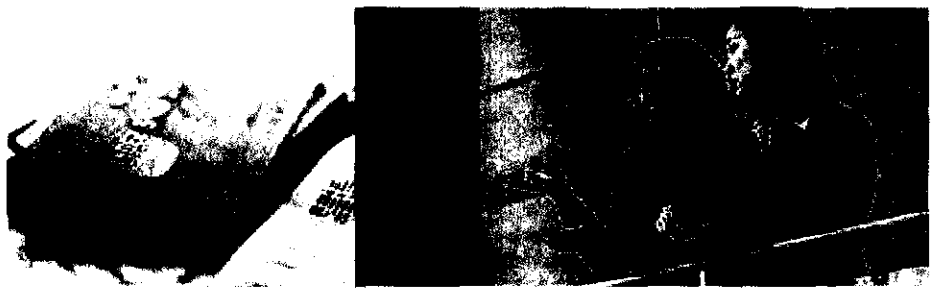
Today, your business depends on your ability to take advantage of new opportunities and introduce new products and services. Oracle FLEXCUBE Universal Banking helps you rapidly capitalize on the fast-growing Islamic financial market.

Across the world, banks and financial institutions are transforming themselves to address new market challenges and optimize their offerings for greater cost efficiency and profitability. Islamic banks are no different.

Forced to provide differentiated customer service, scale up operations to meet global competition, and grow market share to increase their customer base, Islamic banks are reinventing their business models. Added to this is the need to remain constantly compliant with Sharia law. Meanwhile, conventional banks are also making inroads into Islamic banking and expanding their offerings and reach. Consequently, Islamic banking is emerging as an alternative source of banking, and the products and services offered are fundamentally different from those of conventional banking. As Islamic banks grow, technology is increasingly becoming a key enabler for future business.

Oracle FLEXCUBE Islamic Banking, a comprehensive Sharia-compliant application, is a solution for both Islamic and conventional banks. It has been transforming the way banks operate for more than a decade and continues to remain the world's No. 1 choice for banking solutions.

Fact: Oracle FLEXCUBE's powerful product definition facility enables banks to extensively configure the lifecycle processing of financing transactions based on specific requirements.



Provide a Common Platform for Conventional and Islamic Banking

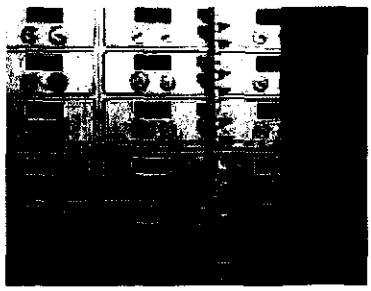
Business Benefits Delivered by Oracle FLEXCUBE Islamic Banking

- Enhance customer service by offering a wide range of Islamic products (Mudharaba, Qard, Mudarabah, Ijarah, Musharaka, Istisna, Salam, Tawarruq, and Sukuks).
- Expand your target customer base with the coexistence of Islamic and conventional banking on the same platform.
- Integrate with a comprehensive governance, risk, and compliance framework.

With more than 790 customers in more than 130 countries, Oracle's solutions are uniquely positioned to address the requirements of financial institutions around the globe. By implementing a comprehensive Islamic banking solution from its Oracle FLEXCUBE suite of products, you can offer both traditional and Islamic banking products to your customers, reducing the need to implement two different systems. Oracle FLEXCUBE Islamic Banking offers three distinct advantages:

- Islamic banks can leverage Oracle FLEXCUBE's proven infrastructure and finely tuned Islamic modules to offer Sharia-compliant products, support operations, and achieve fast implementation at reasonable costs.
- Existing Oracle FLEXCUBE customers can add new Islamic banking products using the same infrastructure, thereby lowering set up costs.
- Banks can offer Islamic banking as a subsidiary, letting Oracle FLEXCUBE manage the Islamic products while the existing core banking system manages its conventional products.

In addition, it is fully compliant with Sharia laws and regulatory requirements such as Basel II and Anti-Money Laundering, allowing banks to ensure corporate governance and reduce risks. A highly parameterized solution, Oracle FLEXCUBE Islamic Banking helps you launch new products faster and rapidly roll them out for additional users and branches, eliminating growth-related bottlenecks. With processing available 24/7, it offers the highest levels of availability and scalability, supporting consistent growth in both the number of users and the number of transactions performed.



Ensure Process-Centric Implementation

Oracle's solutions offer a process-driven product development methodology for financial services institutions based on its process framework for banking, a process repository for transforming banking operations. Specifically, the Oracle solution approach ensures

- **Business process support.** Includes configurable parameters, business process rules, workflows, and multiple deployment options.
- **Interoperability.** Supports open standards, enables reuse, blends into the existing application landscape, and minimizes disruption on switchover.
- **Extensibility.** Allows the application to be accessible anywhere and extendable outside the enterprise, and provides a platform for enhancement.
- **Standardization.** Offers out-of-the-box functionality, embedded support for analytics and reporting, and master data management.

Sharia-Compliant Financial Instruments

Oracle FLEXCUBE Islamic Banking supports the following nine instruments:

- Murabaha
- Qard
- Mudarabah
- Ijarah
- Musharaka
- Istisna
- Salam
- Tawarruq
- Sukuks

Support Sharia-Compliant Financial Instruments

Given the strict prohibition against interest, financial services institutions need to construct different kinds of financial products in order to comply with the Sharia law and follow Islamic financing principles.

Murabaha

Murabaha is a sale with an agreed-upon profit margin. Oracle FLEXCUBE Islamic Banking supports a variety of Murabaha transaction types, which a bank may adopt for its retail and corporate customers.

Qard

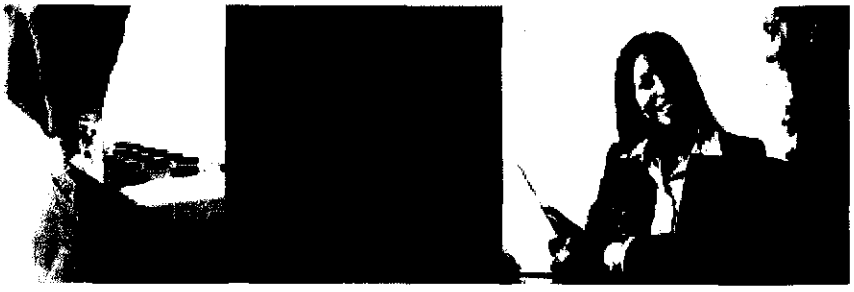
Oracle FLEXCUBE Islamic Banking supports Qard, which are loans without profit. The borrower
is required to repay only the principal amount borrowed but may pay an extra amount as a token of appreciation at the borrower's absolute discretion. Qard contracts can also be used to support current accounts, in which customers lend the money to the bank. The bank generates profit on this loan and returns the capital and some of the profit it has obtained.

Mudarabah

In Mudarabah, the customer provides funds to the bank, which then invests the funds into various investment schemes and financing. Oracle FLEXCUBE Islamic Banking supports a funds-based as well as a pool-based approach for Mudarabah transactions.

Ijarah

Ijarah is a concept closest to the conventional idea of leasing. Oracle FLEXCUBE Islamic Banking supports the complere lifecycle processing for Ijarah financing transactions. This includes payments processing for asset acquisition, rental calcularion and payments, arrears processing, and sale of the asset at the end of the contract period (in the case of Ijarah wa iqtina).



Fact: Oracle FLEXCUBE Islamic Banking is a comprehensive, integrated, and fully Sharia-compliant solution for Islamic banks.

Musharaka (Investment)

Musharaka means "to share." In a banking context, it indicates that all profits or losses are shared equally. The securities module of Oracle FLEXCUBE Islamic Banking enables comprehensive back-office processing for Musharaka investments.

Istisna

Oracle FLEXCUBE Islamic Banking also supports Istisna. In an Istisna sale, the buyer asks the manufacturer to create a specific commodity with material from the manufacturer. The price is fixed after all parties give their consent and agree on all the necessary specifications of the commodity.

Salam

Salam is a sale in which the seller supplies specific goods to the buyer at a future date in exchange for a price fully paid in advance. It is typically used to finance agriculture. The bank must take delivery of the commodity on maturity and it can enter into a parallel contract of Salam with another party to sell the commodity on the future date. (It is prohibited to sell the commodity to the original party.)

Tawarruq

Tawarruq is a finance method with which one can raise loan financing through buying installments in a local commodity owned by the bank. Applicants then authorize the bank to sell their share in this commodity, on their behalf, to a third party for cash and then deposit the proceeds into his account.

Sukuks

Sukuks are Islamic bonds that must be linked to an underlying asset. Banks cannot raise funds by issuing generic fixed or floating coupon-bearing bonds. Banks can securitize a stream of cash flows from Ijarahs or Murabahas and then issue Sukuks. The coupon cash flow for these Sukuks can be the cash flow from the underlying Ijarahs or Murabahas, for example.

Scale Your Business with a Modular, Service-Based Functional Architecture

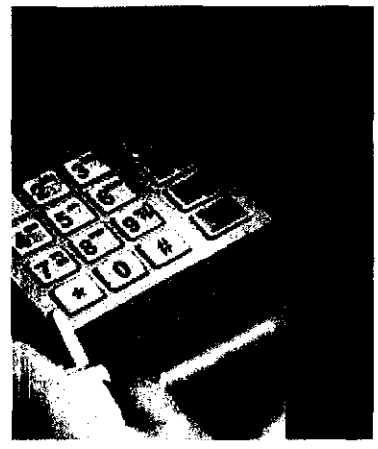
Core banking systems are mission-critical systems that process transactions, track securities positions, and clear payments. A modular architecture such as service-oriented architecture (SOA) will help replace modules from a legacy system selectively on an evolutionary basis, allowing you to take advantage of best-of-breed solutions. The Oracle FLEXCUBE solution portfolio rests on SOA, furthering interoperability, extensibility, and standardization.

Business Modules

<table>
<tr><th colspan="2">Retail / Corporate</th><th>Payments</th><th>Treasury</th><th>Transfer Agency and Fund Accounting</th></tr>
<tr><td>Mudarabah Deposits</td><td>Business
Bills and Collections</td><td>Cross Border Funds Transfer</td><td>Murabaha Money Market</td><td rowspan="2">Investor Services</td></tr>
<tr><td>Consumer Murabaha</td><td>Modules
Letters of Credit and Guarantees</td><td>Local Payments</td><td>Foreign Exchange</td></tr>
<tr><td>Ijarah Financing</td><td>Self-Service Modules
Qard</td><td>Direct Debits</td><td>Securities (Musharaka Investments and Sukuks)</td><td>Mudarabah Asset Management</td></tr>
</table>

<table>
<tr><th colspan="5">Support Services</th></tr>
<tr><td>Expense Processing</td><td>Electronic Messaging System</td><td>Fixed Asset Management</td><td>Nostro Reconciliation</td><td>Cost Allocations</td></tr>
</table>

<table>
<tr><th colspan="4">Core Services</th></tr>
<tr><td>Clearing</td><td>General Ledger</td><td>Limits and Collaterals</td><td>Reporting Systems</td></tr>
<tr><td colspan="2">Management Information and Systems</td><td>Security and Access Control</td><td>Customer Information</td></tr>
</table>



Oracle FLEXCUBE Islamic Banking provides a modular, service-based architecture, allowing you to choose only those modules that suit your needs. Oracle FLEXCUBE's powerful product definition facility enables banks to extensively configure the lifecycle processing of financing transactions based on specific requirements. As operations and business needs grow, they can add new modules without disturbing existing ones. Additionally, as a single integrated solution, Oracle FLEXCUBE Islamic Banking offers a consolidated view of customer relationships, risk management, profitability tracking, and accounting.

Oracle FLEXCUBE Islamic Banking comprises the business modules shown on the previous page. Additionally, some key areas supported by Oracle FLEXCUBE Islamic Banking include

- **Multifund subscription.** The asset management module for Oracle FLEXCUBE Islamic Banking supports multifund subscription. This feature allows customers to subscribe to multiple funds from one computer screen or invest in a fund from any bank branch.

- **Weighted average contributions.** The Oracle FLEXCUBE core module for Islamic banking supports weighted average contributions of depositors. It computes the total profit made by the pool and deducts the management fee and reserves, if any. The remaining profit is allocated to depositors based on their weighted average contribution to the pool.

- **Commodity tracking.** The Oracle FLEXCUBE money market Murabaha module supports tracking of commodities, receipts, and overdue payments. A loan is initiated in receipt of a commodity, with an automatic rule-based status classification facility.

- **Financing assets under construction.** With Oracle FLEXCUBE, a bank can finance assets under construction, define grace periods for suppliers and customers, and support multiple disbursements and collection of installments after the construction period.

- **Grace period disbursement.** Oracle FLEXCUBE supports pre-equated monthly installments loans in which the customer has a grace period before the amortized schedules. It allows disbursement of loans in the grace period, with interest calculated only for this period.

NEW YORK STOCK EXCHANGE (NYSE)

The New York Stock Exchange (NYSE) has developed the next generation of surveillance software for managing Broker Dealers' and Exchanges' risk in the rising regulatory environment. This solution can provide the Pakistani Delegation with a suitable starting framework from both a technology/methodology and industry vocabulary perspective. As the Radar service allows instant modifications in a fully hosted environment, the service affords clients to design a real-time system to their business needs, without incurring unnecessary costs.

NYSE's "Trade Exception Radar" is a real time post trade exception service which captures both structured and unstructured data for real time pattern analysis. As the service utilizes Natural Language Processing and Machine learning concepts, Radar can integrate with the following data sources:

- Global Exchanges (including non NYSE affiliated exchanges)
- Alternative Trading Systems (ATS)
- Order Management Systems (OMS)
- Market Data sources
- News feeds and social media sources

Utilizing a low latency Complex Event Processor (industry's first real time streaming Hadoop engine) for data mining and pattern matching, Radar sends real time alerts and exceptions to the user interface (Analyst Workstation).

NYSE Technologies provides comprehensive transaction, data and infrastructure services and managed solutions for buy-side, sell-side and exchange communities that require next-generation performance and expertise for mission critical and value-added client services. This division operates four units: the Global Connectivity unit, offering one of the world's largest, most reliable financial transaction networks connecting firms and exchanges worldwide; the Trading Solutions unit, which creates and implements high performance, end-to-end messaging software and real-time market data distribution and integration products; the Exchange Solutions unit, which provides multi-asset exchange platform services, managed services and expert consultancy; and the Global Market Data unit, which offers a broad array of global market information products covering multiple asset classes. With offices across the U.S., Europe, and Asia, NYSE Technologies' advanced integrated solutions for a wide range of services has earned the ability to power the trading operations of global financial institutions and exchanges.

NYSE Technologies was founded on the basis of multifaceted security that is in accordance with industry standards and compliance. The management of both virtual and physical environments is made possible by strict governance, risk management and compliance policies, developed and implemented by IT Asset Management (ITAM). All security measures for the physical data center and virtual liquidity network were created in direct adherence with the highest industry standards such as ISO 27002 and the Cloud Security Alliance.

The company's approach to secure cloud computing utilizes a defense-in-depth design strategy, while embedding security into each layer of the network, application, system, database and storage. Given that technology is only as effective as its ease of use, NYSE Technologies includes a convenient single sign-on portal so that an end-user can seamlessly log in with while simultaneously mitigating risk of unauthorized access.

NYSE Technologies Trade Exception Radar

Product Overview

The Radar contains (but is not limited to) the following functionality:

Surveillance Analyst Workstation ("SAW")

Real Time Exception Alerts, including:

- Odd Lot Trade Verification
- Wash Trade Verification
- Duplicate Order Verification
- Short Sell Validation
- Order Limits (defined by firm)
- Mix lot
- Ability to add/edit/remove exception alerts

Real Time Trade Data Querying, including:

- Trader ID
- Symbol
- Side
- Account
- Computer ID
- Message ID
- Execution Venue
- Client Order ID
- Quantity
- Price
- Start Date
- End Date
- Column chooser for non FIX formatted trade format

Report Designer:

- Customer created reports from incoming message data
- Editing and saving of reports created in report designer
- Ability to incorporate trade message data from any OMS and flat files

Entitlement Features:

- Customer will get three roles defined as: Administrator, Analyst, Supervisor
- Entitlement changes are available at client's request
- Customer will be allowed to escalate an exception to the supervisor role

Additional Services

Connectivity and Market Data:

- User will gain access to SAW via web URL
- Customer will specify to NYSE Technologies the method of transaction data loading into SAW (during on boarding process)
- Market Data to be provided by NYSET's Superfeed services
- Additional market data sources can be available and will be scoped during use case analysis

Exception Workflow Management:

- Users can use case management procedures on all incoming and historic exception alerts
- Audit trail of exceptions and case management saved for the life of the service
- Additional entitlements creation for encapsulation of visibility

Data Storage

- Allows users to have immediate access for all incoming data for six to twelve calendar months
- All incoming order and execution data to be saved in long term storage for seven years (meeting SEC 17a-4 requirements)

Regulatory Reporting

- Managed Service of complete OATS submissions
- All rejects or failures resolved and submitted on client's behalf
- End of day snapshot to client confirming OATS submissions and summary of failure/reject corrections and re-submissions
- All Reg-NMS reports available at client's request

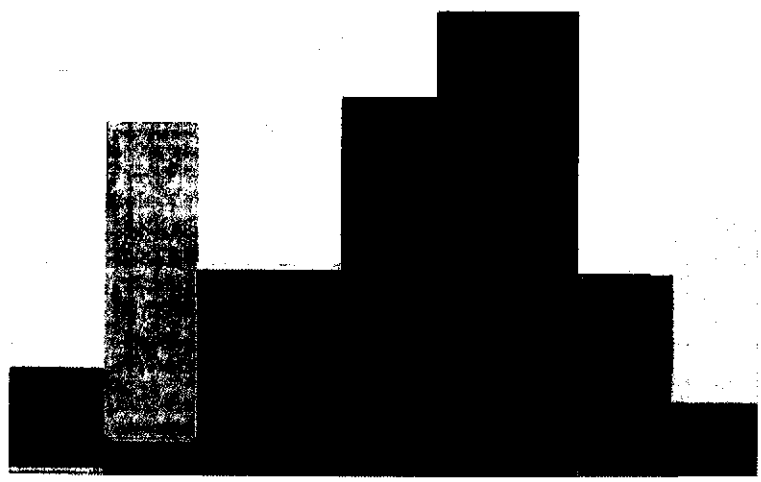
Architecture Flexibility

- Data pattern matching of 200,000 messages sustained
- Underlying complex event processing technology for horizontal scaling (pattern matching speeds can be increased at client's request)

For more information about Trade Exception Radar, please contact Karthik Shanmugham, Managing Director, Global Platform Services at 212.510.6680 or kshanmugham@nyx.com.

NYSE TECHNOLOGIES.

NYSE TECHNOLOGIES:
TRADE EXCEPTION RADAR
FREQUENTLY ASKED QUESTIONS



CONTENTS

1. OVERVIEW 2

2. REGULATORY REPORTING (OATS AND 606) 3

2.1 Can A Cleint view the individual order details of the submitted files as they were submitted to OATS? 3

2.2 Can repairs, mass repairs and resubmits be performed through the tool? 3

2.3 Can files from multiple sources be concatenated prior to submission, specifically with the same market Participant id (MPID)? 3

2.4 Where and for how long are the OATS files archived? 3

2.5 How are future changes withinin oats submission procedures handled? 3

2.6 How would the system determine the account type code (individual, institutional, error, etc.)? 3

2.7 Are individual client 606 reports available? What is the turnaround time? What's the process for ordering delivering? 3

2.8 High Level Diagram of OATS process: 4

3. ORDER FILE INQUIRES 5

3.1 What query parameters are available within the service? 5

3.2 What is the data availability and archive process? 5

3.3 Is the order data (capture and retrieval process) real time or next day? 5

3.4 Is execution data real time? 5

4. SURVEILLANCE 7

4.1 For purposes of customer account surveillance (e.g. cross trade, marking the close) can the system incorporate customer account information such as: 7

5. DATA 8

5.1 Does the product require any customer data other than the account number? 8

5.2 In general, what data must be sent to the hosted solution? 8

5.3 Does the service accept fractional shares? 8

5.4 How many years of history will the service keep? 8

6. RECONCILIATION 9

6.1 Is there a periodical reconciliation process? 9

7. MESSAGING 10

7.1 What connectivity configurations are utilized to send messages from the client to the service? 10

7.2 what processes ensure no messages are lost? 10

7.3 Does sequencing of trade information matter? 10

8. SECURITY 11

8.1 how is the user interface of the system launched? 11

8.2 How is authentication and authorization managed? 11

8.3 What is the general availability/failover policy for the service? 11

8.4 Hosting Services and Security 12

8.5 About the Mahwah Datacenter: 12

1. OVERVIEW

NYSE Technologies is pleased to present documentation on frequently asked questions regarding the Trade Exception Radar service. Materials specified within this document pertain to areas of the service regarding:

- Messaging and Data services
- Connectivity and Reconciliation
- Regulatory Reporting
- Exception Alerting

As the Trade Exception Radar is constructed as a framework service, modifications are possible for most instances. For further elaboration on any areas of the documentation, all questions can be posed to the direct sales account executive or nyse-technologies-sales@nyx.com

2. REGULATORY REPORTING (OATS AND 606)

2.1 CAN A CLEINT VIEW THE INDIVIDUAL ORDER DETAILS OF THE SUBMITTED FILES AS THEY WERE SUBMITTED TO OATS?

NYSE Technologies Response:
The regulatory features of the Trade Exception Radar Service (Hereinafter "Service") provide a fully managed OATS submission (of client's trade date) where results of the submission are sent to the client. Order details are specified within the end of day report sent to the client. If a client would like to submit OATS submissions, NYSE Technologies can distribute the OATS file to the client at end of day.

2.2 CAN REPAIRS, MASS REPAIRS AND RESUBMITS BE PERFORMED THROUGH THE TOOL?

NYSE Technologies Response:
OATS repairs for rejects are monitored and fixed by NYSE Technologies (and will not be present within the front-end graphical user interface). A report of daily repairs is sent to client within the end of day report.

2.3 CAN FILES FROM MULTIPLE SOURCES BE CONCATENATED PRIOR TO SUBMISSION, SPECIFICALLY WITH THE SAME MARKET PARTICIPANT ID (MPID)?

NYSE Technologies Response:
Files from multiple sources can be concatenated prior to submission for the OATS process (with sources with identical or various MPIDs).

2.4 WHERE AND FOR HOW LONG ARE THE OATS FILES ARCHIVED?

NYSE Technologies Response:
OATS reports are sent to the client within the end of day report (to be saved locally). In addition, these files can be saved within the fully hosted environment with NYSE Technologies Archive on Demand services.

2.5 HOW ARE FUTURE CHANGES WITHININ OATS SUBMISSION PROCEDURES HANDLED?

NYSE Technologies Response:
NYSE Technologies would handle all future changes to OATS reporting at no additional charge to the client.

2.6 HOW WOULD THE SYSTEM DETERMINE THE ACCOUNT TYPE CODE (INDIVIDUAL, INSTITUTIONAL, ERROR, ETC.)?

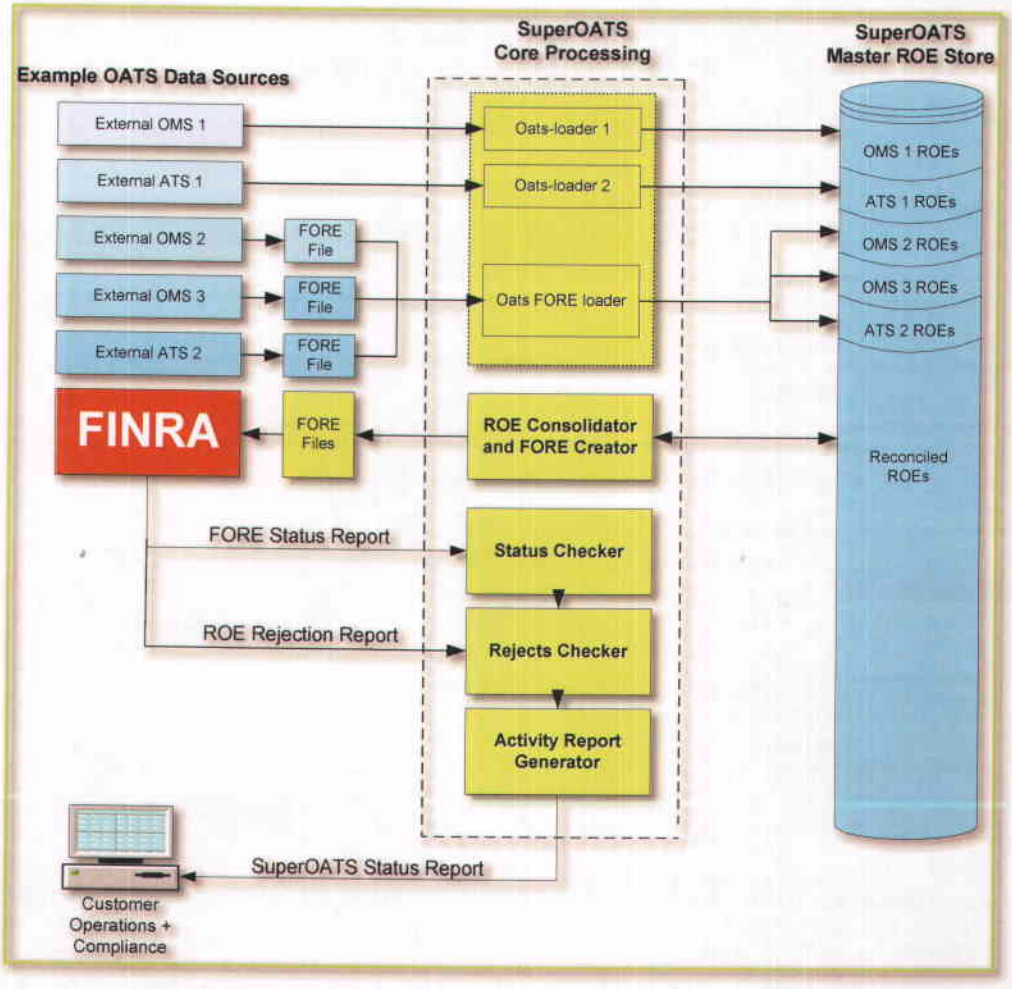
NYSE Technologies Response:
NYSE Technologies would utilize a list of account type codes (provided by client) to pre-configure.

2.7 ARE INDIVIDUAL CLIENT 606 REPORTS AVAILABLE? WHAT IS THE TURNAROUND TIME? WHAT'S THE PROCESS FOR ORDERING DELIVERING?

NYSE Technologies Response:

Creating specific queries for generating 606 reporting on a "client by client" basis can be created within the query and reporting interface within the Service. These reports can be scheduled (by the client) for any specified time period.

2.8 HIGH LEVEL DIAGRAM OF OATS PROCESS:



3. ORDER FILE INQUIRES

3.1 WHAT QUERY PARAMETERS ARE AVAILABLE WITHIN THE SERVICE?

NYSE Technologies Response:
The Service allows any parameter within incoming messages to be queried within the query interface. The column choosing functionality can be utilized for any order/execution messaging format.

3.2 WHAT IS THE DATA AVAILABILITY AND ARCHIVE PROCESS?

NYSE Technologies Response:
The Service's data storage lies within the following areas:

- Short Term Data Storage
  - Short Term Data storage is defined as all incoming data immediately available within the system
  - The duration of short term data can be defined by the client from the base standard amount (30 calendar days) up to years of live data

- Exception and Compliance Workflow Storage
  - Exception and compliance workflow data is defined as information pertaining to alerts raised by the system and actions taken by clients to remediate respective exception
  - Exception and compliance workflow data is stored within the system for the duration of the service
  - If the client leaves the Service, workflow and exception information can be sent to the client for local archiving (on client's data storage)

- Long Term Storage
  - Long term storage is defined as data that archived on a write once read multiple storage (WORM)
  - The long term storage solution's base offering is seven (7) years and can be expanded to the client's needs
  - The format of the data being archived is within the same format that was received (no normalization of the data)
  - The long term storage is designed to meet the SEC 17a-4 requirement for data storage

Please note: There is no differentiation between immediate data and historic data for querying and compliance workflow (pertaining to speed and format of information returned during query)

3.3 IS THE ORDER DATA (CAPTURE AND RETRIEVAL PROCESS) REAL TIME OR NEXT DAY?

NYSE Technologies Response:
The alerts' pattern matching functionality and querying tools can analyze incoming data in real time (metric specific information can be provided upon request).

3.4 IS EXECUTION DATA REAL TIME?

NYSE Technologies Response:

Similar to order data, alerts' pattern matching functionality and querying tools can analyze incoming data in real time (metric specific information can be provided upon request).

4. SURVEILLANCE

4.1 FOR PURPOSES OF CUSTOMER ACCOUNT SURVEILLANCE (E.G. CROSS TRADE, MARKING THE CLOSE) CAN THE SYSTEM INCORPORATE CUSTOMER ACCOUNT INFORMATION SUCH AS:

- *Customer id*
- *Household id*
- *Address*
- *Authorized trader*

NYSE Technologies Response:
The Service is a framework that allows customer information to be entered (or uploaded by client). Specific account information can be incorporated during technical use case discussion (and implemented during on-boarding phase of the Service). As for specific account information, the response is below:

- Customer id - **YES**
- Household id - **YES**
- Address - **YES**
- Authorized trader -**YES**

5. DATA

5.1 DOES THE PRODUCT REQUIRE ANY CUSTOMER DATA OTHER THAN THE ACCOUNT NUMBER?

NYSE Technologies Response:
For the surveillance interface of the Service, no other customer data is needed. If a client would like more customer integrated data (within the surveillance interface), this can be defined during a use case discussion. The regulatory reporting service would need pre defined parameters that will be specified during a technical discussion.

5.2 IN GENERAL, WHAT DATA MUST BE SENT TO THE HOSTED SOLUTION?

NYSE Technologies Response:
The surveillance interface is configurable where any trade events can be integrated. Moreover, different market data feeds can be utilized for exception alert notification. The regulatory reporting feature will need both order and execution data to submit OATS files to FINRA.

5.3 DOES THE SERVICE ACCEPT FRACTIONAL SHARES?

NYSE Technologies Response:
The service can accept fractional shares and will be provided upon request.

5.4 HOW MANY YEARS OF HISTORY WILL THE SERVICE KEEP?

NYSE Technologies Response:
As previously mentioned within this document:

- Short Term Data Storage
  - Short Term Data storage is defined as all incoming data immediately available within the system
  - The duration of short term data can be defined by the client from the base standard amount (30 calendar days) up to years of live data

- Exception and Compliance Workflow Storage
  - Exception and compliance workflow data is defined as information pertaining to alerts raised by the system and actions taken by clients to remediate respective exception
  - Exception and compliance workflow data is stored within the system for the duration of the service
  - If the client leaves the Service, workflow and exception information can be sent to the client for local archiving (on client's data storage)
- Long Term Storage
  - Long term storage is defined as data that archived on a write once read multiple storage (WORM)
  - The long term storage solution's base offering is seven (7) years and can be expanded to the client's needs

6. RECONCILIATION

6.1 IS THERE A PERIODICAL RECONCILIATION PROCESS?

NYSE Technologies Response:
NYSE Technologies will provide a client with a periodical reconciliation process. The frequency of reconciliation reports will be specified during technical use case discussions. The periodic reconciliation process will be specified within the service level agreements of a NYSE Technologies purchase order.

7. MESSAGING

7.1 WHAT CONNECTIVITY CONFIGURATIONS ARE UTILIZED TO SEND MESSAGES FROM THE CLIENT TO THE SERVICE?

NYSE Technologies Response:
The service will receive messages via drop copy session. While the service handles multiple message protocols, NYSE Technologies recommends a FIX protocol format (FIX 4.2 or other FIX formats).

7.2 WHAT PROCESSES ENSURE NO MESSAGES ARE LOST?

NYSE Technologies Response:
The guarantee of full message receipt within the service will be dependent upon message protocol of choice. If the message protocol is within the FIX format, the service will use standard FIX recovery methods. In addition, the reporting of any message loss will be displayed within the reconciliation report (and will be specified within the service level agreements of a NYSE Technologies purchase order).

7.3 DOES SEQUENCING OF TRADE INFORMATION MATTER?

NYSE Technologies Response:
For the surveillance interface, sequencing could matter (depending on the specific exception alert) and will be specified during a technical use case discussion. The regulatory reporting component is not dependent on any sequencing needs.

8. SECURITY

8.1 HOW IS THE USER INTERFACE OF THE SYSTEM LAUNCHED?

NYSE Technologies Response:
The service is a thick client which is hosted with NYSE Technologies' data centers. Users would access the service via CITRIX interface, where he or she can access the Service through a virtual desktop.

8.2 HOW IS AUTHENTICATION AND AUTHORIZATION MANAGED?

NYSE Technologies Response:
Authentication follows a defined process in accordance with information security and identification. The firm will submit a list of authorized users to NYSE Technologies. Users will be defined with varying levels of authorization and utilization capabilities within the GUI. Upon submission and precertification, Radar Graphic User Interface (GUI) logins will be requested and created. Certification requests will be submitted by NYSET on behalf of the new user. Active Directory accounts and automated passwords will be provided to the user. Users will have access to the CITRIX deployment and access to the Radar GUI. A client has complete discretion as to the addition or subtraction of users. Any changes to authorized accounts can be made upon request.

8.3 WHAT IS THE GENERAL AVAILABILITY/FAILOVER POLICY FOR THE SERVICE?

NYSE Technologies Response:
NYSET utilizes a Session Initiation Protocol (SIP) based fail over process, across dual data centers (Mahwah and Carlstadt data centers). Systems are monitored 24/7 (ITRS).

1. DC A: Primary Unix Server – (Active SIP) + Primary Oracle server (Active)
2. DC B: Secondary Unix Server – (Standby) + Secondary Oracle server (Standby)

The fail over process consists of moving the SIP from the primary to the secondary host. The process is managed using dual datacenter hosted AutoSys servers designated to the SIP. All data can be redirected and restarted with minimum interference. The fail over process is initiated manually and monitored.

The general availability of the service is 24 hours for seven days a week. The support levels for the product are as follows:

3-Tier Support Model:

Level 1 – Service Desk (24/6): Knowledgeable service desk trained to respond to 90% of client issues.

Level 2 – Product Experts (24/6): Technical personnel proficient with product intricacies for troubleshooting and analysis of system behavior.

Level 3 – Development Engineers (12/5): Responsible for identifying and resolving any bugs that may arise.

Communications of outages will be specified within service level agreements of a NYSE Technologies purchase order.

8.4 HOSTING SERVICES AND SECURITY

Similar to the NYSET Marketplace, the Trade Exception Radar service utilizes the speed and security of NYSET Secure Financial Transaction Infrastructure® (SFTI®).

The utilization of the SFTI network affords the benefits of:

- Providing a single point of connectivity with lowest-latency access to multiple markets.
- Unparalleled security and resiliency; specifically built for electronic trading and market data traffic.
- Ability to re-use clients' existing connectivity for additional market access and applications
- Access to numerous global execution venues, liquidity pools, market data vendors, clearing applications and other financial service providers.

8.5 ABOUT THE MAHWAH DATACENTER:

- A purpose built data center facility to support highly available IT processing
- 398,000 ft^2 two story building situated on an 28 acre site 34 miles from Wall Street
- Data Center white space scalable to 100,000 ft^2 at 150 w/ ft^2
- Scalable mechanical & electrical infrastructure design
- Redundant fiber diversely routed to site
- 28 MW of total site electrical power
- 48 Hours of emergency generator fuel storage & cooling tower water
- Double action pre-action sprinkler fire suppression
- Armed security staff, state of the art surveillance systems

CA TECHNOLOGIES

CA Technologies is an IT management software and solutions company with expertise across all IT environments — from mainframe and distributed, to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services.

Using a range of CA Technologies' service management solutions, banks are able to provide more proactive and standardized IT support services. A better understanding of the IT infrastructure has enabled banks to reduce the volume of IT issues and resolve problems faster. In addition to improving efficiency, banks are able to reduce costs and safeguard business continuity. Using data from CA Service Desk Manager and CA solutions, the bank is able to identify and address problems in a more proactive manner. For example, CA solutions contains data on the interdependencies between 6,000 configuration items, which enables the bank to determine the potential impact of changes before executing them.

With CA Service Operations Insight (formerly CA Spectrum Service Assurance), IT operations executives and staff can visualize and analyze their infrastructure, applications and transactions together, in the context of the business services they support. This helps pinpoint, prioritize and resolve service problems across technology domains and IT supply chains to diminish risk to services, improve service quality and predictability and optimize operational efficiency. Examples of business services include online banking, retail, insurance claims processing, driver license renewal, warehouse/distribution systems and e911.

CA Service Operations Insight also provides the data necessary for CA Business Service Insight to determine which services are operating in an IT environment, and to compare the service performance against benchmarks. CA Business Service Insight also can then identify alternative services to help better manage contractual relationships with outsourcers, internal parties and customers.

SERVICES DESCRIPTION

CA Identity and Access Management as an Automated Service

Leverage service management to automate and simplify identity administration

agility made possible™

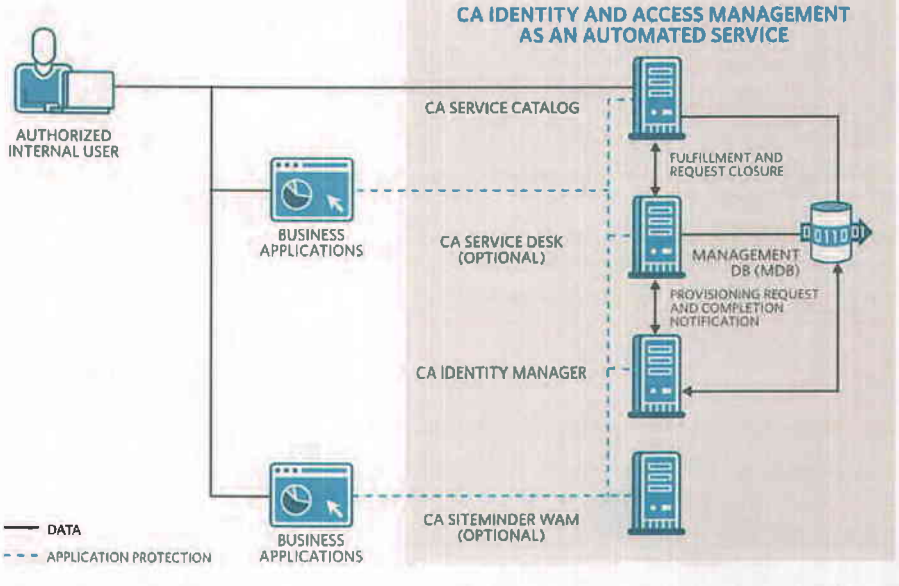
ca technologies

Harness the combined power of CA Technologies service management and identity and access management (IAM) products to use a standard catalog interface for requesting IAM-related IT services and then having them automatically fulfilled. Achieve a successful implementation of this solution through CA Services expertise, deployment methodology, and proven approach to lowering risk and accelerating time-to-value.

Supporting your business

CA Identity and Access Management as an Automated Service enables users to submit identity administration requests by following the same procedure that they use for other IT service requests. Individuals can access CA Service Catalog to initiate identity-related requests and changes. CA Service Catalog then works transparently with CA IdentityMinder™ to fulfill those requests, including navigating through the required approval processes. This integration also offers organizations the option to include CA Service Desk to increase the level of control over the change order process, or CA SiteMinder® to secure access to the major web components of the integration.

The illustration shows you how the integration works. It includes a set of prebuilt components combined with services that enable a smooth implementation and deployment into your environment.



Delivering business value

CA Identity and Access Management as an Automated Service:

- Leverages ITIL®-based service requests to align IT security operations with business priorities
- Reduces costs, simplifies training, and improves the user experience
- Streamlines and automates the identity provisioning process
- Extends and enhances your investment in CA Service Catalog, CA Service Desk, and CA IdentityMinder
- Integrates the separate and distinct industry domains of Service Management and IAM to enable the implementation of new automated processes
- Lowers risk and improves time-to-value with an implementation using prebuilt and tested components, proven methodologies, and best practices

What you get

The CA Identity and Access Management as an Automated Service implementation provides:

- A set of prebuilt components, including CA Service Catalog request forms, CA Service Catalog and CA Service Desk workflow processes, a CA IdentityMinder provisioning connector and transaction and role monitors
- Installation and Configuration Guide
- Services to install, configure, and demonstrate the reference implementation in a development environment, and then install and test the integration in a production environment
- Staff mentoring and knowledge transfer sessions

Why CA Services?

CA Services is committed to your success with CA Technologies solutions, and can help you throughout the entire solution lifecycle, from strategy and consulting to implementation and management. CA Services delivers unsurpassed depth of expertise for insight and control over technology and deployment efforts, and breadth of services offerings to deliver results with confidence.

No one knows CA Technologies like CA Services.

Get started

To purchase the CA Identity and Access Management as an Automated Service solution or to speak with CA Technologies about how you can integrate this solution into your environment, please contact CA Services at at **ca.com/services**.

Copyright ©2013 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. ITIL® is a registered trademark and a registered community trademark of the UK Office of Government and Commerce (OGC) and is registered in the U.S. Patent and Trademark Office.

CS3254_0113

SOLUTION BRIEF

authentication in the internet banking environment:

The solution for FFIEC compliance from CA Technologies

agility made possible™

ca technologies

Introduction to FFIEC Compliance

In October of 2005, the Federal Financial Institutions Examination Council (FFIEC) issued a guidance entitled "Authentication in an Internet Banking Environment" in response to increasingly sophisticated electronic attacks that compromise personal identity information and erode customer confidence in online banking security. The goal of the FFIEC guidance was to improve security for online banking transactions, due to the consensus view that simple username/password authentication was not sufficient for today's online banking environment.

With several years of experience and analysis under their belts, and the continued growth of online fraud, in June of 2011, the FFIEC circulated a Supplement update to this guidance, entitled "Interagency Supplement to Authentication in an Internet Banking Environment". This paper will review the original guidance and how CA Technologies exceeds the requirements outlined in the new Supplement document.

Key Requirements of FFIEC

The Original Guidance

The FFIEC came to recognize that with the rise in volume of online banking transactions, single-factor authentication techniques were simply not adequate security anymore. With this situation in mind, the original Guidance included three important recommendations.

1 Strong Authentication

A common misperception about the original regulation is that it requires specific 2-factor authentication technologies to be implemented for online banking. In fact, it only requires authentication methods that are "appropriate and reasonable", from a business point of view, for the reasonably foreseeable risks associated with a given online banking transaction. Since the minimum standards for effective and appropriate authentication might change over time based on technology advances, this requirement implies that an ongoing process for reviewing authentication strategies needs to be implemented.

2 Risk Assessment

Each bank should perform a detailed risk analysis of their entire online banking environment, including all factors or activities that are involved in all supported customer transactions, including the following factors:

- Types of customers
- Sensitivity of all private customer information
- Typical transaction types and the expected size of the transaction
- Expected transaction rates
- The potential for loss for each transaction type

The final area of the Guidance relates to education and training programs intended to increase customer awareness of the risks and potential threats associated with online banking transactions. Although the Guidance is unspecific about how this awareness effort should be done, it suggests the importance of tracking security-related information such as the number of unauthorized attempts to obtain authentication information, the size of identity theft related losses, and other such events. See **ffiec.gov/pdf/authentication_guidance.pdf**

The Supplement to the original Guidelines called for improving security for online transactions in several areas:

- Improved risk assessments
- Increased use of multi-factor authentication, especially for high-risk transactions
- Layered security controls to detect and respond to suspicious activity, including increased control over administrative functions
- More effective authentication techniques (for example, device identification)
- Improved customer awareness and education

The supplement calls for an overall strengthening of authentication technologies. It notes that out-of-band authentication has taken on a new level of importance given the preponderance of malware running on customer PCs, which can defeat OTP tokens, simple device identification with cookies or basic knowledge-based questions.

These additional mandates are based on the increasing sophistication and organization of financial attacks, as well as the continued increase in the volume and size of financial transactions being conducted online.

The solution for FFIEC compliance from CA Technologies

CA Technologies has built a flexible set of authentication solutions to support a layered, risk appropriate approach to strong authentication and fraud prevention. Many banks attempted to comply with the original FFIEC guidance by simply implementing some basic risk-based authentication techniques but the increase in online financial fraud and the new supplement has increased the pressure to find more sophisticated risk-based solutions. One approach can't alleviate all threats but CA Technologies works with our customers to reach the ultimate goal which is not just compliance, but a strong, flexible, and effective authentication and fraud prevention system to protect the full range of financial transactions.

The CA Technologies solution for Advanced Authentication includes the following:

- CA AuthMinder™ – provides flexible and broad capabilities for strong user authentication
- CA RiskMinder™ – provides real-time protection against identity theft and online fraud via risk-based, adaptive authentication.
- CA ArcotID® – a secure software credential that combines strong key protection with the low cost and simplicity of a software solution, providing strong, two-factor authentication. No hardware tokens are necessary. You are able to add strong authentication to any application without changing your user's login process. The CA ArcotID delivers the strength of PKI with the simplicity of a password, making it ideal for both enterprise and consumer uses.
- CA ArcotID® OTP – a software application that runs on a mobile phone and generates a one-time password that is used to authenticate to online applications and to verify valid credentials for online purchases.

CA AuthMinder and CA RiskMinder, when deployed together, provide the strong, layered security that is the foundation of effective FFIEC compliance.

When planning an FFIEC compliance effort, there are at least three critical areas that need to be considered:

- Strong, two-factor authentication (2FA) capabilities
- Risk-based fraud detection and prevention capabilities
- Fine-grained control of privileged users

Strong Authentication

FFIEC compliance does not require a specific authentication technology for all cases. Rather, it requires authentication that is appropriate for the risk level of a given transaction profile. Therefore, depending on each organization's needs, different authentication methodologies might be chosen.

When selecting authentication methods for a particular transaction, these factors are important:

- Ease of use for the customer
- Ease of IT administration
- Relative level of security offered by each authentication method
- Total cost to purchase
- Total cost to deploy

CA AuthMinder is a versatile authentication server that allows organizations to deploy a wide range of strong authentication methods in a cost-effective and centralized manner. It supports a range of authentication methods which include username/password, security Q&A, OTP via SMS, email or voice, OATH tokens, and the unique software-based CA ArcotID and CA ArcotID OTP credentials. It helps increase security and improve your compliance profile without burdening users or your service desk.

CA AuthMinder can provide the following business benefits to an organization:

- **Deploy multi-factor authentication invisibly:** Your users never have to know that you upgraded them to multi-factor authentication, unless you want them to. They can keep the same username/password sign-on experience with which they have become so accustomed. The solution invisibly protects and verifies their identity without burdensome additional login steps.
- **Lower cost of ownership:** CA AuthMinder's authentication server allows you to authenticate users with a wide range of authentication methods. It can help you manage your authentication environment more efficiently by creating a central point for authentication policy creation and enforcement. If you use CA ArcotID or CA ArcotID OTP software-only approach, there is no hardware to lose, fail, or break. It provides a low cost, easy to distribute second factor authentication method that hardware-based alternatives cannot match. The simplicity and transparency of this approach helps reduce both management and support costs.
- **Reduce risk:** CA AuthMinder centralizes the management and execution of strong authentication. It authenticates users via a wide range of methods, giving you the flexibility to choose the authentication methods that best suit your user groups. It also helps you manage competing compliance demands by creating a central point for authentication enforcement. When CA ArcotID is used as the second factor it helps protect the digital identities of your users behind proven, patented cryptographic technology.
- **Block Man-in-the-Middle (MITM):** CA AuthMinder when used with CA ArcotID, helps prevent MITM attacks. CA ArcotID authenticates only with the domain that issued it, helping protect your users from Phishers and Pharmers where OTP tokens and Grid Pads cannot.
- **Achieve high-performance:** To meet the rigorous security, availability, and data integrity demands of the financial services industry, CA AuthMinder was designed from the start to provide industry leading security and performance. To provide authentication services to millions of users, it was designed with virtually unlimited horizontal scalability, with a goal of unparalleled ease-of-use and extremely low latency.
- **Enjoy virtually unlimited scalability:** CA AuthMinder provides excellent vertical scalability through increasing memory/disk/processors. It achieves full-featured horizontal scalability with additional local or remote servers. Horizontal scalability provides performance gains as well as high-availability features for critical deployments.

Risk Assessment: Fraud Detection and Prevention

The incidence of identity theft and online fraud continues to grow as financial organizations are trying to find a good balance between the strength of security necessary and the level of inconvenience for their business and retail consumers. It is critical that organizations have the ability to enforce risk-based rules and parameters and use analytical modeling techniques to reduce their exposure to fraudulent activity. However, overbearing countermeasures that require repetitive user interaction can create a negative experience and affect customer loyalty. The challenge is to instantaneously detect and block fraudulent activity before fraud losses occur, without affecting or distracting legitimate users.

CA RiskMinder is an effective first line of defense against identity fraud. You can verify and detect suspicious activity for consumer and enterprise online services without burdening intended users. It is a robust, multi-channel risk assessment and fraud detection solution that transparently helps you detect and prevent fraud before losses occur. You can create an adaptive risk analysis process that assesses the fraud potential of every online login and transaction based on level of risk, user and device profiles, and organizational policies. As a result of the real-time, calculated risk score, users can be allowed to continue, be required to provide additional authentication credentials, or be denied access.

CA RiskMinder can provide the following business benefits:

- **Reduce losses due to fraud:** CA RiskMinder helps prevent fraud losses by blocking high-risk transactions before they complete, or requiring additional authentication for unusual or suspicious transactions. It can also be combined with CA AuthMinder to implement step-up authentication when encountering a suspicious transaction as part of a comprehensive multi-factor authentication solution. It can also be deployed alone to assess risk of individual login attempts to a portal based on a variety of input factors.
- **Address regulatory requirements:** CA RiskMinder helps you to meet a number of government and industry regulations including FFIEC, HIPAA, and SOX as well as your own internal security requirements.
- **Protect existing infrastructure investment:** You can integrate CA RiskMinder with any Internet-facing application via API's or web services in order to add real time fraud detection. It integrates with your existing access management, VPN, online banking, and e-commerce software and other security products, avoiding the need for you to upgrade other parts of your network to add Web fraud detection.
- **Match rules to your environment:** The customizable rules engine enables you to configure CA RiskMinder to match your business practices and risk tolerance, rather than forcing you to change your operations to fit your security tool. This allows you to reach the appropriate balance between the strength of your security and the impact on the end user.
- **Deploy and use multi-factor authentication invisibly:** Your Web users can keep the same username/password sign-on experience with which they are familiar. CA RiskMinder affects only those users whose behavior does not match their personal profile, historical data and your policies. There is no change to the user experience and therefore no new calls to the help desk or additional support costs.

Control of privileged users

The FFIEC Supplement specifically calls out strong and effective control over privileged users as a requirement for compliance. Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations, and on the overall security and privacy of corporate assets and information. Therefore, it is essential that privileged users be allowed to perform only those actions that are required for their specific responsibilities, and only on the appropriate assets. In addition, the use of Admin shared accounts (such as "root") pose a compliance challenge because each activity must be associated with a single person, in order to identify the culprit in the case of unauthorized behavior.

CA ControlMinder™ is a leading solution for privileged user management that controls access to host systems and critical data and files residing on these systems. Policies can be defined that help ensure that only properly authorized users can gain access to each such system or resource. In this way, CA ControlMinder extends the basic security capabilities supported by each native operating system and provides an expanded, consistent, and more granular set of security capabilities across the systems in your environment.

The solution also supports extensive privileged user password management (PUPM), which helps provide the accountability of privileged access through the issuance of passwords on a temporary, one-time-use basis, or as necessary while providing accountability of users' actions through secure auditing. It also includes CA User Activity Reporting (CA UAR) which provides user activity and compliance reporting usage across physical, virtual, and cloud environments. It verifies security controls and streamlines reporting and investigation of user and resource access activities to accelerate and simplify compliance and improve efficiencies.

CA ControlMinder can provide the following business benefits to an organization:

- **Fine-grained access control policies:** helps ensure that only authorized privileged users can access your critical data and applications. It provides improved and more granular security than is available through native operating systems.
- **Improved compliance:** allows you to proactively and more easily display fine-grained control over privileged users. This helps to simplify and reduce the cost of compliance audits since you have evidence of compliance.
- **Improved password security:** supports one-time use administrative passwords so that privileged users cannot share passwords, thereby improving security and helping to reduce the occurrence of over-privileged users. In addition, it helps eliminate shared accounts so that each action can be associated with a specific individual, further helping simplify compliance audits.
- **Improved security for virtual environments:** helps enforce segregation of duties rules on the hypervisor, so that the hypervisor administrator cannot access virtual machine configurations via the hypervisor.
- **Hardening of the entire operating environment:** helps to harden the operating system as well as the hypervisor, reducing both external and internal security risks and improving operating reliability.

Solution Capabilities and Benefits

FFIEC Requirements	CA Technologies Solution	Solution Benefits
Better Risk Assessment	CA RiskMinder provides a comprehensive risk and fraud detection system that uses device, location and historical user information to assess the risk of any specific transaction.	• Uses standard rules, customized rules, and external data sources to arrive at a risk score • Uses fraud modeling to help identify and prevent fraud in real time. • Makes a suspect transaction appear to complete correctly to the user, while moving it to a special queue for further analysis prior to actual transaction completion.
Adopt Stronger Authentication Standards for High Risk Transactions	CA AuthMinder: • Provides two-factor authentication with our patented CA ArcotID solution. • Provides two factor authentication with our CA ArcotID OTP solution. • Can generate One Time Passwords (OTP) and use Out of Band (OOB) channels including SMS, IVR and email to send an OTP to the user. Users can then enter the correct code back into the portal to identify themselves. • Provides a solution to protect against MITM attacks.	• CA ArcotID appears to the user as a username and password so it's easy to use. With PKI "under the covers" it brings the strength of PKI to the solution without the related complexity for the institution or the user. Automatically helps protect users from phishing and MITM attacks • CA ArcotID OTP appears just like an OTP generated from a single purpose token except it uses the customer's own mobile device. It can support multiple accounts on the same device and protect the seed value with patented technology. • Delivers second factor information through any number of out of band channels. • Provides flexibility in using additional information in the authentication process as required
Layered Security Programs	CA RiskMinder and CA AuthMinder • Provide a comprehensive layered security solution that provides: – Fraud monitoring – Authorization from multiple devices – OOB verification – Step up at certain levels – IP blocking	The layers can include: • Strong 2FA authentication. • Device, location, transaction information collection. • Built in rules and custom rules for determining risk based on collected factors as well as custom models. • Ability to incorporate additional external data into the risk evaluation process.
Effectiveness of Certain Authentication Techniques	CA Technologies provides: • Complex device identification • Challenge questions – Shared secret – OOW	Increased effectiveness of device identification due to: – the use of over 50 different parameters – the ability to work without a cookie Increased effectiveness of challenge questions due to: – the ability to customize the number and type of questions required (including "out of wallet") – the ability to use additional 3rd party, identity proofing questions
Control over privileged users	CA ControlMinder Password Vault CA RiskMinder and CA AuthMinder	• Increased granularity of control over what resources Admins can access. • Ability to control use of critical system services. • Reduced risk of inadvertent or malicious improper actions by privileged users. • One-time use passwords improve security and eliminate the use of shared accounts. • Easier and less costly compliance audits due to the ability to prove what Admins have done on the system.

technologies

Summary

FFIEC is an important driver of compliance activities for a large number of major financial and banking institutions. This standard was initiated in order to ensure that adequate security, in the form of strengthened authentication, was being used for high-value online banking applications.

FFIEC compliance requires risk-based authentication policies, strong two-factor authentication capabilities, as well as improved control over the actions of privileged users. Some companies adopt a minimalist approach to FFIEC compliance, and do only the minimum required to satisfy auditors. But, this approach is short-sighted because it fails to incorporate the business benefits of increased confidence (and therefore loyalty) on the part of a financial institution's customers, which often results from a comprehensive approach to strong user authentication, coupled with a simple and effective user interface.

The CA Technologies solutions for Advanced Authentication and Privileged User Management can provide an effective and layered platform for reducing authentication risk and simplifying compliance with FFIEC.

For more information on these solutions, please visit: [illegible]

fiserv.

FISERV, INC.

Fiserv is a global provider of financial services technology. The company serves more than 16,000 clients worldwide, including banks, thrifts, credit unions, investment management firms, leasing and finance companies, retailers, merchants and government agencies. The company provides solutions for issues related to payments, processing services, risk and compliance management, customer and channel management, and service optimization.

Fiserv's experience with customer relations management has several applications that can help steer the growth of Pakistan's branchless banking services. Fiserv offers total management and operations support for ATM networks. Beyond handling basic transactions like cash withdrawals and balance inquiries, Fiserv also helps to implement bilingual screens, no-envelope depositing, PIN change systems, and round-the-clock monitoring tools.

Fiserv does similar work to help improve online banking platforms. The company's expertise can allow newly-online banks to better aid customers, offering advanced online banking transactions, such as viewing account balances and history, making transfers, canceling checks, viewing check images and accessing electronic statements. Mobile banking solutions can be supported by Fiserv's fraud and risk management solutions.

SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION (SWIFT)

SWIFT is a member-owned cooperative that provides the communications platform, products and services to connect more than 9,500 banking organizations, securities institutions and corporate customers in 209 countries. SWIFT enables its users to exchange automated, standardized financial information securely and reliably, thereby lowering costs, reducing operational risk and eliminating operational inefficiencies. SWIFT also brings the financial community together to work collaboratively to shape market practice, define standards and debate issues of mutual interest.

SWIFT enables its customers to automate and standardize financial transactions, thereby lowering costs, reducing operational risk and eliminating inefficiencies from their operations. By using SWIFT customers can also create new business opportunities and revenue streams.

Economic changes in the payments landscape have forced the banking community to find new ways to reduce their operational costs, mitigate their liquidity risk and increase the revenue and efficiency of their core payment products. Under the pressure of regulators, the cash management service offering becomes more transparent to meet new customer expectations. While conforming to regulation is a must, service quality becomes a key differentiator.

SWIFT has developed offerings in payments and cash management to help the banking community meet these urgent challenges:

- **Enhance customer service**: automate exceptions and investigations in order to reduce enquiry turn-around time and to provide transparency on enquiry status to your customers, provide a compelling value proposition for wholesale payments to corporates or person-to-person retail payments for immigrants (SWIFTRemit) – including mobile payments.
- **Improve liquidity and risk management**: SWIFT liquidity risk services support financial institutions in their efforts to build their liquidity dashboards and develop liquidity risk analytics in an efficient way.
- **Increase operational efficiency and save costs**: SWIFT's single window allows you to rationalize your connectivity channels with:
- Correspondent banks for clearing and settlement of domestic or foreign currency payments using SWIFT's payments clearing messaging services
- High value payments clearing and/or settlement systems operating on a real-time gross settlement basis using SWIFT's secure and reliable FIN domestic services for high value payment market infrastructures
- Retail payments clearing systems using SWIFT's cost efficient services for retail payments market infrastructures: the services help to clear "batches" of payments prior to settlement at discrete intervals, with or without netting.

Mobile payments

Three winning strategies for banks

Highlights

- Mobile payments are a top priority
- There is competition from non-banks
- Banks can use mobile payments to get closer to customers
- In particular for mobile money transfers, banks should collaborate to develop a global service

Executive summary

Mobile payments are a hot topic in the financial industry and a top priority for banks, because:

- The ever growing ubiquity of the mobile phone: on a world population of 7 billion, there are 5 billion mobile phones, but only 2 billion people have a bank account;
- Consumers are using their mobile phones to make payments in over 130 deployments with a 100 more planned and several new initiatives announced each week;
- It is a growing market predicted to increase to 900 million users and USD 1 trillion in transaction value by 2015.

Many banks have launched a mobile payments service or wallet, but this opportunity also brings specific challenges:

- There are many new entrants investing heavily in mobile payments: mobile network operators like Vodafone, e-commerce companies like Google, retailers like Carrefour, payment service providers like PayPal, as well as money transfer operators and card companies;
- It is still an immature business where only a few initiatives have succeeded in attracting a significant user base;
- It is an unclear business case for many banks who wonder what is the up-sell when a payment becomes mobile and who may see little value in a telco-led model;
- It is a complex matter where legal frameworks are not yet harmonised, technology is evolving with a need for partnerships, and where banks may feel they lack the expertise.

This competitive and fast evolving landscape creates doubt. Many banks wonder what to do: just stand by and watch or respond more pro-actively? What is our bank's mobile payments strategy?

Our recommendation to banks regarding mobile payments is two-fold:

1. Play to your strengths. Double-guessing under these circumstances can be costly. The path to success is to use clear criteria: respond to an obvious customer demand, use technologies that satisfy that need, and decide based on a clear business case.
2. Use mobile payments to bring your customers closer to your bank, in a new "experience banking model" (cf SWIFT's white paper on Correspondent Banking 3.0).[1]

We see three areas of strategic opportunity for banks:

- Mobile banking: using a mobile phone to access a bank account and make payments – can provide more convenience to customers. Banks should actively invest and expand this channel now, in particular for corporate treasurers;
- Mobile commerce: using a mobile phone to buy products. This is driven by e-commerce companies looking to uplift their product sales and generate revenue from advertising. This is more a 3-5 year play as the customer/retailer value still needs to mature. Banks should

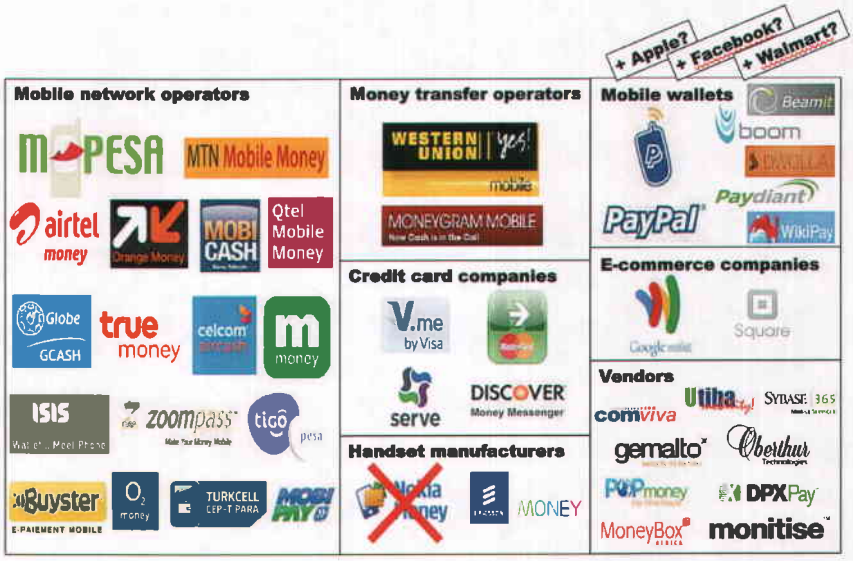


Figure 1: Non-banks leading innovation in mobile payments

Each area may present opportunities for collaborative solutions: offer a serviced platform for mobile banking connectivity, provide a hosted application to distribute payments services onto a mobile commerce wallet or develop a mobile payments service for international money transfers.

In conclusion, mobile payments are a strategic opportunity for banks, both as a defensive play against new entrants, as well as a growth prospect to convert cash into electronic transactions.

A top priority

Mobile payments are a top investment priority for banks.

In fact, the world's biggest banks continue to focus most of their announced IT initiatives on mobile financial services (including payments) and online banking.[2]

This is not surprising given the ever-growing ubiquity of the mobile phone. Out of a world population of 7 billion, over 5 billion or 70% have a mobile phone, whereas only 2 billion or 30% have a bank account. Take India: on a population of 1.2 billion over 800 million have a mobile phone and only 250 million have a bank account.

Consumers are increasingly using their mobile phones to make payments. A global inventory lists over 130 live mobile money deployments and nearly 100 more are planned.[3] Several new initiatives are announced every week.

This is a growing market. Mobile is the payment technology that will have the greatest growth over the next five years.[4] Growth predictions for mobile payments vary from 350 to 900 million users generating USD 430 billion to 1 trillion in transaction value by 2015.[5]

Specific challenges for banks

Many banks have launched a mobile payment service or wallet.

This is a very competitive and fast evolving battlefield with specific challenges for banks.

New entrants

Many non-banks have entered the mobile payments market, often with innovative solutions. Mobile network operators like Vodafone, MTN, Orange and airtel have deployed mobile payments services in several countries or have set up joint ventures between them, like Isis in the US or project Oscar in the UK. Money transfer operators like Western Union and MoneyGram, as well as card companies like Visa, MasterCard and Amex all have multiple mobile payments initiatives. Payment service providers like PayPal are throwing their full weight into mobile. E-commerce companies like Google are deploying wallets for contactless payments using NFC (Near Field Communications).

An immature business

Only a handful of these mobile payments services have succeeded in attracting a significant user base (over 1 million users). New initiatives may fail to go beyond pilot trials and some services (like Nokia Money in India) have ended altogether.

Unclear business case

For many banks the business case to do mobile payments is not clear. Mobile payments and linked commerce will represent USD 20-25 billion in revenue by 2016 from new revenue opportunities and potential loss mitigation.[6] But this a very different kind of payments opportunity for banks to pursue as most of the revenue may be advertising related. Banks will need to compete for these new mobile value-added services and revenue streams. In addition, banks need to determine which role to play in these new value chains. In a telco-centric model for example, the bank's revenue share from providing the trust account function may be limited to 10% whilst 55% goes to the mobile network operator and 35% to the distributor.[7]

A complex matter

Deploying a mobile payments service is not straightforward as legal frameworks across countries are not harmonised, technology is still evolving, there is a need for multiple partnerships, and in general banks may feel they lack the expertise.

Three strategic opportunities

For many banks this competitive and fast evolving landscape creates doubt. They wonder what to do: just stand by and watch or respond more pro-actively?

We see three strategic areas of opportunity and actions for banks to use the mobile phone to forge closer relationships with their customers in a new "experience banking model" (cf SWIFT's white paper on

Correspondent Banking 3.0)[1]:

- Mobile banking: using a mobile phone to access a bank account and make payments;
- Mobile commerce: using a mobile phone to buy products;
- Mobile money transfers: using a mobile phone to send money to someone.

Let's examine this in more detail as each area comes with its own opportunities and challenges.

Mobile banking

Mobile banking is using your mobile phone to access your bank account; receive debit/credit alerts and statements via SMS; check balances and recent transactions by browsing a simple mobile-enabled website; conduct basic operations via a menu; or transfer funds and pay bills using an application on a smart phone (see box 1). Many banks offer one or more of these options, like ICICI for example.

Box 1: Technology options

- SMS: communicate with payments services via short messages; can work with short codes. If a menu is required, access from a SIM card (after replacement) or an application folder (loaded from Micro SD card).
- USSD (Unstructured Supplementary Services Data): conversation-like telecom protocol to access menu on server by sending short code (e.g. dial *525#).
- WAP (Wireless Application Protocol): to access simple text-only web page (online).
- IVR (Interactive Voice Response): menu accessed by calling toll-free number ("to transfer money, press 1").
- Application on smartphone typically downloaded.

Mobile can fundamentally change the retail banking experience and strengthen customer-bank relationships.

Some banks also have mobile banking services for corporate treasurers[8], but these are often basic services to initiate and approve payments, receive transaction alerts and view account balances.

Figure 2: Three strategic opportunities for banks in mobile payments

The good thing here is that the bank is in total control: the mobile phone purely acts as a channel to access the financial application that is owned by and runs at the bank.

Our recommendation: Banks should actively expand their mobile banking offering, which today is often still underdeveloped particularly toward corporates. A unique value proposition can turn mobile banking into a cost saving (instead of contacting a call centre) and revenue generating channel (increase loyalty, target marketing to cross-sell core banking services). This means banks should invest more in resources: a survey of 150 banks across Europe indicates that 70% are planning to add more functionality, but the majority have fewer than 10 people dedicated to mobile.[9]

Collaborative opportunity? Many smaller and medium-sized banks will be looking to deploy a mobile banking channel to connect their customers. Rather than build one, they are more likely to buy a product. In that case, it could make sense to provide a serviced mobile platform that can be white labelled.

Mobile commerce

Mobile commerce is using your mobile phone to buy digital or physical goods and services, remotely from a website or in proximity like a shop, metro station or vending machine.

Not considered here as mobile payments are:

1. Direct carrier billing, where purchase of e.g. digital content like ringtones is charged to a mobile phone bill and that bill is paid by a traditional payment method like credit transfer or direct debit. This practice is very successful however. Examples of companies that facilitate this are boku, Zong, mopay and PaymentOne, each servicing 200 million to 3 billion customers for 250-300 carriers in 60-80 countries.
2. Mobile point of sale, where a card reader is attached to a mobile phone or tablet to swipe a credit card. Whilst it has the potential to significantly increase the number of points of sale, the resulting payment is a traditional credit card transaction. Such card readers are provided by companies like Square, Intuit and iZettle.
3. Mobile product scanning, where a mobile phone is used to scan a product's bar code at an Apple store for example and links it to your iTunes account. In that case, your iTunes bill is settled by a credit card payment.

There is currently a buzz around NFC payments (see box 2). Used for example in Japan: 65 million enabled handsets, 15 million customers initiating 30-50 million transactions/month with 750,000 merchants; excluding transit.[10] Several projects have been launched in some 35 countries in Europe, the US and China[11], but many have a long way to go to reach a mass market. Google Wallet is one example.

Here, consumer and e-commerce companies are better placed than banks to develop these solutions since they own the product or can enhance the shopping experience: browse the web to find and compare products, locate a store nearby, select the product from a smart poster,

receive a discount, and pay for it –all with a mobile phone, in one experience. Their interest is in generating an uplift in business from a higher average ticket spend and visitor frequency or from selling advertising, rather than in the payment itself.

Box 2: NFC
(Near Field Communications)

- Two-way contactless communication over short distance (few centimetres), between NFC-enabled phone and reader (e.g. POS terminal or smart poster)
- To enable a phone: 1) embed NFC chip, 2) glue NFC sticker at back, 3) insert Micro SD card (for iPhone e.g. Wireless Dynamics or DeviceFidelity provide a case)
- NFC vendors: e.g. Innovision/ Broadcom, NXP Semiconductors, INSIDESecure, Gemalto, ViVOtech
- NFC itself does not make a payment, still need to load virtual credit card(s) on phone.
- NFC-enabled phones to grow from 7 million in 2011 to 203 million in 2015 (Yankee Group).
- More in developed markets as emerging markets generally have basic handsets
- More resources: Wikipedia NFC page, NFC forum

Several telecom companies have started mobile wallet initiatives, but some have had to open up to reach a larger audience, ask for regulatory approval or delay projects[12]. Handset manufacturers may play a leading role by embedding their NFC chip in the phone.

However, there is a large degree of uncertainty about wide-scale adoption. Retailers and users need to be convinced of its value over existing payments alternatives. There are concerns about security: we must make sure that account and credit card details will be safe if the mobile phone is lost or stolen. And there is a high degree of technology evolution: where, for example, does the secure element sit to NFC-enable the handset and store the financial application? A whole new business has emerged for banks to distribute their payment and credit card services over the air onto the mobile phone via a Trusted Service Manager.[13]

Our recommendation: A few banks have engaged in mobile commerce, but in general banks should remain realistic. This is not an easy area to get into as it requires a considerable investment that may not produce immediate returns. On the other hand, early involvement can develop a good understanding of how this all works. Banks should therefore look to partner with e-commerce companies to gain experience, insert their financial services in the commerce transaction, and then enhance the business of their payments products with better consumer insights. Another strategy for a large transaction bank can be to provide the back-end payments infrastructure to these e-commerce companies.

Collaborative opportunity? If this business further develops, many banks will need to use a Trusted Service Manager. Instead of each bank operating such a system, it could make sense to deploy a set of such applications as a hosted service in the cloud to provide more choice and reduce the total cost of ownership.

Mobile money transfers

In developing countries with a low banking and high mobile phone penetration, mobile wallets[14] can bring basic payments services to the un/ under-banked. Often starting with money transfers, these services become more sophisticated over time to include paying for bills and goods, pre-paid debit cards, ATM withdrawals, salary disbursements, etc.

These are typically provided by mobile network operators using a mobile wallet (see box 3). Two examples are SMART Money in the Philippines (launched by SMART in 2000, over 9 million wallets, connected to 9,000 ATMs, over 4,000 cash-in/cash-out centers, 15 partner banks and 95,000 agents) and M-Pesa in Kenya (launched by Safaricom in 2007, 30,000 agents, 14 million users, 70% of all electronic transfers in Kenya, USD 1 billion transferred/month).

Mobile network operators see this as an up-sell, a value-added service. Their business case comes from transaction or subscription revenues, reducing mobile subscription top-up distribution costs and increasing customer retention. They have a large agency network that can be re-used. They also have a better marketing and consumer deployment experience than many banks.

Whilst successful in some developing countries, these cannot be replicated as such in developed markets because of specific success factors: 1) a strong, latent demand for remittances; 2) in a country with low banking, high mobile penetration; 3) with a legal framework that enables easy customer registration and is in proportion to the risk of very low value payments; 4) starting with domestic remittances and mobile top-up; 5) by a dominant player, motivated to establish a leading position in a closed system; and 6) supported by a large agent network[15].

This agent network is key for people to pay cash into their mobile wallet and to cash money out. The service provider must make sure the agents support its product and that there is sufficient

Box 3: Key mobile wallet/platform vendors

- Comviva: Ex-Bharti Telesoft; provides value added services to mobile operators; deployments with Orange in Africa, Tigo in Africa and Latin Americas, and South East Asia.
- Fundamo: HQ in South Africa, acquired by VISA; mobile financial services provider; deployments with MTN in Africa.
- Gemalto: HQ in Amsterdam; provides digital security solutions, incl. for NFC; platform for mobile money transfers.
- Monetise: HQ in London; delivers mobile banking, payments and commerce networks; VISA partnership.
- Oberthur: HQ in France; provides smart cards; partnership with Utiba; deployed by e.g. airtel in Africa.
- Sybase 365: HQ in the US; SAP company; provides mobile messaging and commerce including remittances; bought paybox.
- Utiba: HQ in Singapore; pioneer in mobile financial services with G-Cash, deployments in Asia Pacific, Latin America.

liquidity in the network (if a person wants to cash out their salary, but the agent does not have any money, the SMS on their phone has no value, except to make other mobile purchases).

So where is the next big opportunity? Several readiness and condition frameworks, as well as detailed country analyses are available.[16] These, combined with population size (to develop a significant business), lead us for example to Nigeria, India, Pakistan, Brazil, Mexico and Colombia.

Our recommendation: Banks should consider making a bolder move in mobile money transfers. They should take an opportunistic approach and individually partner with a mobile network operator for a specific deployment in one country, as well as work together to deploy a global mobile payments service for international money transfers and remittances.

Collaborative opportunity? If banks are to develop a global mobile payments service, it could make sense to develop this collaboratively.

Obstacles to growth in mobile money transfers

Let's have a closer look at mobile money transfers. Whilst there are several domestic deployments, many still need to build their customer base or create the basic service. We see three obstacles to further growth and global adoption:

Box 4: Differences in legal frameworks (examples)

- MNO friendly: Philippines (MNOs can perform banking functions), Kenya (wallet seen as transaction accounts), Nigeria, Malaysia, Thailand, Indonesia.
- Flexible: Europe (e-money directive – often taken as example, MNO can get PSD license), US (MNO to register at FinCEN as money service business), Japan (non-discriminatory rules, MNO to deposit money in bank account)
- Banks only: South Africa (bank-led except for agents, lower KYC/AML requirements), India, Bangladesh, Tanzania, Uganda.

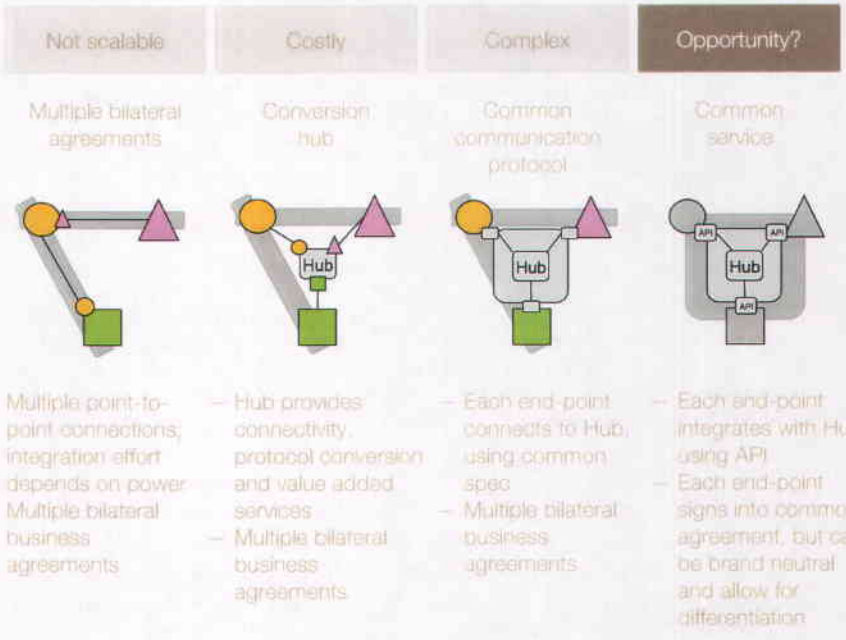


Figure 3: Options to achieve interoperability across mobile payments services

Regulation
In several countries there is already a regulatory framework for e-money and mobile payments, while in others it is still evolving. Conditions vary between countries on who can operate such a service, the transaction and wallet size, and the type of transaction allowed (see box 4).

Regulators are concerned about mobile payments being used for money laundering and fraud. Several have adopted a proportionate approach, balancing advancing financial inclusion with ensuring the stability and soundness of the country's financial system.

Cooperation
Not one single bank or mobile network operator covers the whole world, so there is a need for cooperation and partnerships.[17] Joint ventures between mobile network operators may not be obvious as they are very competitive on their core voice and data business. Joint ventures with banks may not be obvious as parties have different business objectives, different perspectives on revenue sharing, and different mind sets (mobile operators are more agile, banks focus on robustness).

Examples include Equity Bank with M-Pesa, State Bank of India with airtel, Banamex with América Móvil, Alfa-Bank with VimpelCom, Garanti Bank with Turkcell and Avea.

Interoperability
Today, most mobile payments services are closed-loop systems whereby one customer cannot send a payment to a customer in another system, even within one country. Interoperability is the metaphorical elephant in the room: all agree it can boost volumes, but with their own company's interests taking priority, nobody wants to let anyone in whilst expanding market share.

Still, interconnectivity is growing. For example: G-Cash has bilateral agreements with several other systems. Western Union links to M-Pesa; BICS' HomeSend is a hub that includes communication protocol as well as FX conversion; India's IMPS is multi-bank by design and underpinned by the country's ACH[18] and we also see this model in the UK supported by VocaLink. By and large however, mobile systems do not interconnect on a global basis.

The ideal model for interoperability

Interoperability may be required, but what does it actually mean and how can it be achieved? For end-customers interoperability simply means that it works and is easy, fast, safe and cheap.

For service providers, interconnecting means a lot of acrobatics behind the scenes:

- Technical: establish secure real-time connectivity between service providers, conversion of communication protocols (from SMS in one system to USSD in the other);
- Customer product features: the cost of making a mobile payment, the maximum amount allowed, product types supported (just payments or also micro-credits), feature compatibility (send payment or also beneficiary initiated, possibility to include notification text, specific features present in one system but not another, possibility to create a viral wallet or not);
- Commercial conditions between service providers: split of revenues and costs, FX conversion, charges to customers (deducted from initial or received amount), providing transparency upfront of these charges, amounts and execution timeframes to customers;
- Legal: contractual agreements, responsibility and liability, ensure minimum level of KYC and AML by each party, recourse procedures;
- Clearing and settlement and related liquidity and risk management.

There are several options to achieve this, ranging from multiple bilateral agreements to a conversion hub, a common communication protocol, or a common service where companies adhere to the same set of rules.

It is not clear which model will prevail, but it is worth exploring the opportunity of a common service.

The case for a global bank-owned service

Today, most domestic mobile money transfer services are run by mobile network operators that have begun to target the international remittance market. For example, Vodafone Money Transfer in Qatar, which has nearly 1.7 million expatriates, can send money transfers to 10 countries. Mobile network operators also link together or connect with money transfer operators and credit card companies: e.g. G-Cash and Maxis, MoneyGram and SMART Money, Western Union and M-Pesa, MTN and VISA. Card companies are also creating their own international P2P services: e.g. Visa acquired Fundamo, American Express created Serve.

Should banks stand by and watch? Aren't money transfers, mobile included, the business of banks?

A sustainable business for telcos?

In the long run, mobile money transfers may not be as profitable as some mobile operators thought:

1. Not a core activity: mobile network operators see mobile payments as a value added service, whereas for banks it is a core service. This will impact resource allocation.
2. Limited revenues: the business case for a telecom company to deploy a mobile remittance corridor can have a quick and strong payback albeit with limited revenue. Only 10% of mobile operators see this service as accounting for more than 10% of their bottom line.[19]
3. Increasing costs: as volumes rise and become systemically important or go cross-border, regulators will impose higher KYC/AML checks, compliance conditions, business continuity, more frequent and detailed reporting, etc., thereby increasing the operator's cost and reducing margins. For banks, this cost is already part of their operating model.
4. Increasing competition: a regulator may initially facilitate one operator to thrive in order to develop a basic payments infrastructure, but before long the system will be opened up to other providers to avoid excessive market power, drive further financial inclusion and allow customers the choice of service provider. Over 70% of mobile network operators expect 3-5 competitors in their market in 3-5 years.[20] Some have applied for a bank or payment service provider licence, such as Rogers in Canada or O2 in the UK. They thereby become bank competitors.
5. Interoperability: to further grow volumes, telecom companies will have to interconnect their mobile payments services, but making them globally interoperable is quite complicated.

A good business for banks?

International money transfers are a core business of many banks. Banks have reason to protect and grow that business with innovative services, mobile payments included:

1. This is a sizeable business for banks. Over 215 million people live outside their country of birth. Worldwide recorded remittance flows are expected to reach USD 536 billion by 2013; detailed information about top emigration countries and migration corridors is available.[21] Banks currently have 30% of this business; there is market share to be gained.
2. This is a high margin business, where willingness to pay is much greater than in domestic or face-to-face transactions at point of sale. In addition to person-to-person (P2P) payments, banks can use their existing relationships to attract additional volumes from businesses (B2P) and governments (G2P) for salary and social payments.
3. Instead of playing a secondary role in a telco-led model, banks can capture 65% of the value if they run the mobile payment service (still likely needing an agent network). For banks, the transactional payments business may not be the end-game, but a way to build relationships and up-sell more banking products, such as savings, credit and insurance.

A bold yet pragmatic approach

Rather than trying to achieve interoperability between multiple mobile ecosystems, which will take forever and can be quite costly, banks should consider developing a global service for mobile person-to-person payments that each bank can plug into.

Key characteristics of such a service would be:

- Transparent and compelling. Not built on a platform that converts a patchwork of multiple bilateral systems, but a single and consistent offering;
- Open. An API allows banks to insert their mobile money transfer services, may be open to other providers as well;
- Simple to use. Money is sent to the receiver's mobile phone number, rather than to an account number and bank code;
- Work off existing bank accounts replenished via ACH or direct debit. This is similar to PayPal, but now the money is kept in the banking system;
- Brand neutral, allowing for differentiation. Whilst providing a common infrastructure, each bank can brand and differentiate the service for its customers;
- Include agency networks and cash out capabilities. In particular at the receiver's side, typically in a developing country without bank accounts but with mobiles (e.g. HDFC Bank in India's partnership with Vodafone).The mobile wallet can be combined with a pre-paid card to make a POS purchase or withdraw money at an ATM;
- Buy instead of build. The service does not need to be developed from scratch, as there are several wallet systems and providers out there to choose from;
- Adopt a pragmatic approach. Although bank-owned, the service could be run as a commercial company to have the necessary execution and deployment agility.

"Let's just all use SWIFT, because it works". That was a proposal in the opening of a conference panel discussing the interconnectivity of mobile payments services.

There are some initiatives where banks collaborate on a domestic level, like clearXchange in the US or IMPS in India. Who can bring banks together to work on mobile payments on a global level?

- The mobile network operator community? The GSMA, for example, has global coverage and is actively driving mobile payments, but as it represents the interests of mobile operators, banks at large may not be willing to join.
- The interbank world? SWIFT, for example, operates globally and has a track record of interoperability. Mobile payments initiatives, however, tend to be driven by banks' retail organisations which are not very familiar with SWIFT-related transaction processes.
- A mobile payments association? Mobey Forum, for example, is bank-led, but can it gather a global execution capability?
- An international standards body? ISO, for example, has a global, cross-industry representation, but as they are chiefly concerned with standardisation, could they drive commercial adoption?
- A platform vendor? Can they ever be inclusive enough?

In conclusion, mobile payments have a strong growth potential.

Many banks have developed a mobile payments service or wallet. But many non-banks have also entered the mobile payments market, often with innovative solutions.

Banks can seize mobile payments as an opportunity, provided they define a clear strategy and invest accordingly. To that purpose, we recommend a series of actions for banks to pursue in mobile banking, mobile commerce and mobile money transfers.

In particular regarding mobile money transfers, banks should look to make a bolder move and develop a global person-to-person payments service that is mobile-enabled.

In doing so, banks will pro-actively shape the future of mobile payments.

SWIFTNET SERVICES FROM ORACLE FINANCIAL SERVICES SOFTWARE

ORACLE
FINANCIAL SERVICES

SWIFT Ready Services India 2009

HELPING FINANCIAL INSTITUTIONS MAXIMIZE THEIR RETURNS ON SWIFTNET INVESTMENTS

FEATURES

- Unique end-to-end implementation methodology
- Offerings cover consulting, implementation support interfaces, and services on SWIFTNet
- Onsite/offshore resource insourcing and 24/7 support
- Customized on-the-job training for technical and operational staff

BENEFITS

- Reduce costs through optimized components.
- Gain access to technical experts and specialists with experience in the global support and maintenance of SWIFTNet infrastructure.
- Implement SWIFTNet services and integrate solutions such as SWIFTNet Accord.

Today, many new and compelling challenges in the messaging space are driving financial institutions to maximize their returns on SWIFTNet investments. These organizations are looking at centralizing SWIFTNet messages, adopting International Organization for Standardization 20022 message standards, subscribing to new SWIFTNet solutions, and extending their reach to players such as market infrastructure and corporate customers. Oracle Financial Services Software is the leading IT solutions provider to the financial services industry. As a SWIFT-accredited SWIFTReady service provider, Oracle Financial Services Software can help your organization prepare a road map for its SWIFTNet products and solutions.

Partner with Oracle Financial Services Software for SWIFTNet Consulting, Implementation, and Support Services

Oracle Financial Services Software's SWIFT-accredited SWIFTNet consultants possess a deep and intuitive understanding of the financial messaging domain—in particular, of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and its changing requirements—and the business needs of financial institutions. These experts are well-equipped to offer you consulting, implementation, and support services on a SWIFTNet infrastructure.

Talk to SWIFTNet Consultants from Oracle Financial Services Software

Certified by the SWIFT Service Partner program, Oracle Financial Services Software's experts have consulted on numerous projects to help multinational banks and financial institutions worldwide implement their SWIFTNet initiatives. From selecting the connectivity pack, through sizing and installing the necessary hardware, to configuring and integrating the SWIFT interfaces and solutions, Oracle's consultants work with customers every step of the way—and beyond, by maintaining the SWIFTNet infrastructure through Oracle's cost-effective, 24/7 onsite/offshore support model. One of the largest SWIFTNet infrastructures in the world—carrying nearly 6 percent of the total FIN (financial application) traffic—is a key Oracle Financial Services Software project.

Your organization can benefit from Oracle Financial Services Software with

- Consulting services for secure IP network connectivity, along with the implementation, configuration, and maintenance of SWIFTNet infrastructure

components—including SWIFT Alliance Gateways (SAGs), SWIFT Alliance Webstations (SABs), SWIFT Alliance Access/Entry (SAA/E), SWIFT Alliance Messenger (SAM), and SWIFTNet Link (SNL)—establishing closed user groups in real-time gross settlement or corporate environments, and integrating back-office applications

- High-end, techno-functional consulting services for financial institutions to implement new SWIFTNet services and integrate solutions such as SWIFTNet Accord, SWIFTNet Trade Services Utility (TSU), SWIFTNet Funds, and SWIFTNet Exceptions and Investigations (E&I)
- Customized on-the-job training, allowing technical and operational staff to achieve straight-through processing expertise in the payments segment

More important, when you partner with Oracle Financial Services Software, your organization gains

- Access to SWIFT-accredited technical experts and a large pool of specialists with significant experience in the global support and maintenance of SWIFTNet infrastructure for large banks
- Reduced costs resulting from the onsite/offshore nature of Oracle's implementation methodology
- Readily available infrastructure and minimum turnaround times for SWIFTNet support services, a result of Oracle's experience with ongoing global assignments
- 24/7 support, ensuring seamless operation
- In-place processes for production support assignments
- Smoother implementation of newer SWIFTNet services such as SWIFTNet Accord, SWIFTNet TSU, SWIFTNet Funds, and SWIFTNet E&I
- Network provisioning
- End-user training

Further Value-Added Services

Oracle Financial Services Software also offers the following value-added services:

- Consulting and implementation services for SWIFTNet Phase 2 migration
- Consulting services and customized technical and operational training, allowing new SWIFT members and participants to connect to SWIFTNet
- Establishment of disaster recovery sites to ensure continuity of business (COB)
- Consulting services for
  - Creating a SWIFTNet road map, including technical and functional upgrades to SWIFTNet infrastructure
  - Implementing end-to-end consumer-to-business solutions over SWIFTNet

RELATED SERVICES AND SOLUTIONS

Oracle delivers a comprehensive portfolio of applications, technology, and services to help customers get the most out of their investments in financial messaging services and standards. With Oracle's financial messaging solutions and services, customers can integrate their complete range of applications that are generating and receiving financial messages using global standards and networks—from supporting front-office trading standards (such as FIX) through integrating with payments (such as SEPA) and securities settlement infrastructures through SWIFT.

FINANCIAL MESSAGING INTEGRATION SERVICES

- Offers a portfolio of financial messaging applications
- Provides SWIFT implementation and integration services

RELATED SOLUTIONS

- Oracle Service Bus for Financial Services: SWIFTReady Financial EAI Label
- Oracle FLEXCUBE Messaging Hub
- Oracle's PeopleSoft Financial Gateway: Supports EDI ANSI X.12 EDI, BAI, EDIFACT, ISO20022, Fedwire, NACHA, and SWIFT messaging standards

- Integration of business applications with SWIFTNet components and interfaces through supported adapters, including Transaction Delivery Agent, SNL Remote API, and IBM WebSphere Message Queuing
- Integration of business applications with SWIFTNet components and interfaces
- SWIFT-mandated technical upgrades
- Configuration and facilitation of browse links for various types of market infrastructure such as Continuous Linked Settlement Bank and Banca d'Italia's BiRel
- Site-specific, best-practice process documentation and audits
- Global CoB setup and test execution
- Problem tracking with SWIFT
- Professional consultancy and single point of reference

Contact Us

For more information about Oracle Financial Services Software's SWIFTNet services, please visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative, or e-mail us at financialservices_ww@oracle.com.

Oracle is committed to developing practices and products that help protect the environment

Copyright © 2008, 2009, Oracle and/or its affiliates. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. 0309

ORACLE

SAFRAN

MorphoTrust USA

MorphoTrust USA & L-1 Identity Solutions

Morpho, a high-technology company in the Safran group, is one of the world's leading suppliers of identification, detection and e-document solutions. Morpho is specialized in personal rights and flow management applications, in particular based on biometrics, a sector in which it is the world leader, as well as secure terminals and smart cards. Morpho's integrated systems and equipment are deployed worldwide and contribute to the safety and security of transportation, data, people and countries.

MorphoTrust Transaction Solutions are designed to simplify and secure transactions where ensuring the identity of the individual is paramount. Wherever a transaction requires verification that a person is who they claim to be, MorphoTrust has the solution.

- They have unparalleled experience in the collection of biometric data including facial and fingerprint solutions for state and local governments
- They have more than 10,000 document authentication systems deployed in mission-critical environments including border control, transportation, departments of motor vehicles and critical infrastructure locations
- Their systems manage the largest databases of fingerprint data in the U.S. via our work with multiple agencies within the federal government
- They are one of a small number of commercial organizations approved and trusted to send transactional fingerprint data directly to the FBI on behalf of the state agencies that regulate trusted professions such as education, transportation, healthcare and commercial transport
- Their self-service solutions uniquely include biometrics as a way of establishing a trusted identity with unmanned kiosks and online-facilitated transactions

Whenever transactions are tied to establishing a trusted identity, while protecting personally identifiable information, only MorphoTrust has the Identity Framework and expertise to deliver complete solutions demanded by government and commercial entities. From simple self-service solutions, to more comprehensive and sophisticated solutions for aviation and commercial ID authentication, MorphoTrust enables trusted transactions.

Examples of our competencies in this area include the following solutions:

- Biometric screening solutions and devices
- Border management solutions and devices
- Self-service and kiosk solutions
- Document authentication, scanning and archiving solutions and devices
- Online/mobile solutions
- Aviation, retail and banking solutions

L-1 Identity Solutions provides a full range of finger/palm, face, iris, and multi-biometric products for government-sponsored civilian identification management programs and criminal identification management procedures managed by law enforcement and military agencies.

Introducing MorphoTrust USA

A Morpho Company, and part of the Safran Group

- Multi-modal biometric software chosen by the Department of Defense Enterprise
- Prime contractor for the Department of State's facial recognition program for Passports and Visas
- Primary supplier of iris recognition software for tactical use within the Department of Defense
- Driver license issuance solutions to 41 of 50 states and D.C.
- Largest nationwide network of ID service centers, across all 50 states, with over 2.5 million applicants enrolled annually

The Leading Provider of Identity Solutions in the U.S.

You knew us as L-1 Identity Solutions. Now we are MorphoTrust USA – with a new name, a stronger company and focused on simplifying, protecting and securing the lives of the American people. We support the goal of "One Person, One Identity" – verifying that applicants are who they claim to be and delivering the highly secure credentials that Americans use each day to exercise their civil rights, such as voting, and enjoy the many benefits and services afforded to those living in the U.S. Our solutions for driver license issuance, for example, enable Americans to obtain credit, open a checking account, apply for a job, drive a car, board a plane, or even order a drink at the local pub. They also help the American public, government agencies and commercial businesses reduce identity fraud and enhance national security.

A Proxy Company

MorphoTrust is uniquely governed by Proxy and National Security Agreements. This means that even though we are owned by Safran, we are considered to be a U.S. company. We must hire only U.S. citizens and ensure the protection of all personally identifiable information entrusted to us.

What We Offer

MorphoTrust is the trusted partner for all U.S. states and D.C., as well as many federal agencies and commercial businesses. We deliver complete solutions for secure ID issuance, such as the U.S. driver license and passports, as well as for border management, public safety, law enforcement, retail, travel and applicant vetting. We enroll and verify the identities of applicants through the use of sophisticated biometrics (finger, face and iris), document authentication and data verification. We also have deep expertise in database management, workflow, system integration and architecture, delivering some of the largest, most complex systems for collecting applicant biometrics, searching large databases to identify potential fraud and security breaches, or for enrollment purposes. Our solutions fall under the MorphoTrust™ Identity Framework which encompasses the entire ecosystem of our offerings, including the people, expertise, proven systems and methodologies used to deliver our solutions.

- MorphoTrust™ Secure ID Issuance Solutions
- MorphoTrust™ Enrollment Solutions
- MorphoTrust™ Identity Management Solutions
- MorphoTrust™ Identity Management Practices
- MorphoTrust™ Transaction Solutions
- MorphoTrust™ Investigative Solutions

Learn more by downloading the MorphoTrust Intro Brief found at: www.morphotrust.com.

PAUL HASTINGS

VISA

PAUL HASTINGS LLP. / VISA

Paul Hastings LLP has a wealth of knowledge, experience, and insight to guide clients through today's evolving financial landscape. The firm represents leading U.S. and international banks from their offices in financial centers across the U.S., Europe, and Asia.

Paul Hasting's clients include the world's largest card association and America's largest electronic bill payment company, second largest money remittance business, and largest issuer of prepaid cards. They also represent numerous other businesses engaged in such diverse areas as check electronification, payment processing, and credit, debit and stored value cards.

Visa is a global payments technology company that connects consumers, businesses, financial institutions and governments in more than 200 countries and territories to fast, secure and reliable digital currency. The company continues to provide consumers, businesses and governments with a better form of payment. Visa operates VisaNet, the world's largest retail electronic payments processing network, handling an average of 150 million transactions every day. In total, more than $6.3 trillion in global consumer spending is transacted on Visa-branded payment products annually.

Underlying these products is a robust set of processing services that are powered by VisaNet — including core transaction processing, risk management and information-based services. These services can be tailored to individual countries or regions and serve the needs of financial institutions, governments, businesses, merchants and consumers around the globe. Each day, VisaNet connects up to 2 billion cards, millions of acceptance locations, 1.96 million ATMs and 15,000 financial institutions.

Since VisaNet's inception as one of the world's first electronic credit card authorization systems, Visa has invested valuable time and assets into continually improving, refining and expanding its global processing system.

STAY CURRENT

PAUL HASTINGS

February 2012

FDIC Updates Guidance on Payment Processor Relationships

BY KEVIN L. PETRASIC

In its recently issued Financial Institution Letter, FIL-3-2012, the Federal Deposit Insurance Corporation ("FDIC") updated the agency's November 2008 guidance on the potential risks to insured depository institutions of payment processor relationships.[1] The updated guidance is in response to the increased number of deposit relationships between insured institutions and payment processors utilizing institutions' deposit accounts to process payments for third-party merchants and, in some cases, other payment processors.

The FDIC guidance addresses bank relationships with companies that process payments for a wide variety of entities, including telemarketers, online businesses, and other types of merchants. A particular emphasis of the newly issued guidance relates to FDIC expectations regarding how institutions should be monitoring and mitigating risks arising from these relationships, as well as due diligence efforts necessary to understand the underlying risks related to payment processor relationships with merchants, as well as other payment processors that a processor may service.

While focused on depository institution payment processor relationships, FIL-3-2012 highlights a number of important regulatory and supervisory issues presented by the intersection of traditional bank products and services with rapidly evolving payment systems practices and technologies, including card-based, internet and electronic funds transfers, and other emerging e-commerce and mobile payment systems products and services. The FDIC guidance presents important insights for insured institutions with respect to a wide variety of third-party relationship management issues. These issues are important to insured institutions, entities that utilize institution products and services in dealing with third parties, and vendors providing or managing third-party relationship products and services for or through insured institutions.

Overview

As noted in the FDIC's guidance, payment processors typically process payments either by creating and depositing remotely created checks ("RCCs"), also known as "demand drafts," or by originating Automated Clearing House ("ACH") debits on behalf of merchant customers. Payment processors may use their own deposit account to process such transactions, or may establish separate deposit accounts for their merchant clients in order to process the transactions.

The FDIC guidance highlights the following important considerations for depository institutions maintaining or establishing payment processor relationships:

- Institutions should conduct careful due diligence and prudent underwriting in establishing, and careful monitoring in maintaining, account relationships with third-party payment processors;
- Institutions should pay particular attention to account relationships with high-risk entities that could expose the institution to risks arising from unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act;
- Institutions should carefully review and monitor heightened money laundering and fraud risks that may exist with payment processors that fail to verify merchant client identities and monitor customer merchant business practices;
- Institutions should monitor and review consumer complaints or unusual return rates that may indicate the inappropriate use of personal account information and possible deception or unfair treatment of consumers;
- Institutions should have policies in place promptly to address fraudulent or improper activities involving payment processor relationships; and
- Institutions failing to manage risks arising from payment processor relationships may be subject to various enforcement actions, including civil money penalties and restitution orders.

Know Your Payment Processor

Perhaps the most important message in the FDIC's newly issued guidance is the need for insured institutions to know and understand the risks presented by an individual payment processor relationship, including the payment processor's processes for verifying the identity of its merchant customers and their business operations and practices. Institutions that fail to implement adequate controls to understand and manage third-party risks arising from a payment processor relationship expose the institution to elevated money laundering and fraud risk, along with legal, reputational, and compliance risks if consumers are harmed. To manage the risks, insured institutions must understand, verify, and monitor the activities and the entities related to each account relationship, particularly given the absence of a direct customer relationship with merchant clients of the payment processor.

Managing the Payment Processor Relationship

"Deposit relationships with payment processors expose institutions to risks not customarily present in relationships with other commercial customers. These include increased operational, strategic, credit, compliance, and transaction risks."

Certainly, an important aspect of managing a payment processor relationship is the contractual agreement that forms the basis of the relationship. At a minimum, contracts with payment processors must provide a depository institution with "access to necessary information in a timely manner." In addition, a contract should provide for immediate termination of the relationship where a processor exposes the institution to undue risks, as well as establishing an adequate reserve requirement to cover anticipated charge-backs. In managing payment processor relationship risks, insured institutions are expected to oversee all transactions and processing activities, as well as to manage and mitigate operational risks, Bank Secrecy Act (BSA) compliance, fraud risks, and consumer protection risks arising from the relationship.

"Insured institutions should also consider the potential for legal, reputational, and other risks, including risks associated with a high or increasing number of customer complaints and returned items, and the potential for claims of unfair or deceptive practices."

An important point stressed in the FDIC guidance is the potential liability to institutions that fail to

adequately manage payment processor relationships and, as a result, may be viewed as facilitating a payment processor's or merchant client's fraudulent or unlawful activity. A particular concern is potential liability for "facilitating or aiding and abetting consumer unfairness or deception under Section 5 of the Federal Trade Commission Act."

Several additional issues highlighted by the FDIC include risks posed by payment processors that use multiple financial institutions to process merchant client payments, and payment processors that solicit business relationships with troubled depository institutions. In both cases, payment processors may be engaging in opportunistic activities that are not serving the best interests of the insured institution. Particularly vulnerable targets include smaller, community banks that lack the infrastructure to properly manage or control a third-party payment processor relationship.

In managing payment processor relationships, institutions should also monitor consumer complaint activity, including complaints received at the institution, complaint activity at a payment processor or with its underlying merchants, and other independent sources of complaint data or other investigations or legal action. When identifying problems, institutions are expected to act promptly to address possible consumer harm. Where potentially fraudulent or improper activities are involved, appropriate responses include filing a Suspicious Activity Report and taking directed action against a payment processor and/or merchant, such as suspending or terminating the relationship or freezing an account to cover future charge-backs.

Internal Risk Controls

An important aspect of effectively managing a payment processor relationship is implementing and maintaining internal controls to mitigate risk. Appropriate and well-defined controls include "enhanced due diligence; effective underwriting; and increased scrutiny and monitoring of high-risk accounts for an increase in unauthorized returns, charge backs, suspicious activity, and/or consumer complaints."[2] Effective controls will help in avoiding risky payment processor relationships, as well as in detecting and minimizing risks arising from fraudulent merchant activities in existing relationships.

A. *Establishing the Relationship*

Financial institutions are expected to implement policies and procedures designed to avoid risky payment processor relationships. Institutions should have clearly articulated thresholds for unauthorized returns, a strong due diligence and underwriting policy for screening new payment processors, including understanding the nature of the business operations and existing merchant relationships, and a method for authenticating the operations and assessing the underlying merchant risks. Relevant factors include:

- Identifying a processor's major lines of business and merchant customer volume;
- Reviewing a processor's due diligence standards for new merchants;
- Reviewing corporate documentation and external information on principal owners and operators;
- Conducting an on-site review of a processor's business operations;
- Reviewing a processor's promotional materials to determine target clients;
- Reviewing "gateway arrangements" where a processor re-sells its services to a third party;
- Assessing potential conflicts of interest that exist between processor management and institution insiders;

- Assessing the adequacy and verification of information on a processor's merchant clients and merchants' affiliates; and
- Conducting independent operational audits on a payment processor calibrated to the degree to which the institution will rely on the processor for merchant client due diligence.

B. *Maintaining the Relationship*

The FDIC guidance notes that an important aspect of managing risk in an existing payment processor relationship is monitoring transaction activity for higher rates of returns or charge backs and/or high levels of returns arising from unauthorized RCCs or ACH debits. All of these circumstances can be indicative of fraudulent activity. An equally important and often more difficult issue involves BSA/AML compliance. While institutions are required to implement comprehensive compliance programs, the FDIC guidance notes that "nonbank payment processors generally are not subject to BSA/AML regulatory requirements, and therefore some payment processors are more vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions." Thus, institutions maintaining payment processor relationships should have procedures in place to monitor transaction activity, volume, merchant data, and charge-back history.

> *"Consumer complaints and/or high rates of return may be an indicator of unauthorized or illegal activity."*

Institutions should also regularly screen consumer complaint activity at a payment processor and its merchant clients. This will enable institutions to identify and detect risks related to fraud and/or illegal activity. In this regard, institutions should have formalized procedures for routine audits of third-party payment processing relationships. Such audits should review merchant client relationships and processors' contractual obligations to merchants that may impact the institution.

Action Plan – Establish and Maintain Effective Risk Mitigation Techniques

A critical aspect of an insured institution's payment processor program is establishing and maintaining effective oversight and controls to minimize potential risks arising from such relationships. Key issues for an effective program are assessing risk tolerance, verifying a payment processor's business operations, evaluating ownership and control, and establishing ongoing monitoring of account relationships. Equally important are institution policies and procedures for detecting and addressing fraudulent or improper activities, and for avoiding and addressing consumer harm.

As with any activity involving third-party arrangements, institutions should pay close attention not only to their own internal monitoring and controls, but also to those of the payment processors in which they establish and maintain an account relationship. In assessing risks posed by payment processor relationships, institutions must understand the unique business operations of each payment processor relationship, as well as the relationships that each payment processor has with each of its merchant clients. This requires a coordinated compliance program in which the institution and payment processor must partner to minimize operational risks and avoid supervisory scrutiny.

Institutions should review their existing policies and procedures both for establishing payment processor relationships and maintaining such relationships. Internal risk controls should be calibrated based on the particular circumstances of each payment processor relationship (including the nature of the processor's underlying merchant clientele) and institutions should be particularly mindful of maintaining contractual rights, terms, and conditions that provide remedies to address potential problems. These include invoking appropriate institution responses to address potentially fraudulent or improper activities, such as filing Suspicious Activity Reports, where appropriate, and taking directed

action against a payment processor and/or merchant, including suspending or terminating a relationship or freezing an account to cover future anticipated charge-backs.

Paul Hastings lawyers are actively working with insured institution and payment processor clients to identify and address issues and risks related to payment processor relationships, including developing and implementing risk mitigation policies and programs for institutions and processors to establish and maintain effective, safe, and profitable payment processor programs.

✧ ✧ ✧

If you have any questions regarding the FDIC's recently issued payment processor guidance, please do not hesitate to contact any of the following Paul Hastings lawyers:

Atlanta

Chris Daniel
1.404.815.2217
chrisdaniel@paulhastings.com

Todd W. Beauchamp
1.404.815.2154
toddbeauchamp@paulhastings.com

Kevin Erwin
1.404.815.2312
kevinerwin@paulhastings.com

Diane Pettit
1.404.815.2326
dianepettit@paulhastings.com

Palo Alto

Cathy S. Beyda
1.650.320.1824
cathybeyda@paulhastings.com

San Francisco

Thomas Brown
1.415.856.7248
tombrown@paulhastings.com

Stanton R. Koppel
1.415.856.7284
stankoppel@paulhastings.com

Washington, DC

V. Gerard Comizio
1.202.551.1272
vgerardcomizio@paulhastings.com

Kevin L. Petrasic
1.202.551.1896
kevinpetrasic@paulhastings.com

Erica Berg-Brennan
1.404.815.2294
ericaberg@paulhastings.com

Lawrence D. Kaplan
1.202.551.1829
lawrencekaplan@paulhastings.com

Michael Hertzberg
1.202.551.1797
michaelhertzberg@paulhastings.com

Helen Y. Lee
1.202.551.1817
helenlee@paulhastings.com

Scott Lieberman
1.202.551.1751
scottlieberman@paulhastings.com

Amanda M. Jabour
1.202.551.0376
amandajabour@paulhastings.com

[1] FDIC Financial Institution Letter FIL-3-2012, "Payment Processor Relationships: Revised Guidance" (January 31, 2012).

[2] *Id.* at 3.

Stay*Current* is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2012 Paul Hastings LLP.

IRS Circular 230 Disclosure: As required by U.S. Treasury Regulations governing tax practice, you are hereby advised that any written tax advice contained herein or attached was not written or intended to be used (and cannot be used) by any taxpayer for the purpose of avoiding penalties that may be imposed under the U.S. Internal Revenue Code.

SYMANTEC

Symantec helps consumers and organizations secure and manage their information-driven world. The company's software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

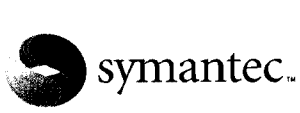
Symantec solutions for banking help protect customer information and brand reputation by securing sensitive data across business lines and heterogeneous systems for improved transparency and returns on new and existing IT investments. Symantec Data Loss Prevention solution enables banks, credit card companies, and credit-reporting institutions to protect confidential data such as customer identity and account information, intellectual property, and financial results. The company also delivers a solution to ensure high availability and centralized management across a bank's numerous applications and heterogeneous platform technologies for branch applications, call centers, payments and trading operations, and other core banking system.

With more banking applications subject to around-the-clock business service level agreements, banks are working to ensure continuity of IT operations as well as reduce the cost of the bank's operational resiliency strategy. Symantec delivers a solution to ensure high availability and centralized management across the bank's numerous applications and heterogeneous platform technologies for branch applications, call centers, payments and trading operations, and other core banking system.

Symantec Hosted Services uses the power of cloud computing to secure and manage information stored on endpoints and delivered via email, Web, and instant messaging. Building on the foundation of MessageLabs market leading software-as-a-service (SaaS) offerings and proven Symantec technologies, Symantec Hosted Services provides essential protection while virtually eliminating the need to manage hardware and software on site.

Symantec Protection Center unifies information security management across systems, networks and data to effectively protect against the inherent risks in today's IT infrastructures. This resource helps organizations strengthen their security defenses by providing a cohesive view of enterprise security, improving incident response times and driving greater operational efficiencies.

WHITE PAPER: SYMANTEC SECURITY RESPONSE



Threats to Online Banking

Candid Wüeest
Symantec Security Response, Dublin

Originally published by Virus Bulletin, July 2005. Copyright held by Virus Bulletin, Ltd., but is made available courtesy of Virus Bulletin. For more information on Virus Bulletin, please visit http://virusbtn.com/

Threats to Online Banking

Contents

Abstract.....4

Introdction.....4

Evolution.....4

Local Attacks.....5

Remote Attacks.....6

Joint Forces.....7

Conclusion.....8

References.....9

About the Author.....10

Abstract
The number of malicious applications targeting online banking transactions has increased dramatically in recent years. This represents a challenge not only to the customers who use such facilities, but also to the institutions who offer them, as evidenced by an ongoing trail in the US. These malicious applications employ two kinds of attack vector – local attacks which occur on the local computer, and remote attacks, which redirect the victim to a remote site. The possibility also exists that both approaches will be combined. Some attacks may be foiled by adopting security measures such as transaction numbers (TAN). However, it is likely that the risks associated with online banking transactions will remain until new transaction methods, such as PKI based methods (public key infrastructure), are widely introduced.

Introduction
A Miami businessman is suing his bank for the loss of $90,000. He claims that, in February 2005, this money was stolen from his online bank account via an unauthorized transaction. Investigations have revealed that the businessman's computer was infected with a Trojan capable of logging keystrokes, including his full account details. It is likely that the theft of this information was the trigger that led to the unapproved transaction to a foreign bank account. So far, the businessman's bank has refused to compensate for his loss [1].

This fraud case is not an isolated incident. The prevalence of malicious applications that steal financial account information has increased dramatically over the last year, often resulting in victims losing hard currency. In May 2003, only around 20 such Trojans existed in the wild. Two and a half years later, the number has increased to more than 2,000 [2]. Why?

There are several factors that may have influenced the evolution of this type of malicious application, but maybe the dramatic increase in their prevalence is just because they have a higher chance to succeed than expected. The case of the businessman in Miami is just one example of many that have succeeded.

Evolution
In the early stages, Trojans that steal financial account information targeted only a handful of online banks. For example, in August 2003, PWSteal.Bancos.B [3] stole account information from only five banks.

This has changed dramatically. PWSteal.Bancos.T [4], discovered in April 2005, contains a list of 2,764 URLs from 59 different top-level domains. The corresponding organizations range from small local bank branches to international banking groups. In February 2005, a Trojan named Trojan.Goldun.B [5] was discovered stealing account information for an online payment service called e-gold. The Trojan disguised itself as a security update for e-gold. When a user executed the deceptively-named file SecurityEgold.exe', the Trojan registered itself as a browser helper object (BHO) and monitored Internet Explorer for visits to pre-defined URLs. Any account information that was gathered by the Trojan was posted via a PHP script on a domain controlled by the attacker. The log file on the server storing the data was accessible by

anyone, most likely due to a misconfigured web server. A quick look at this log file showed a growing list of account numbers and corresponding passwords. Within an hour, the PHP script had added another 13 valid-looking account credentials. The site was online for another 24 hours before being shut down.

Interpolation of this data leads to the conclusion that the Trojan.Goldun.B attacker had received details for a large number of accounts, providing him with the opportunity to steal hard currency from the victims. The attack vectors used by this kind of malicious application can be categorized in two groups: local and remote attacks. Local attacks happen on the local computer during an online banking session. Remote attacks do not execute code on the local computer, but redirect the victim to a remote site.

Local Attacks

A common mistake made by end users is believing that their online banking session is perfectly safe when they use an SSL connection. Security experts continually state that everything is safe if there is a yellow padlock symbol in the browser window.

Figure 1: The yellow padlock symbol as displayed in Internet Explorer.

But SSL is designed as a secure tunnel from the end user computer to the bank mainframe and does not protect the end points such as the end user's computer. The PWSteal.Bankash.A [6] Trojan exploits this fact. The Trojan drops a DLL and registers its CLSID as a browser helper object in the registry. Thus the Trojan is able to intercept any information that is entered into a web page before it is encrypted by SSL and sent out. This functionality can also be achieved by injecting the Trojan directly into the web browser's memory space, which also can often bypass desktop firewalls when making outgoing connections. Other local attack methods include running a layered service provider (LSP) monitoring all network traffic, writing its own network driver, or displaying a carefully crafted copy of a website on top of the official website.

The PWSteal.Bancos family does the latter. When an infected user visits one of the predefined domain names, the Trojan generates a pop-up window which overlays the current browser window. The pop-up window contains an exact copy of the original service website login page. When information is entered into the fake form and the send button is pressed, the spoofed pop-up window closes, leaving the old browser window. Meanwhile, the harvested account credentials are sent to a remote server. These are only some of the possible methods that will work even if the session is SSL encrypted. These procedures will also bypass the virtual keyboard – a countermeasure that has been introduced by some online banking systems against key loggers. Here, the user clicks on a virtual keyboard displayed on the screen, rather than pressing the real keys on their keyboard, but this only shifts the problem: screen captures,

fake website pop-ups and malicious code running inside the web browser can record exactly the same information as key loggers. No matter how the information is entered into the web form, once it is entered, it can be intercepted.

A further step towards better security therefore, would be the use of non-static user credentials. A user name and a static password are simply no longer enough to protect online banking sessions. Some companies have already responded to these threats by introducing dynamic passwords including RSA secured ID tokens [7] or one-time passwords on paper lists called transaction numbers (TAN).

Unfortunately this does not solve the problem entirely. Since the method for entering authentication data has not changed, the password still can be intercepted. The only additional hurdle is that the attacker must use it first, before the legitimate user does. This behavior has not yet been observed in the wild, but consider the following scenario: a Trojan, intercepting a password by any of the discussed methods, simply has to send this information to the attacker. Meanwhile, it blocks every other connection from that computer. Thus the current online banking session is never completed. A network driver, LSP, BHO, or rootkit that hooks network API calls could do this. All the attacker needs to do is to use the unused, one-time password quickly to establish an online banking session from his or her own computer, enabling the attacker to do whatever he or she likes. Some companies therefore ask for multiple TANs during a session, one for login and one for each transaction made. Others ask for a specific TAN on a list and the position is chosen at random each time. Still you do not achieve 100 per cent security, as a man-in-the-middle attack can trick the user into revealing this information.

One next step towards better security may be PKI (public key infrastructure) smartcards, which have already been introduced by some banks. These cards can be attached to the computer using a USB card reader and can act as a challenge-response authentication or use a zero knowledge authentication, leaving the attacker with little useful information.

Remote Attacks

Usually, the attacker sets up a copy of the web page he wants to impersonate on a server he controls. In the past attackers often linked directly to the original images on the legitimate web server, which left easy-to-follow traces in the webmaster's log files. Nowadays, attackers tend to keep resources locally. Once the bait server has been set up, the attacker sends out emails that trick the user into visiting the spoofed website. These emails often prompt the user to visit the online service in order to provide some urgent data verification, or indicate that the user is required to visit the website because of some update process in the main database of the service provider. This form of social engineering attack, with the goal of acquiring user account information, is also known as phishing.

The location of the real server is obfuscated or masked using exploits or by other, not so well known methods. For example, one can translate the quartet of an IP address (such as 216.239.57.99) into a decimal number (such as 3639551331). Then a fake user authentication can be added that is made to

look like the impersonated domain (http://mySecureBank.tld@3639551331). This trick fools some users into believing that they are clicking on a link that leads to the mySecureBank.tld domain. Instead, it goes to 3639551331, which is the IP address of google.com represented as a decimal number. The use of international domain names (IDN), introduced by ICANN in June 2003, adds a further complication to the matter of identifying URL obfuscation. The fact that international characters can be used in domain names raises the issue of domain names that have been spoofed simply by replacing some of the letters in their name with letters from different alphabets that look the same.

For example, an attacker could register the domain 'mySecureBank.tld', where the 'a' is replaced with an 'a' from the Cyrillic character set, which looks identical. If a hacker finds a domain-authenticated SSL service, he or she can even add an SSL padlock in his attempt to fool the end user, as demonstrated by Johanson [8]. Trojan.Blinder [9] utilizes another example of obfuscation. Trojan.Blinder uses JavaScript to layer a white box over the location field of the browser hiding the fake URL. The box contains a spoofed URL that looks like a legitimate website. The position of the box is even recalculated and reapplied multiple times per second to ensure a seamless integration with the browser.

Furthermore, obfuscation is not even necessary. As seen in February 2005, large DNS poisoning attacks can lead to browser redirection, without even modifying the end user's computer directly. Once the user is on a spoofed website everything entered there can be captured.

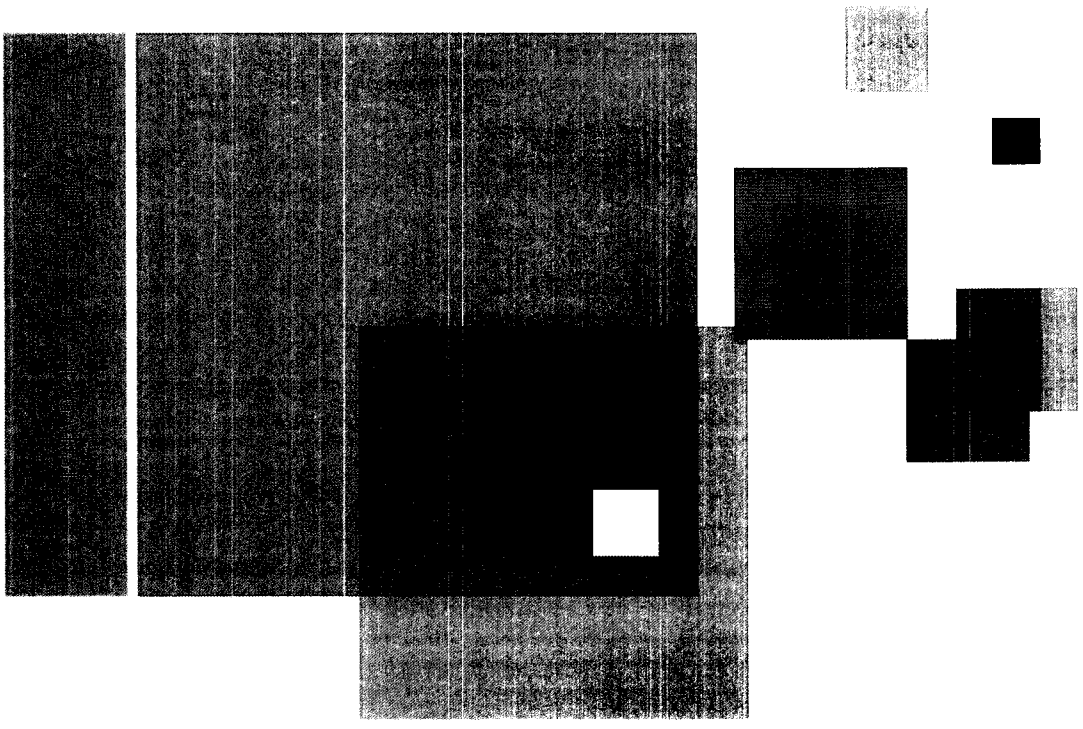
Joint Forces

If an attacker combines local and remote attacks more serious damage can result. For example, a Trojan running on an infected computer can alter the local hosts file to redirect any requests for mySecureBank.tld to an IP address controlled by the attacker. This behavior has already been observed in a number of adware threats in the wild. To complete the illusion, the Trojan can also install a self-signed root certificate on the infected computer. Free tools like OpenSSL can be used to help create these certificates. This enables the attacker to generate official-looking SSL connections from the infected computer to the malicious web server hosting the spoofed website. The chances of an average user noticing these changes are very slim.

Once the user has been trapped on such a spoofed website, the attacker can act as man-in-the middle and relay any challenge-response protocol that might be implemented by the original online banking system. At the moment we are not aware of a Trojan in the wild performing such an attack, but that does not mean that there couldn't already be one doing this. Such an attack could be countered by carefully checking the IP addresses involved in the session and their owners.

Conclusion

These examples show that the biggest threat to online banking is still malicious code executed carelessly on the end-user's computer. The attackers tend to target the weakest link. Once the attacker has control over a user's computer, he or she can modify the information flow to his or her advantage. This may have happened in the case of the businessman from Miami.
The situation most likely will not change until new transaction methods are introduced.
So, whenever using an online financial system today, ensure that your system is still under your control and not a spoofed puppet, or you could end up featuring as the businessman in the next fraud case article.



Banking Trojans

Who should read this paper

Banking malware, specifically banking Trojans, are reaching alarming new levels of sophistication. Go behind the scenes to understand how these attacks operate and how a layered security solution that includes fraud detection and strong authentication can help protect your business and your customers against online fraud.

WHITE PAPER: DEFEND YOUR INSTITUTION AGAINST TROJAN-AIDED FRAUD

Banking Trojans

Understanding Their Impact and How to Defend Your Institution Against Trojan-Aided Fraud

Contents

Introduction **1**

Banking Trojans: A growing threat **1**

A look inside the beast **2**

Statistics and logs 2

Advanced controls 3

Sophisticated backdoor 3

Extensive command list 3

Detecting and preventing trojan-assisted fraud **4**

A multilayer security solution from Symantec **6**

Detecting and protecting against fraud 7

Protecting identity with two-factor authentication 7

Conclusion **7**

Glossary **8**

Introduction

Banking malware, specifically banking Trojans, are reaching alarming new levels of sophistication. New variations are constantly being introduced to thwart detection by antivirus software on the victim's PC. And real-time capabilities built into the Trojans make it difficult for banks and account holders to spot fraud attempts as they occur.

Trojans today pose a clear threat to the trust in online banking that financial institutions have worked so hard to establish for their consumer and business customers. Plus, there's the threat to the bottom line: extensive fraud losses and potential lawsuits can add up to significant hard dollar costs. In 2009, a Maine- based construction firm sued its local bank after cyber thieves stole more than a half million dollars through illegal transfers from the company's online account[1] — a precedent that could set off further lawsuits against banks for not taking steps to prevent this type of fraud.

What steps can your company take to defend itself against sophisticated malware that's running on business employees' and consumers' devices? Industry experts agree that deploying a layered security strategy is your best defense. A multilayer security solution can help your institution establish a continuum of protection to detect, prevent, and mitigate fraud stemming from cybercriminals using banking Trojans.

This paper examines the current threat of banking Trojans, taking you behind the scenes of the most prevalent Trojan, Zeus, for a look at the power it can give cyber thieves. We'll cover the implications of these sophisticated Trojans for your business and how a layered security solution that includes fraud detection and strong authentication can help protect your business and your customers against online fraud.

Banking Trojans: A growing threat

Malware continues to grow at exponential rates, with Trojans now being the most common type at 66 percent of all malware.[2]Trojans infect a victim's computer to enable a cybercriminal to perform malicious functions like making it part of a botnet (collection of remotely-controlled computers) or stealing confidential data like passwords and credit card information. Hundreds of criminal groups are operating Zeus- fueled botnets called Zbot botnets.[3] The number of infected PCs is estimated at 3.6 million in the U.S., or 1 percent of all PCs in the country.[4]

Trojans like Silentbanker and Clampi have been infecting users' PCs for years, but by far the most prevalent of the banking Trojans is Zeus.[4] This data-stealing Trojan has been circulating since 2006, capturing infected users' banking logon credentials and sending them back to a command-and-control hub. Zeus is propagated through scams such as spam messages purportedly from Verizon Wireless®, a fake password reset request from MySpace®, a notice from the IRS, and a critical update for Microsoft Outlook®.[5]

Zeus infects PCs, waits for their users to log on to a list of targeted banks and financial institutions, and then steals their credentials and sends them to a remote server in real-time. Additionally, it may inject HTML into the pages rendered by the browser, so that its own content is displayed together with (or instead of) the genuine pages from the bank's Web server. In this way it is able to ask the user to divulge additional personal information, such as payment card number and PIN, one-time passwords, and more.

To evade detection and removal, Zeus uses rootkit techniques. The Zeus kit is a binary generator. Each use creates a new binary file, and these files are different from each other — making them notoriously difficult for antivirus or security software to detect. To date, very few variants have had effective antivirus signatures against them, and each use of the kit usually makes existing signatures ineffective.

1-"Maine Firm Sues Bank After $588,000 Cyber Heist," Brian Krebs, The Washington Post, September 23, 2009
2-"Security Report Finds Rise in Banking Trojans, Adware, Fewer Viruses," Robert Westervelt, SearchSecurity.com, January 6, 2010
3-"Year in Review," Marcia Savage, Financial Services Information Security News, December 8, 2009
4-"Antivirus Rarely Catches Zbot Zeus Trojan," Kelly Jackson Higgins, DarkReading, September 16, 2009
5-"New Verizon Wireless-Themed Zeus Campaign Hits," Angela Moscaritolo, SC Magazine, November 16, 2009

Zeus is also spawning a next generation of banking Trojans with even higher levels of sophistication. These newest Trojans not only collect credentials, but use them in real-time to thwart basic fraud detection measures. For instance, researchers recently identified a Trojan dubbed URLZone. URLZone is programmed to calculate on-the-fly how much money to steal from an account based on how much money is available.[6]

A look inside the beast

To understand just how powerful a Trojan like Zeus can be, let's look briefly at a sample of the capabilities it provides to cybercriminals.

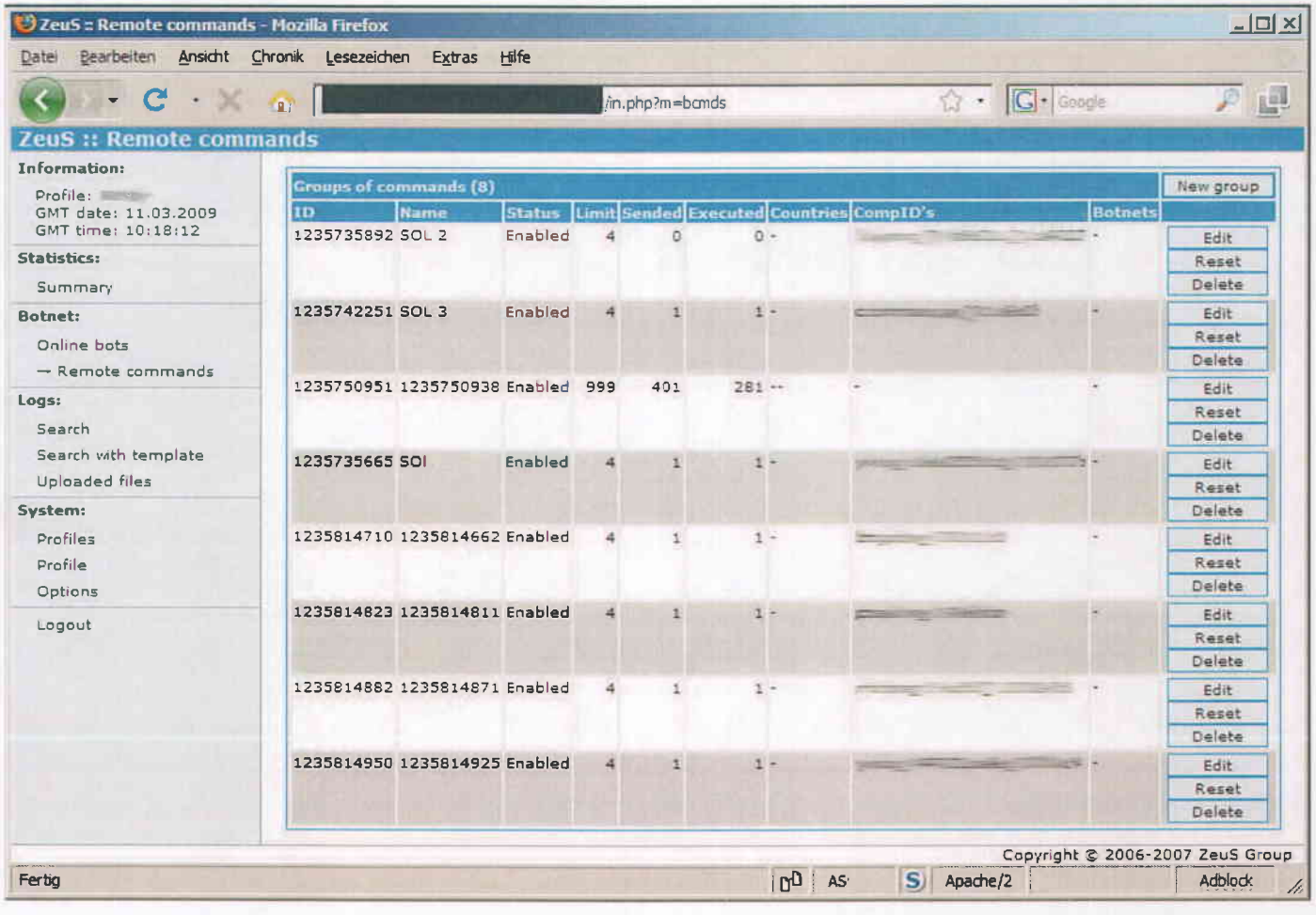


Figure 1. Remote Commands Tab

Statistics and logs

Zeus provides statistics like the total bot count and total logs in the database. A cybercriminal can also search the logs using specified strings, log type, or a time range. For example, Zeus lets a cybercriminal search for FTP or HTTPS credentials captured on a specific date. The Trojan can steal credentials for online bank accounts from HTTPS connections and protected storage.

6-"New Banking Trojan Horses Gain Polish," Robert Vamosi, Computerworld, November 25, 2009

Advanced controls

Zeus also lets hackers arrange infected PCs into groups. For instance, a hacker can group all the PCs with fast Internet connections together for a high performance botnet. The Remote Commands Tab shown in Figure 1 lets cybercriminals define commands for an entire botnet, bots from a certain country, or just a single computer.

Sophisticated backdoor

With the Screenshot function, a fraudster can get a screenshot of each infected system currently online. The Zeus Trojan installs a backdoor, which creates a SOCKS proxy and a Web proxy on the infected system. Fraudsters can use these proxies to hide their identities while they access victims' online bank accounts to steal money. Figure 2 shows that by clicking on a proxy, the fraudster can get useful information about the proxy (for example, on which port the proxy is installed or whether the proxy is already being used or not).

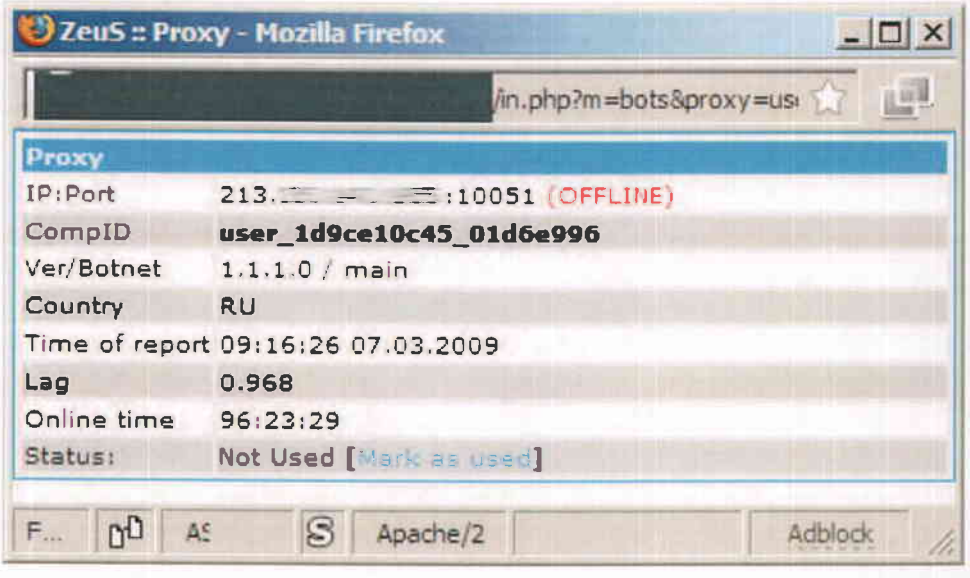


Figure 2. Proxy Information for an Infected Machine

Extensive command list

Zeus includes more than a dozen different commands to enable hackers to control infected PCs. For instance, a command can be executed to make an infected client download additional malicious code as shown in Figure 3.

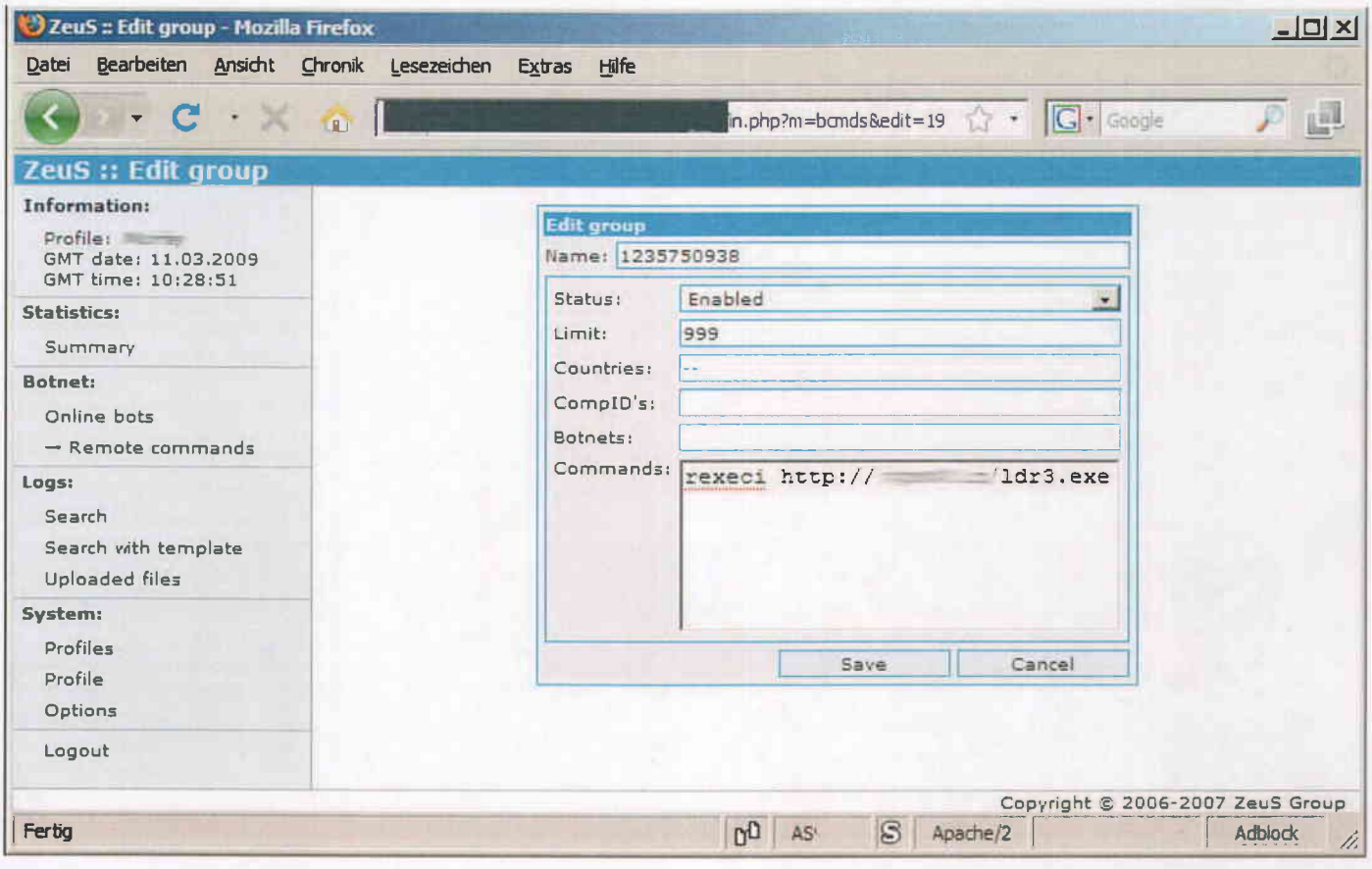


Figure 3. Remote Command to Download More Malware

Detecting and preventing trojan-assisted fraud

Using Zeus or other banking Trojans, cybercriminals can bypass many of today's standard security mechanisms. That's why a layered security defense is critical: no one security component is failproof against every possible threat. It takes a multilayer strategy to defend against sophisticated fraud attempts.

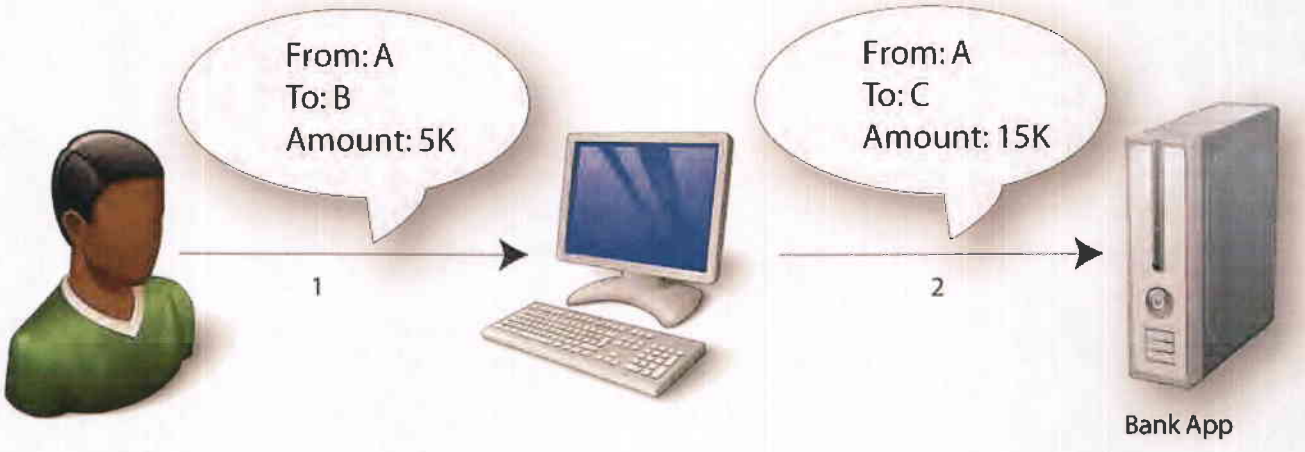
By layering technology such as two-factor, or strong, authentication and fraud detection, financial services companies can better protect themselves and their customers. For instance, some cybercriminals don't have the wherewithal to mount a Zeus scam. It takes technical know-how, resources, and time to execute a real-time Trojan attack. For this reason, two-factor authentication (2FA) is particularly effective at preventing many fraud attempts. However, comprehensive fraud detection is needed to stop more sophisticated attempts originating from Trojans.

Using transaction monitoring and applying transaction verification processes, a comprehensive fraud detection system can detect a suspicious transaction that is out of profile for the legitimate user or that includes risky fraud patterns. For instance: a fraudster uses Zeus, accesses a victim's online banking account, and transfers money to a money mule. Since this is probably the first time money is transferred to the money mule's account, the fraud detection system flags this transaction as suspicious. Out-of-band (OOB) transaction verification can then stop the fraudster by contacting the legitimate account owner offline to confirm the transaction.

The more clever criminals may try to thwart detection by attempting multiple, low-value transactions to several money mules. This is a known fraud technique to avoid the value limit applied by many banks. The fraud detection system can and should be configured to detect such a scenario, creating an alert (OOB challenge), and stopping the scheme.

To illustrate the effectiveness of a sophisticated fraud detection system, consider the following scenarios: a transfer with a Trojan-infected PC where the bank has no fraud detection system and a transfer with a Trojan-infected PC where the financial institution is using a fraud detection system.

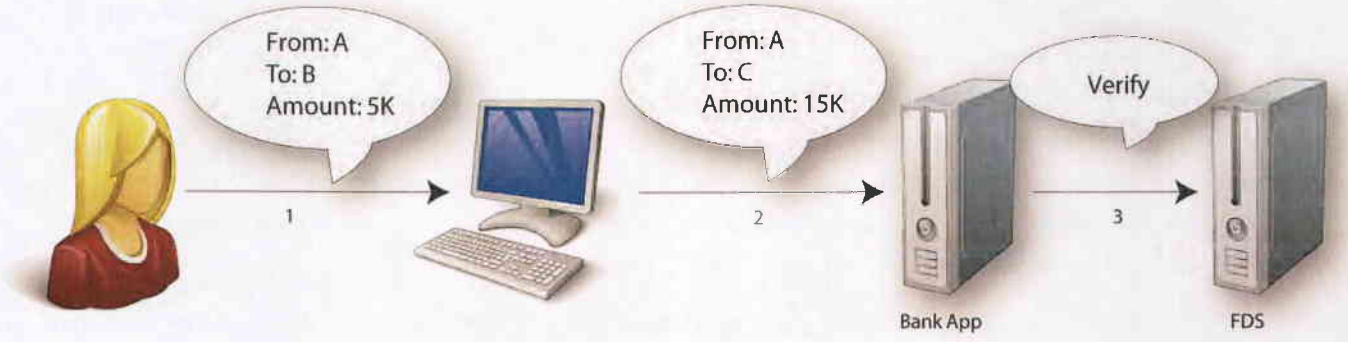
Scenario A: Money transfer flow with a Trojan-infected PC - no fraud detection



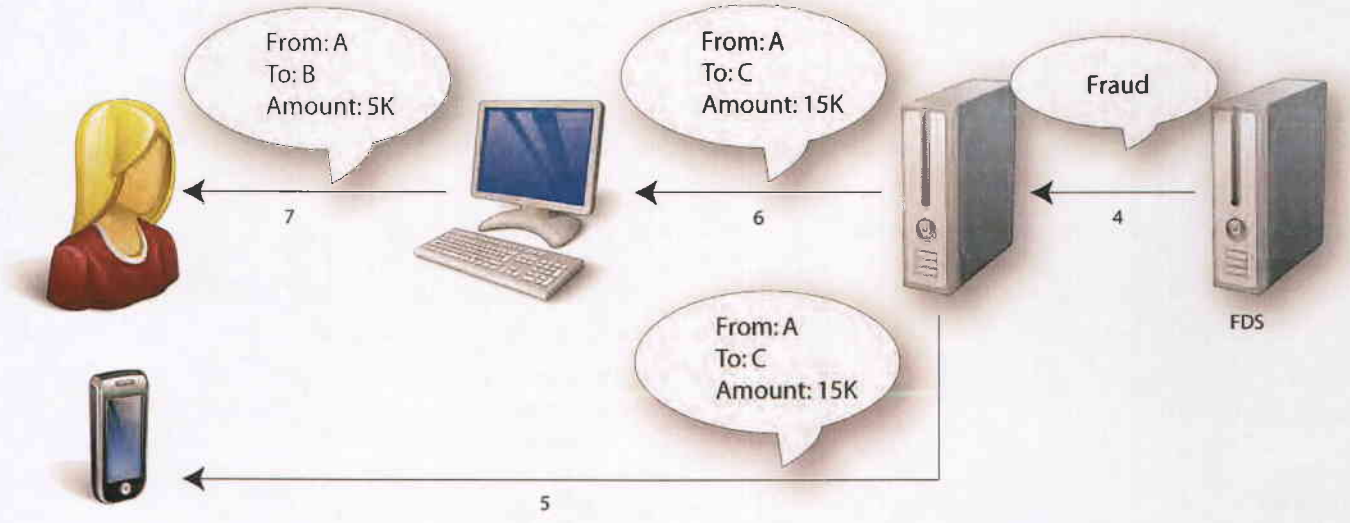
- The user wants to transfer $5,000 from account A to account B
- The Trojan alters the request to move a different amount to a different account

- The bank application asks the user to confirm the transaction request after validating it
- The Trojan alters the response from the bank so that it reflects the original details and appears legitimate to the end user, who confirms the order

Scenario B: Money transfer flow with a Trojan-infected PC - with fraud detection



- The user wants to transfer $5,000 from account A to account B
- The Trojan alters the request to move a different amount to a different account
- The bank application verifies the transaction against the fraud detection system



- The fraud detection system identifies the transaction as suspicious
- The bank application sends an SMS to the customer (alternatively, automated voice calling can be used) with the transaction details as recorded by the bank application together with a one-time password
- The bank application asks the user to confirm the transaction with the one-time password as it appears in the SMS text message
- The customer sees information in the confirmation request screen that doesn't match the information in the SMS text message and doesn't enter the code. The transaction is not completed and fraud is thwarted

A multilayer security solution from Symantec

With the Symantec layered security approach, our state-of-the-art security products and services, such as fraud detection and strong authentication, complement each other to create a solution that is even stronger than the sum of its parts. Symantec provides financial services organizations with not only the means to protect against identity theft and fraud, but also the opportunity to reinforce consumer

trust at the same time. These layered security solutions empower companies to make security protection conspicuous while deploying sophisticated fraud detection and prevention capabilities in the background.

Detecting and protecting against fraud

VeriSign® Identity Protection Fraud Detection Service works in real-time for detecting and preventing identify theft and transaction fraud, providing effective protection against cybercriminals using banking Trojans. Combining complex business logic with advanced machine learning techniques, Fraud Detection Service provides an efficient and robust transaction monitoring solution to block criminal acts attempted with stolen identities. Behavioral patterns, including machine fingerprints, are learned for each user based upon previous legitimate activity, while anomalous actions are detected and reported as suspicious.

Business rules are also applied for identifying high-risk characteristics and scenarios. When the risk score exceeds a predefined threshold, the user is challenged and required to pass a higher level of authentication. With OOB verification, a fraud attempt can be effectively halted.

For financial institutions and other account holders, Fraud Detection Service includes modules that monitor the three most sensitive events for these businesses: log on, trading, and money transfer. All three of these modules identify suspicious scenarios related to deceptive entries into the system, unauthorized money movements, and criminal scams. And particularly important when it comes to real-time Trojan attacks, Fraud Detection Service has the capacity to process more than a thousand transactions per second to detect anomalies in real time.

Protecting identity with two-factor authentication

Symantec™ Validation and ID Protection Service (VIP) is a cloud-based, two-factor authentication (2FA) service that protects enterprises and users from unauthorized account access—above and beyond simple user name and password—with an additional factor of authentication. Symantec VIP cloud-based service is hosted by Symantec, and users can choose from a variety of supported 2FA credentials, ranging from security hardware tokens to software-generated credentials to SMS and voice for OOB authentication.

Using Symantec VIP OOB authentication features, banks can defeat man-in-the-middle and man-in-the-browser attacks. Simple, automated voice call or SMS messages can be delivered on devices customers typically carry. Symantec VIP is easy to deploy and integrates with existing infrastructure. Symantec VIP OOB authentication is highly customizable, with templates that fit current workflows, and custom prompts that can be integrated with a bank's brand.

Conclusion

As this paper has shown, banking Trojans are formidable threats. But there is a way to defend against these and other forms of cybercrime attempts: with a layered security solution that includes a fraud detection system designed to recognize and prevent fraudulent transactions. Symantec VIP Authentication Service and VeriSign® Identity Protection Fraud Detection Service deliver the superior fraud prevention and detection that banks and other financial institutions need to protect themselves and their customers. As part of a comprehensive suite of identity protection and authentication services, Symantec delivers the multilayer security needed to help thwart today's and tomorrow's cybercriminals.

EMC²
where information lives®

EMC CORPORATION

EMC Corporation is the world's leading developer and provider of information infrastructure technology and solutions that enable organizations of all sizes and in every industry, in the public and private sectors to transform the way they compete and create value from their information. EMC offerings expand from systems to software to services and solutions. EMC help customers design, build, and manage intelligent, flexible, and secure information infrastructures.

EMC Solutions range from Automating Data Centers, Backup, Recovery and Archiving, Business Continuity, Compliance and Information Security as well as Infrastructure Consolidation and Optimization and Information Infrastructure Virtualization.

EMC Banking solutions target customer centricity, risk management and compliance, and business and IT efficiencies. The company's solutions allow users to drive down costs, improve time to market, increase revenue generation, and address regulatory requirements. As a strategic global advisor to the industry, EMC provides banking institutions with market-leading expertise.

The company provides specific solutions for Loan Orginiation as well as Payment Electronification. These solutions build upon EMC's information management and hardware and software offerings and address two of today's most important banking applications: reducing time-to-market and operating costs while increasing revenue and customer service.

EMC is represented by more than 400 sales offices and distribution partners in more than 60 countries. As part of EMC's commitment to the local markets around the world, EMC continues to open offices in different countries to better serve its customers and enable their technology resellers. In the region of Turkey, Emerging Africa & Middle East region EMC has offices in Turkey, KSA, Egypt, Pakistan and Nigeria, Kenya and Qatar with the headquarter located in UAE.

EMC CONSULTING-MOBILE BANKING

Building Customer Loyalty

ESSENTIALS

The Banking practice offers mobile solutions that enable financial institutions to:

- Increase customer loyalty
- Increase fee income from transactional services
- Reduce the technology costs of sales and service delivery
- Increase the effectiveness of targeted marketing
- Reduced operations costs
- Increased security & reduced fraud exposure

The Banking Practice is part of EMC® Consulting's Financial Services Industry Consulting Practice. Its purpose is to help banking executives address the variety of complex and rapidly evolving business, regulatory and IT challenges of the banking and financial services industry.

INDUSTRY TRENDS AND CHALLENGES

The growth of mobile banking and payments capabilities are one of the most significant retail banking trends. Mobile banking services give organizations the ability to differentiate the bank's services and build customer loyalty. The rapid development of mobile capabilities is described by the following trends:

- Channel convergence. Rapid increase of tablet devices is based in part on their ability to combine the best of desktop and hand held device applications. As such they represent the potential point of convergence for banking desktops, online banking and mobile banking applications creating, de facto, a consistent experience and dramatically simplify underlying technical architectures and reducing technology costs. Even in scenarios where traditional channel applications are not replaced, mobile applications will interact seamless with these capabilities enhancing the customer experience.
- LOB convergence. Increasingly banking, brokerage, payment applications will exist on the same mobile device. Customers will expect that applications provided by the same institution will behave seamlessly, not just in terms of view of look and feel, what also from the perspective of consistent representation of data and the ability to move money from one LOB or one application to another.
- Banking application and other mobile application convergence. Increasingly banking applications need to participate seamlessly with other mobile applications. Presence on social networking sites, context aware advertizing, integrated transaction fulfillment or payment services are examples of the move from a traditional online banking experience to an experience where digital banking capabilities logical complement other applications in the digital experience
- Mobile payments and transactional services. The movement toward mobile payments is one of the most dramatic examples of the integration of banking and other digital applications. Mobile payments take many forms including device initiated credit and debit transactions, digital wallet transactions, and peer to peer payments. This movement continues to develop quickly and poses substantial risk as well as opportunity to existing payment models.

- Data monetization. Closely aligned with digital application convergence and mobile payments is the trend toward data monetization. Organizations have long seen the potential to more accurately profile customer behaviors using electronic transactional data to improve targeted marketing. Increased levels of digital shopping and transactions increase this potential. New data technologies for capturing and analyzing transaction data that exists within and within the organization make this capability increasing feasible.

EMC CONSULTING SOLUTIONS

EMC mobile banking and payments solutions are based on a combination of EMC strategy, user design, application development, data management and information security solutions. EMC's approach to mobile solutions is based upon an open architecture that allows full participation of banking services with other financial service LOB's and other applications that exist in the mobile digital environment. Capabilities include:

- Strategy and roadmaps. EMC Consulting helps clients develop a mobile strategy that provides robust multi-channel solutions for clients to understand consumer activity, while helping to improve ROI by targeting customers more effectively. Mobile advisory services guide the mobile journey by completing the following: a business opportunity matrix, mobility use cases, mobility reference architecture, mobility readiness, a vision for cloud enabled mobility and, an integrated roadmap recommended next steps.

- User experience improvement. EMC helps clients drive revenue growth by increasing the quality and effectiveness of the customer sales and service experience. User experience improvement is achieved through world-class, user-centered design capabilities; process improvements addressing product origination and funding, and service enrollment and activation; desktop application rationalization and integration; and experience architecture design providing a consistent experience across all channels: branch, call center, ATM, online bank, mobile and social.

- Application development. EMC assists clients to develop native, open mobile applications that participate seamless with traditional banking application channels and emerging mobile applications and payment capabilities. EMC provides an application development and integration framework based on VMware that can reduce application development time and facilitate flexible integration with other applications to support fulfillment, transaction initiation and money movement activities.

- Data solutions. EMC provides strategy and roadmap, architecture and system development solutions for data monetization and customer profiling. EMC's Banking and Enterprise Information Management practice have solutions that can aggregate data from internal systems and from the internet and provide targeted marketing recommendations in near real time enabling offers to occur in context with other mobile / digital activity.

- Information security. EMC Consulting offers multi channel information security solutions based on the EMC RSA family of products. Information security solutions include governance, adaptive authentication, security monitoring and alerting capabilities. The current version of RSA Mobile SDK provides mobile channel protection and the already announced next version of RSA mobile will include automatic channel detection and location awareness features.

- Application rationalization and virtualization. EMC Consulting supports delivery channel convergence with its application architecture and development solutions. Applications virtualization can enable the use of a single application architecture stack to support the different form factors required by different channels (screen size) and devices (phone, tablets, laptops, etc.). Application convergence can increase business agility and leverage existing application investments while reducing costs through reduction of development, maintenance, management and operation costs.

WHAT MAKES EMC CONSULTING UNIQUE IN THE INDUSTRY?

EMC consultants average 15+ years of experience in the industry before consulting to the industry. Our expertise spans everything from in-depth industry business knowledge to world-class technical skills. We focus on asset-based consulting, delivering a blend of industry-specific solutions and service offerings, to help our clients achieve their business and IT transformation objectives. EMC Consulting has supported the complete transformation lifecycle for a number of the world's largest banks, brokerages and diversified financial services firms - supporting the 10 largest global banks and 5 of the 6 largest global financial data services companies in the Fortune 100. We accelerate our client's initiatives through a combination of tools, technologies and proven methodologies.

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/consulting

LET EMC CONSULTING HELP YOU REALIZE YOUR AMBITIONS

As part of EMC Corporation – the world's leading developer and provider of information infrastructure technology and solutions – EMC Consulting provides strategic guidance and technology expertise to help organizations exploit information to its maximum potential. With deep industry insight, EMC Consulting guides and delivers innovative and proactive thinking to help clients unlock the value of their information and accelerate IT transformation. EMC Consulting drives execution for clients, including more than half of the Global Fortune 500 companies, to transform information into actionable strategies and tangible business results.

EMC²

INFORMATICA®
The Data Integration Company™

INFORMATICA CORPORATION

Informatica is the world's number one independent leader in data integration software. With Informatica, thousands of organizations around the world gain a competitive advantage in the global information economy with timely, relevant and trustworthy data for their top business imperatives.

The company has had great success in business to business banking operations. Seventy percent of the top 10 global banks use Informatica for payments infrastructure. Incoming data comes from a variety of sources which complicates data management. Data is also often inconsistent and suspicious. Informatica solutions support data in many formats and with disparate interfaces. This reduces the cost of supporting multiple payment formats by 50 percent or more. Informatica solutions support structured, semi-structured, and unstructured files, both in real-time and in batches. The company's products identify, separate and investigate suspicious payments. They are able to visualize relationships between payee records and prohibited lists across all sources. The solutions will correlate payments and different sources of data. It can identify quality issues, as well as potentially fraudulent behavior.

Informatica also offers payments processing and compliance monitoring solutions. Banks are challenged with screening large batches of payments for a few suspicious items, therefore blocking significant transaction volume. Backlogs in payment review often exceed three days, incurring interest costs paid to customers. Informatica's payment infrastructure offers management and monitored layering of payments. The solutions manage payments through the management stage. As a consequence, payment processing is reduced from three days to four hours. Manual inspection effectiveness is increased, and service level agreement (SLA) escalations are reduced by 90 percent. Informatica has had a partnership with Society for Worldwide Interbank Financial Telecommunication (SWIFT) since 2001. The company holds SWIFT certification, and company solutions support SWIFT messaging.

Informatica has more than 700 customers in financial services, with 34 out of the top 50 global banks being customers. In addition, 17 out of the top 20 U.S. bank holding companies are clients. The Informatica platform offers governance, risk and compliance solutions, including a Basel-compliant data warehouse to integrate credit, market and operational risk data for Basel reporting. For the European Central Bank, the warehouse delivered a return on investment (ROI) within one year and improved customer satisfaction by providing a common integration platform for data integration and delivery. The enterprise data warehouse reduced development costs by 75 percent for the Reserve Bank of India and streamlined data collection from months to one day by replacing hand coded processes, which allowed officials to monitor and analyze macro-economic trends.

INFORMATICA

BROCHURE

Informatica SWIFT Alliance Gateway Solution

Delivering Faster, Better Integration for High – Value SWIFT Alliance Gateway Adoption

SWIFT Ready Application Messaging Data Services 2010

BENEFITS:

- Transform complex data into a SWIFT-compliant format and vice-versa
- Keep up to speed with changes to the SWIFT standard
- Make complex data available to consuming applications cost-effectively

Informatica SWIFT Alliance Gateway Solution is based on Informatica B2B Data Transformation, enterprise software for complex-data transformation, and enables SWIFT gateway providers to help their clients reduce time, complexity, and costs for SWIFT Alliance Gateway operations and communications.

The Solution Provides Three Main Components

- Informatica Data Transformation Studio, an Eclipse-based visual development environment that enables IT personnel to define and deploy complex data transformations without the exorbitant time and cost of custom development;
- Informatica Data Transformation Engine, an embedded run-time engine that provides high-throughput execution across a wide range of infrastructure platforms and applications;
- Informatica Data Transformation Library for SWIFT, a comprehensive library of pre-built
- SWIFT transformations that enables all types of SWIFT message formats to be created or parsed automatically.

Together, these integrated components power a solution for accessing complex data from any source, from legacy to unstructured or semi-structured content; transforming it into a SWIFT-compliant format and vice-versa; and making it available to consuming applications cost-effectively.

The SWIFT Standard and the Integration Challenge

Financial institutions worldwide are looking for ways to advance interbank communications and straight through processing (STP) of their pre- and post-trade execution and cash management data to save costs, reduce operational risks, and improve customer service. While the SWIFT standard plays a vital role in such efforts, its full and effective adoption can be a complex and challenging process. To help their customers achieve true STP, SWIFT Alliance Gateway providers need to deliver solutions than allow the efficient integration of SWIFT messages into proprietary applications and back-office legacy interfaces, while remaining current with the latest SWIFT messaging standards.

SWIFT Standard Evolution and Migration

With new updates introduced each year, SWIFT Alliance Gateway providers face a constant challenge maintaining compliance as the SWIFT messaging standard evolves. This challenge will continue to grow with the migration to ISO 20022 (also known as ISO 15022 XML and ISO 15022 Second Edition), a common platform for the development of messages in a standardized XML syntax. SWIFT will use ISO 20022 for new work in funds management and for new products and services, while continuing to maintain ISO 15022 in the short term for post-trade activities. For gateway providers and clients alike, this migration introduces new complex data integration issues that will slow adoption, cause spikes in ongoing communications, and increase operational costs.

CHALLENGE

A regional German bank needed to be able to handle additional extensions of the ISO15022 standard. The Bank's SWIFT Alliance Gateway provider turned to Informatica.

Requirements

- Integrate with an existing real-time risk management application framework with a Microsoft® Excel front-end
- Parse and validate message files of up to 50Mb at a time
- Generate Excel files containing a subset of message data within minutes

Solution

- Use Informatica Data Transformation Studio to filter the base ISO15022 MT536 data definition to adhere to application specifications
- Use Informatica B2B Data Transformation to generate an Excel file representing the modified MT536 structure
- Create, test and deploy two Informatica B2B Data Transformation transformations: one to parse MT536 structure, and a second to serialize this structure into Excel
- Deploy the resulting Informatica B2B Data Transformation transformations to the bank's existing SWIFT Alliance Gateway infrastructure

Outcome

- The bank gained the ability to parse and validate incoming file-based MT536 data, filter the needed data, and write it directly into the Excel file used by their risk management application framework
- With end-to-end processing time for statement messages measured in tens of milliseconds, even the largest daily files could be processed in minutes

SWIFT Message Integration with Middleware and Back-Office Systems

For member banks and other financial institutions, the integration of existing systems to SWIFTNET and the conversion of other data standards can consume a disproportionate share of operational costs. For SWIFT Alliance Gateway providers, integration with a customer's back-end processing systems poses an initial barrier to customer adoption, and leads to unnecessarily high costs over time as the provider must maintain multiple proprietary interfaces across its customer base.

Lowering the Cost and Speeding Deployment of SWIFT Alliance Gateways

The Informatica SWIFT Alliance Gateway Solution offers SWIFT Alliance Gateway providers a pre-built, comprehensive SWIFT transformation library combined with Informatica B2B Data Transformation, the leading software for complex data transformation. Gateway customers can access complex data from any source – from legacy to unstructured or semi-structured content – transform it into a SWIFT-compliant format and vice-versa; and make it available to systems throughout the organization.

Informatica B2B Data Transformation, the industry-leading software for complex data transformation, includes three software components: Informatica Data Transformation Studio, an easy-to-use graphical user interface that automates the creation of complex data transformations; Informatica Data Transformation Engine, an embedded run-time engine for executing transformations across all leading middleware platforms in real-time, and provides comprehensive and flexible event logging and reporting; Informatica Data Transformation Libraries, a comprehensive library of pre-built transformations that address an array of industry standards. The result is rapid development and deployment of complex data transformations and a significant lower cost of ownership from traditional approaches.

Competitive Differentiation for Gateway Providers – Greater SWIFT Benefits for Their Customers

The value of the Informatica SWIFT Alliance Gateway Solution is extended through the Informatica SWIFT transformation library. Unique in the complex data transformation marketplace, this comprehensive set of pre-defined transformations enables SWIFT Alliance Gateway providers to improve competitive differentiation, reduce the cost of on-boarding new customers, and expand their services by quickly adding new formats to the gateway.

Financial institutions, in turn, benefit through the reduced cost and risk of adopting the SWIFT Alliance Gateway Solution as well as faster time-to-deployment. Informatica's SWIFT transformation library, coupled with Informatica B2B Data Tranformation's visual development environment, facilitates the rapid deployment of any-to-any transformations between the SWIFT Alliance Gateway and existing systems. Over time, the Informatica solution lowers operational costs for gateway customers by simplifying and automating complex data transformations.

By offering the Informatica solution as part of their SWIFT Alliance Gateway offering, gateway providers can enable their customers to:

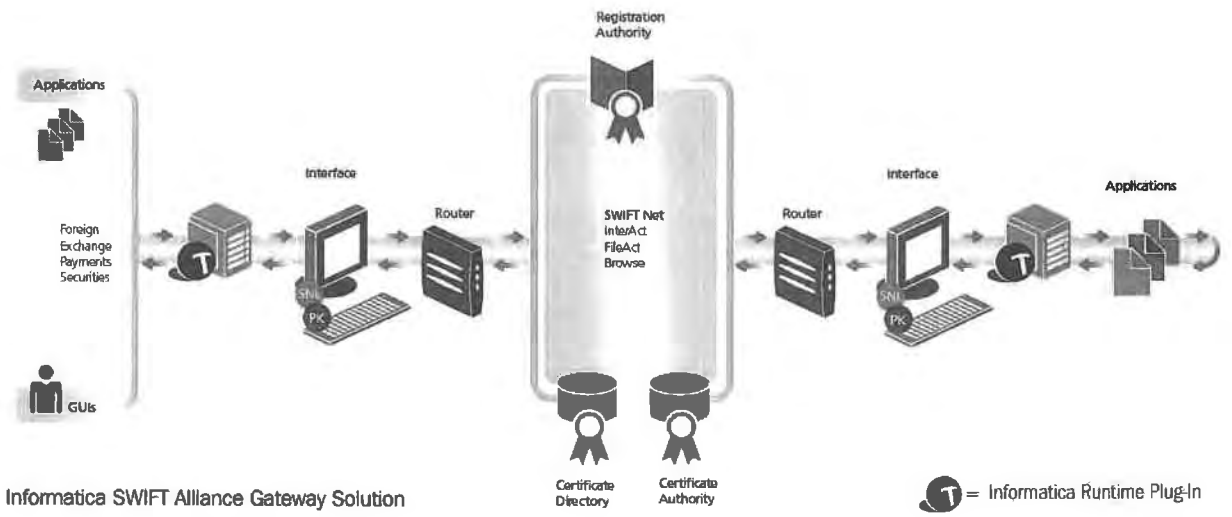
- Integrate SWIFT Alliance Gateways with legacy applications and extend SWIFT adoption benefits throughout the organization.
- Transform outbound messages based on internal and proprietary data formats to comply with SWIFT, enabling faster and more cost-effective communications with partners.
- Transform data between different versions of SWIFT, significantly simplifying migration as new versions of the standard are introduced.
- Transform incoming funds transfer requests from Excel, Word, or PDF into valid SWIFT messages, while enabling STP.
- Streamline integration between internal systems and third party providers such as credit agencies, funds providers, appraisal services, and servicing systems to reduce processing costs while speeding transactions.
- Offer additional services to counterparties, such as moving services from third-party providers to in house solutions, allowing the customers to further leverage SWIFTNet, reduce dependencies on multiple providers, and lower operations and communications costs.

A Flexible Software Solution for Cost-Effective Integration Enterprise-Wide

As a highly efficient, embeddable execution environment, the Informatica SWIFT Alliance Gateway Solution gives SWIFT Alliance Gateway providers a single platform for developing repeatable and maintainable transformations for each client engagement. The solution's small footprint allows it to be plugged into SWIFT Alliance Gateway software as an embedded component and provides out-of-the-box integration between SWIFT and a broad range of complex data formats. Transformations can be maintained easily with Informatica Data Transformation Studio, which enables quick debugging and updating as changes occur, significantly reducing projects costs and increasing developer productivity. Gateway providers can also use the Informatica solution to cost-effectively expand their service offerings to include consumer payments and a range of other offerings that address other data types.

Informatica B2B Data Transformation leverages existing IT infrastructure as an add-on to all major middleware platforms, including:

- Informatica PowerCenter
- Native OS environments
- IBM WebSphere
- Oracle Fusion Middleware
- J2EE Applications
- SAP NetWeaver
- Microsoft BizTalk
- webMethods
- Microsoft .NET



Informatica SWIFT Alliance Gateway Solution

JUNIPER NETWORKS

Juniper Networks has modernized financial services solutions to offer a receptive and secure environment for managing high-volume transactions and relations contingent upon a lower cost arrangement. Juniper solutions maintain client loyalty incentives that depend on improved employee efficiency, assist in ensuring risk management and regulatory compliance, sustain revenue expansion and profitability with new service offerings, and reduce both capital and operating expenditures. Juniper's finance service network solutions maximize and increase application delivery, safeguard people, privacy, and assets, speed up service deployment, maximize branch locations and simplify operations.

Juniper Networks works with financial institutions worldwide to implement changes in their networks, as required by business initiatives. The company's foundation for secure and assured networking is the Enterprise Infranet, an IP infrastructure that controls traffic across the entire network by coordinating network, application, and endpoint intelligence. Enterprise Infranets operate as a service layer on top of the existing infrastructure, meeting new business requirements while preserving prior network investments.

Retail Banking
Retail banks provide customers with an essential physical presence to an increasingly virtual world. To be effective in this role, branches must optimize available WAN links to enable a broader range of applications, leverage existing core systems, and share people and other resources. The WAN Acceleration platform integrates key WAN application performance technologies to address bandwidth, latency, and contention issues, ensuring optimal application flows.

IP Telephony
Juniper Networks secure and assured voice networking offers predictable service quality, high availability, pervasive security, and flexible deployment support - all of which financial enterprises need to effectively deploy IP telephony. By pairing Juniper Networks routing and security appliances with their preferred IP PBX, financial institutions can deploy best-in-class voice and networking solutions and benefit from the broadest selection of voice features.

HIGH-PERFORMANCE NETWORKING SOLUTIONS FOR FINANCIAL SERVICES

Flawless and Consistent Execution with Juniper Networks' Service Enabling Solution Suite

Challenge

In financial services, security and privacy are essential. At the same time, computerized trading and service offerings have made transaction speed increasingly important in order to compete with fortunes literally gained or lost based on microsecond order execution.

Solution

Juniper offers a variety of products to help financial services organizations excel in today's highly volatile and competitive market. These solutions combine products that work together to create a consistent user experience, unparalleled security, and a greatly simplified and consistent IT approach to the business.

Benefits

- Greatly simplified data center operations with significantly reduced latency
- Speed and consistency, from the data center to the remote user
- Inter and intra center redundancy and fallover for seamless operations regardless of external conditions
- Cooperative security in the network by the network
- Flexibility, lower TCO, and future-proofing of the network

Today's financial services institutions face enormous challenges. First and foremost, they must comply with a number of different regulations designed to ensure security and privacy of customer transactions and financial data. Because customers themselves as well as core business operations are often affected by a security breach, a violated organization can lose its reputation overnight, and this can directly affect the viability of the business. This was the case earlier this year when Heartland Payment Systems (HPY)1 disclosed that intruders had hacked into the computers it uses to process 100 million payment card transactions per month for 175,000 merchants. In this kind of high risk environment, IT infrastructures that maintain security and privacy are virtually "table stakes" in today's financial services industry.

Financial services must also address unique requirements around the speed and efficiency of their networks. Latency and network downtime are perhaps more costly in this industry than in any other. To maintain a competitive edge and meet order execution requirements that have moved from milliseconds to microseconds, financial organizations are streamlining infrastructure and are looking for ways to reduce latency wherever possible. Disparate network management systems and multiple operating systems can add needless complexity and contribute to high operating and management costs, thus resulting in undesirable or even insurmountable limitations on the business.

These factors combine to create an environment where the network is far more than just a means of connectivity. It can be a significant asset or a disastrous liability. Juniper Networks® can help you make the most of your network with a suite of cooperative products that provide high performance and low latency, streamlining and securing infrastructure while maintaining operational efficiency. And, Juniper's solutions can be deployed incrementally, eliminating the requirement for forklift upgrades or disruptive network changes. This increases agility, performance, and security for the financial services institution while reducing costs.

The Challenge

Today's financial services institutions, including exchanges, brokerage houses, and banking services, face enormous hurdles. Data security and privacy are mandated by a host of regulations that include Basel II, Gramm Leach Bliley, Payment Card Industry Data Security Standard (PCI DSS), Sarbanes Oxley (SOX), Markets in Financial Instruments Directive (MiFID), and Regulation NMS to name a few. Meeting these regulations is not just a matter of compliance; providing security and privacy can make or break a business, since financial services companies are among the industries that lose the most customers after a data breach, estimated to be about 5.5 percent. And because the threat environment is constantly evolving, financial institutions must remain one step ahead.

Financial services must also contend with unique needs related to the speed and efficiency of their networks. Not only is network downtime unacceptable, mere latency can dramatically affect the bottom line as well, especially in those segments that are principally concerned with market transactions. In these businesses, almost by definition, information delayed is money lost. In the trading world, for example, a transaction could result in the purchase of thousands of shares, and missing it by just nanoseconds can cost huge amounts of money for buyer or seller. A 1-millisecond advantage in trading applications can be worth $100 million a year to a major brokerage firm, by one estimate.

These requirements have led financial services organizations to consolidate, reduce latency, and streamline operations wherever possible. Nowhere is this requirement as evident as in the data center, where years of force fitting campus switches into service has created multiple tiers of devices, each of which adds latency and complexity. In order to innovate while retaining high availability, today's financial services organization must accelerate consolidation, optimization, and virtualization initiatives to stay ahead. At the same time, financial services enterprises must remain flexible and broadly compatible, in order to seamlessly roll out new applications and resources.

Financial services, like most enterprises, also face a growth in branch office and remote computing. These organizations may directly service customers and are often the "storefront" to the outside world. As a result, all locations must exhibit "LAN-like" performance and retain optimal and consistent performance regardless of physical location. At the same time, enterprises must build operational consistency into their networks in order to provide end-to-end security as well as lower total cost of ownership (TCO).

The Juniper Networks Financial Services Solutions

Juniper's innovative financial services solutions deliver products that work together and also work with other standards-based products throughout the network to help you realize an infrastructure that is:

- High-performance, featuring unified switching and routing platforms that extend from the branch to the core
- Operationally streamlined, cutting through server sprawl with optimized, virtual platforms
- Threat resistant, with a portfolio of products that can dynamically adapt to changing network conditions
- Consistent in architecture and management, thereby lowering your TCO
- Agile, enabling you to roll out new products and services

Juniper's offerings consistently address all locations of the financial services deployment, from the data center to the campus, from the branch office to the remote user. Product portfolios are designed to interoperate and to provide a consistent experience from location to location. Juniper's market leading switches and routers collapse antiquated architectures and add virtualization, lowering TCO as they speed performance. Juniper's security solutions are built to cooperate with each other as well as with other standards-based offerings, and are available in modular data center/campus form factors that you can add to as you grow, or in integrated platforms that provide the branch/remote office with a host of functionality in one appliance. Juniper's products can be managed through a single pane of glass using Juniper Networks Network and Security Manager. Overall network visibility is provided with the Juniper Networks STRM Series Security Threat Response Managers and Junos® operating system, which ties together routing, switching, and security devices.

Speed and Consistency, from the Data Center to the Remote User

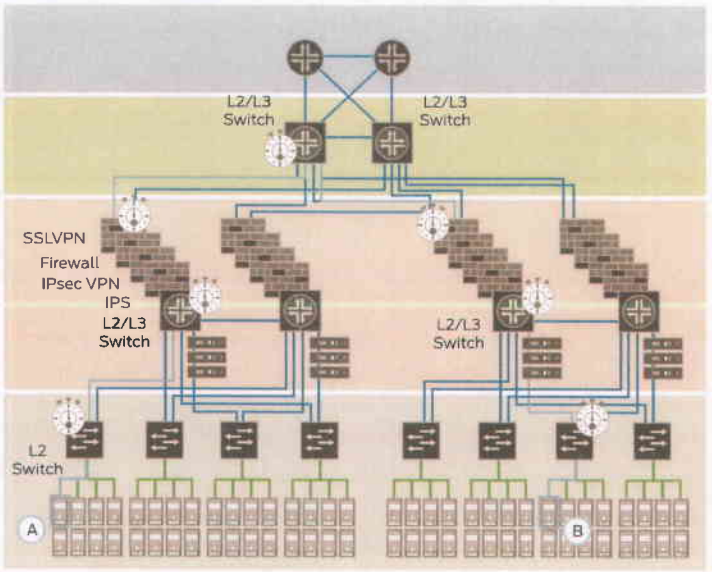
Juniper's financial services solutions begin in the data center, where architectures are perhaps the most complicated. Switches intended for the campus LAN have often been pressed into service in the data center, resulting in three tiers of devices at the access layer, the aggregation layer, and the core. In some cases, there is even an extra distribution layer. It is not uncommon to have a different operating system in each of these layers, making the overall deployment expensive and cumbersome to manage. The access tier serves as the direct interface to servers, and is typically deployed as top of rack or end of row switches connecting servers deployed in racks. Multiple uplinks from the access layer

interconnect to the aggregation layer. The aggregation layer is required due to the large number of uplinks from the access layer, which is generally a larger number than can be supported by devices within the core of the data center.

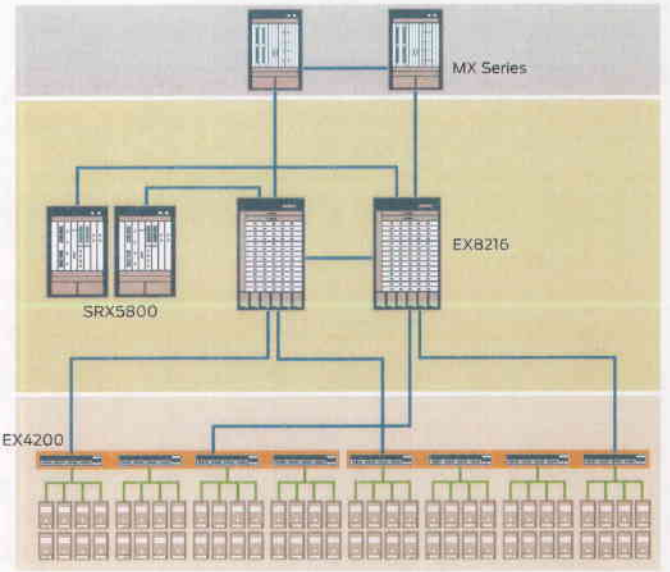
Racks can be consolidated in either end of row or top of rack switch configurations. Unfortunately, these end of row and aggregation switches were originally built for campus environments and can present several limitations in this use case, including Forwarding Engine, Routing Engine, and their switch fabric. This means that oversubscription corner cases are unpredictable and you can't provision a new application with confidence. Meanwhile, in order to transit the network, data must go throughout the entire tiered infrastructure to reach its destination, which results in increasingly unacceptable latency in the network. Security is an afterthought, and often provisioned via a disparate mix of security blades across the aggregation layer. Not only does this take up space and power, but it represents yet another management/operating system that IT staff must master. To be successful in today's marketplace, financial services institutions need to virtualize the access layer and collapse the core and aggregation layers, while consolidating and virtualizing security appliances.

Juniper has the answer with a complete line of Juniper Networks EX Series Ethernet Switches. The Juniper Networks EX4200 Ethernet Switch features Virtual Chassis technology, which dramatically reduces latency across racks. In fact, the EX4200 has the lowest latency in its class at 1.96 picoseconds. The EX4200 also reduces the number of uplinks required, and drastically lowers the number of switches you have to manage by up to 10 times, which saves you not only in capital expenses, but in ongoing power, space, and cooling costs. Best of all, the EX4200 enables end of rack chassis features at a top of rack price, and gives you the flexibility to choose the configuration that works best for you. In fact, Virtual Chassis technology can save you up to 33% over a standard configuration.

The EX Series can also help you realize your goal of collapsing the core and aggregation layers. This begins with Juniper's unique Virtual Chassis technology, and carries through to Juniper Networks EX8200 line of Ethernet switches in the core. The EX8200 line features industry leading line rate density, which can serve to collapse the aggregation layer. Not only does this simplify the architecture, but it reduces latency as it decreases your space, power, and cooling requirements. In fact, the Juniper Networks EX8216 Ethernet Switch features massively scalable 12.4 Tbps fabric, 2 billion packets-per-second (pps) line rate performance, and the ability to aggregate as many as 6,000 servers in a single domain.



Before—Server sprawl



After—Optimized network

Replacement of the access and aggregation tiers with EX Series switches results in:

- Management of up to 10 physical EX4200 switches as a single logical device, which drastically cuts down the number of devices being managed.
- Fewer number of uplinks from the access tier, because a low latency, high-performance Virtual Chassis backplane is the preferred mechanism for server-to-server traffic. Access to aggregation interconnections need only serve the traffic in and out of the data center or across networks within the data center.
- No extra cost to use Layer 3 protocols-based connectivity between access and aggregation tiers, unlike competitive products.
- Reduction in the total number of ports required in the aggregation tier—hence requiring fewer switches and fewer switching tiers (fewer switches translate into fewer ports to aggregate by high tiers in the hierarchy).

As you speed up data center traffic, the ability to apply security and policy consistently is vital, since today's blended threats need only a single chink in the armor to spread throughout your network. Juniper delivers, with best-in-class products including Juniper Networks SRX Series Services Gateways. Powered by Junos OS, Juniper's single unified operating system, the SRX Series gateways provide a host of features in a variety of cost-effective platforms that scale. SRX Series for the high end, the fastest firewall in the world, offers functionality that can be added to the platform as your deployment grows. SRX Series for the branch features integrated functionality in right-sized form factors for remote or branch offices.

> The problem with branch offices today is that they have become independent islands of IT. This is the culmination of many years of incremental addition, beginning at a time when the operational overhead of IT and communications at the branch level simply couldn't have been predicted. "Banks today are reinvigorating their business by making the branch a value center that offers a broad range of customer services. It is important to consider the impact these new services may have on IT infrastructure."
>
> Don Free,
> Financial Industry Analyst, Gartner Group

Juniper also has unique capabilities for the remote user, including its market leading Juniper Networks SA Series SSL VPN Appliances. Not only does the SA Series provide secure, role-based access to applications and resources, but it also dynamically provisions Juniper Networks WX Client and antimalware/antispyware at the same time. This gives you the ability to extend your security stance, even to remote, unmanaged devices, while you speed performance.

Consolidate a Highly Available Data Center While Extending Your Reach

In mission critical data center networks, any outage is unacceptable. In financial services institutions, the requirements for high availability go beyond network outages to encompass slowdowns as well, since latency measured in milliseconds can literally sink a business. High availability requirements in the data center are becoming similar to carrier availability requirements. Inter and intra site redundancy is vital in the financial services industry, both to speed performance and to reduce costs. Advanced routing capabilities enhance application performance, security, and availability. Juniper's long experience in creating products to satisfy the world's largest service providers is the foundation for products that make the data center highly available as well as easy to manage and maintain.

High availability in the data center is provided through a number of features, such as those found in Juniper Networks MX Series 3D Universal Edge Routers. The MX Series provides industry leading port density, power savings, performance, and reliability for data center network core and aggregation deployments. High availability begins with Junos OS, Juniper's unified operating system used throughout the entire switching and routing platform. Junos OS separates the forwarding and control planes, and this creates a modular software architecture that is remarkably resilient. This design enables individual processes to restart without bringing down the entire router.

MX Series routers also feature a wealth of powerful features that have been designed specifically for use in large, mission critical networks. Unlike routers from some vendors, Juniper's products feature MPLS that is designed to operate at scale. Virtual private LAN service (VPLS) also extends VLANs, enabling mobility. The MX Series provides unprecedented levels of Layer 2 and Layer 3 scalability, as well as IP multicast, which is frequently not offered in competitive products. With the MX Series, financial services organizations can effectively collapse the core and the WAN edge, resulting in lower capital and operating expenses.

The MX Series, as well as the rest of the Juniper portfolio for the data center, runs over a common operating system with a single management system, accelerating application deployments and leading to improved efficiencies in space, power, cooling, and management. Juniper Networks M Series Multiservice Edge Routers and MX Series 3D Universal Edge Routers at the edge provide high performance, port dense routing and switching functionality without compromise on a single platform.

Enable Flexibility as You Future Proof

In order to remain competitive, today's financial organization must be agile, able to roll out new applications and services quickly and effectively. The number of different management and operating systems running in the average network, however, can make this task almost insurmountable. Juniper's products address this issue in three ways. First, Juniper builds its products around open standards. This enables you to choose the right product for each of your requirements, and avoids the cost and limitations of single vendor lock in. Second, Juniper has built its routing, switching, and security appliances around a single operating system—Junos OS. This means that your IT staff has only one OS to learn, and this saves you money. And, because each release of Junos OS is backwards compatible and the release train is predictable, you never have to worry about upgrading to the latest release. Finally, most Juniper products are managed by Network and Security Manager. This makes it easy to deploy new products or design new policies around a service offering. Best of all, with NSM, you can push a policy throughout your deployment from a single management console. And the STRM Series can unite your entire network, including devices from third-party vendors, to give you a single consolidated view of your deployment.

Security in the Network by the Network

Juniper Networks Adaptive Threat Management Solutions feature a suite of products that are designed to work together cooperatively. Any one of Juniper Networks Adaptive Threat Management Solutions can be deployed as a best-in-class point product on its own—after all, each has consistently been rated among the top devices in its category. But because these devices are designed to work together, they offer benefits that go beyond the unique functionality that each offers individually. The ability to communicate interactively, regardless of location, makes the network work with you to maximize productivity, mitigate risk, and ensure compliance with regulatory statutes.

Adaptive Threat Management Solutions include these products:

- Juniper's suite of firewalls
- SRX Series Services Gateways
- SA Series SSL VPN Appliances
- IC Series Unified Access Control Appliances
- IDP Series Intrusion Detection and Prevention Appliances
- Network and Security Manager
- STRM Series Security Threat Response Managers

See it—Control it

Key among Juniper's offerings are products designed to offer visibility and control, because you cannot control what you cannot see. Juniper offers comprehensive and innovative centralized management, monitoring, and reporting capabilities with its STRM Series devices. The STRM Series not only works with your Juniper devices but with the third-party devices you have already deployed as well, to give you a single "aerial" view of what's going on throughout your network in real time. This gives your IT department the ability to monitor, trend, and report on activities throughout the deployment, as well as to easily meet regulatory compliance with over 1,500 pre-formatted reports. Still more operational simplicity is provided via NSM, the single platform that can provision and update virtually every product in the Juniper Networks portfolio, as well as create and push policies throughout your entire enterprise.

Summary—Meeting Financial Services Challenges with Juniper Networks Solutions (Consistent, highly available and secure across the financial services network)

Juniper Networks innovation in financial services solutions delivers a responsive and trusted environment for handling high volume, time sensitive transactions and interactions based on a lower cost structure. Juniper's solutions help to ensure risk management and regulatory compliance by working together to provide unwavering performance from anywhere in the network. With a Juniper solution, you can ensure a consistent experience from both a threat and a throughput perspective, whether users are remote, in the branch, or on campus. And because Juniper Networks products are based on industry standards, products within the solution can be added incrementally and are compatible with other standards-based products from any vendor.

Next Steps

For more information, visit us online at **www.juniper.net** or contact your local Juniper sales representative.

[1]Ponemon

Cpay360

2012 Overview of Mobile Banking Technology

The popularity of smartphones, evolving consumer expectations and the emergence of competitors from outside the financial industry has started a mobile banking revolution that is vital to financial institutions. The majority of large financial institutions already offer basic mobile functions such as account access, ATM/branch locators and bill payment. The 2012 plan for these FIs will most likely be focused on mobile RDC (remote deposit capture), P2P (person-to-person) payments and actionable alerts. Mobile point-of-sale payments, however, are not currently on the radar for most firms. Financial institutions have a good understanding of what it will take to promote mobile POS systems but they are leery to invest in products that have unknown consumer demand and merchant interest.

In order to get a better understanding of the position mobile banking has in financial institutions' product mix, a survey of 10 top-tier banks and credit unions was done by Forrester Consulting. The survey was conducted in September 2011 and respondents included mobile banking strategists and decision makers from 10 institutions ranging from $1 billion to over $100 billion in assets. The total assets of the surveyed institutions combined are in excess of $2.5 trillion and account for one-third of all U.S. deposit accounts. The survey was conducted as a follow-up to a similar survey of the same financial institutions conducted in October 2010.

Figure 1: "Which of the following services does your financial institution offer via mobile devices today?"

	$1-10 Billion (4)	$11-100 Billion (3)	$100 Billion+ (3)
Transfers between accounts at your institution	3	3	3
Bill payment	3	3	3
Contactless /Point of Sale (POS)*	0	0	2
Self-servicing**	0	1	1
Transfers between institutions	0	0	1
Person-to-person (P2P) payments***	0	0	1
Remote deposit capture	0	0	1
Remote payments (including social media)	0	0	0
Trading	0	0	0

*For POS, FI's only
**Self servicing includes: Search transactions, Request to message in secured inbox, Send messages to customer
***Your P2P payments can be made through email or mobile phone number (downloadable app only).

Mobile Banking Is Maturing Rapidly

Nine out of 10 of the financial institutions surveyed have a mobile banking application that provides basic account access, and almost all provide ATM and branch locators, transfers between accounts and bill payment. The larger financial institutions with assets of $100 billion or more are the market leaders for adoption of new technology such as contactless/point-of sale (POS) payments, person-to-person (P2P) payments and remote deposit capture (see Figure 1). None of the FIs currently offer remote payments, in which a mobile device is used to make a purchase from a non-physical location, such as online shopping via mobile browser, or trading securities as an element of mobile banking.

Mobile Apps are Focused on Retail Banking Customers

90% of the financial institutions surveyed offer at least basic mobile banking services to retail banking customers and the same number support mobile services for credit card account holders. However, only 70% offer mobile services to small business customers and only one institution provides mobile financial services to corporate customers. These figures indicate that retail customers are the primary focus for financial institutions when it comes to mobile banking.

Financial institutions are supporting or plan to support more mobile devices than they were a year ago. Seven respondents currently support Android and six support iPhone. Half of the FIs surveyed plan to support the Blackberry. Providing support for Android is a top priority moving forward, along with support for the iPhone and tablets. While none of those surveyed currently offer support for tablets, this is now on the priority list for many institutions, with several respondents planning to support the iPad tablet.

Mobile Banking Apps to Include More Functions

The surveyed financial institutions are increasingly offering new services. Ideas for 2012 include enhancing the value of existing mobile banking offerings by covering all the basics and adding more robust functionalities, (see Figure 2) such as:

- Mobile deposit capture
- Person-to-person payments
- Two-way SMS actionable alerts
- Personal financial management
- Picture Bill Payment (allows users to take a picture of their bill via mobile device and then pay biller)

Transactional capabilities represent the largest concentration of planned investment in mobile banking into 2012.

Mobile Payments Takes Mobile Banking Beyond the Basics

There are four areas of mobile payments:

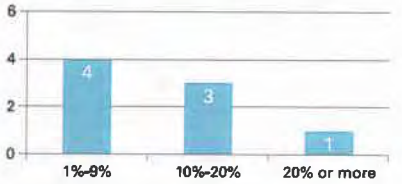
1. Bill payment
2. Person-to-person payments (P2P)
3. Internet purchases
4. Point-of-sale payments (POS)

Mobile bill payment is now considered a basic mobile banking feature and is offered by 9 out of the 10 FIs surveyed. Only one institution currently supports person-to-person (P2P) mobile payments,

however this function was named as the biggest mobile payments priority for 2012, by seven of the 10 respondents.

The majority of the financial institutions surveyed plan to invest in mobile payments in the next 12 months. One institution has dedicated 20% of its digital technology budget to mobile payments while another four plan to invest more than 10% of their spend on mobile payments (see Figure 3).

Figure 3: "What percentage of your department's digital technology budget is being spent on mobile payments in the next 12 months?"



Base: Ten Mobile Strategists at top tier U.S. banks and credit unions
Source: Mobile Banking and Payments Update, a commissioned study conducted by Forrester Consulting on behalf of Fiserv, September 2011

Mixed Emotions Regarding Point-of-Sale Payments

Of the four areas of mobile payments, POS payments have received the bulk of the industry headlines. Media announcements about mobile wallets and contactless payments have captured the attention of consumers. It seems that the ability to use a mobile device to pay for goods or services at retail locations is quite popular among tech savvy consumers.

According to the FIs surveyed, technology limitations are no longer preventing financial institutions from investing in mobile POS payment systems. Recent industry advancements have proved that the technology for mobile payments is available and that in many cases existing payment networks can be used to support these transactions.

With technology limitations not a deterrent factor, merchant acceptance is now the main concern for financial institutions, followed by unknown consumer demand. While community financial institutions are understandably hesitant in supporting mobile POS payments, large FIs are starting to make the investment.

Customers Drive Developments in Mobile Technology

The rapid development of mobile payments is largely due to consumer demand for enhanced convenience. Financial executives report that the shift from physical to electronic payments is easier with a mobile device. A smartphone is a personal device carried closely by customers, very similar to a consumer's wallet. Consumers are basically transitioning from a traditional wallet to a

mobile wallet. FIs understand that mobile payments must be quicker and easier than current payment options, and more universally available. As the popularity of smartphones increases and mobile payment capabilities become more widespread, interest in mobile banking is likely to grow. Financial institutions can benefit by not only providing these mobile services but also educating consumers on their potential to offer enhanced convenience and security.

Merchant Acceptance

Merchant acceptance of mobile POS payments is an important concern. However, banks and credit unions believe merchants will be more obliged to accept mobile payments under these circumstances:

- The costs to implement and support POS technology are affordable
- There is a potential to reduce costs to serve customers
- There is adequate customer demand

Financial institutions believe that mobile payments offer distinct competitive advantages and new methods for merchants to promote their business via mobile technology. However, the survey respondents believe merchants are still hesitant to implement mobile payments because they are unsure about the value, reluctant to invest in unfamiliar technology, and concerned about the level of consumer interest. With these vital concerns, it is no surprise that only 50% of the surveyed institutions have plans for mobile POS payments.

New Competition

Generally, the survey participants see mobile payments as an opportunity for financial institutions. Banks and credit unions concerned about ROI believe the business case for mobile payments will be proven by reduced service costs, increased interchange by migrating more payments to card accounts and the ability to reach underserved markets such as the unbanked and underbanked population.

When asked about the recent emergence of new nontraditional competitors such as Google Wallet and PayPal, the surveyed financial institutions recognized the threat of these firms and others like them. One of the interviewed executives said that these competitors, "Put more urgency on the need to move in the mobile payments space." Another executive described the unbanked consumers by referring to them as "smart people that understand that the evolution is at hand." A few of the participants saw moves by non-traditional payment providers as validation that mobile payments will reach the mainstream. As one respondent summarized, "these announcements bring a lot of optimism that mobile payments are really going to happen with leaders like Google.

While financial institutions see the media hype around mobile applications as confirmation of mobile payments popularity, the majority of those surveyed stated that such announcements have had minimal impact on their mobile payments strategy.

Financial institutions need to separate the fact from the media hype surrounding mobile payments. However, the threat posed by non-bank competitors in the mobile payments arena should not be underestimated. There is a risk that as consumers become accustomed to using mobile payments capabilities provided by third parties that they will disassociate their bank from transactions and as a result, lose affinity for their financial institutions.

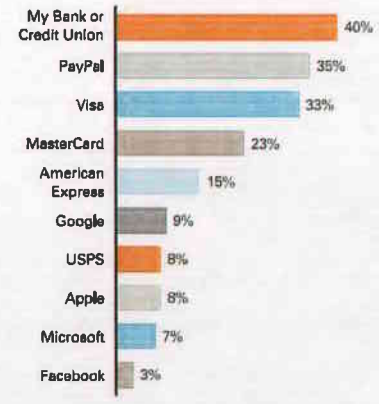
Consequently, being left behind in the rapidly growing mobile payments market can prove costly for community banks and credit unions. Companies such as Google, Square Up and telecommunication providers that are willing and able to provide consumers with the mobile payment options they want could lure customers from financial institutions that do not move quickly. If financial institutions do not provide the mobile payments services desired by consumers they will turn to another provider and will be unlikely to return, even if their financial institution offers the service in the future. As third parties aggressively pursue the mobile payments space, it may be time for financial institutions to become more proactive in pushing forward with their own mobile payment strategies.

The Competitive Advantage of Financial Institutions

Financial institutions possess many precious resources when it comes to mobile payments, the most important of which is consumer trust. According to the 2011 Fiserv Consumer Trends Survey, 40% of consumers trust their financial institutions to handle mobile payments, dominating all other entities including PayPal, Visa and MasterCard.

Because consumers trust their financial institutions to provide secure financial transactions, consumers will look first to their financial institution for mobile payments. Financial institutions are in a position now to put the advantages they have to good use and give consumers what they are demanding – mobile banking services that enable transactions, especially mobile payments.

Figure 4: Financial Institutions Most Trusted Providers of Mobile Payments: "Which of the following do you trust for handling mobile payments?"



Base: U.S. online households
Source: 2011 Consumer Trends Survey, Fiserv, Inc., August 2011

Statement for the Record

by

Errol Weiss

Director of the Cyber Intelligence Center

Citi

Before the

House Financial Services Subcommittee on

Capital Markets and Government Sponsored Enterprises

Hearing on

"Cyber Security for the Capital Markets"

June 1, 2012

Good morning Chairman Garrett, Ranking Member Waters, and members of the Subcommittee.

My name is Errol Weiss; and I am the Director of Citi's Cyber Intelligence Center, which is responsible for collecting, analyzing, and exchanging threat intelligence in an effort to protect the Citi brand, global business operations, technology infrastructure and client trust against cyber threats world-wide. This morning I am testifying on behalf of the Securities Industry and Financial Markets Association (SIFMA) on how to best protect capital markets from emerging cyber threats.[1]

I. Introduction

SIFMA supports the goals of the Administration and Congress to limit cybersecurity threats to the American people, businesses, and government through a more integrated approach. The increase in cyber intrusions and cyber crimes in the past decade is cause for great concern, particularly to those in the financial services sector. SIFMA member firms are on the front lines defending against cyber threats to the financial markets and we take this role very seriously.

[1] The Securities Industry and Financial Markets Association (SIFMA) brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA's mission is to support a strong financial industry, investor opportunity, capital formation, job creation and economic growth, while building trust and confidence in the financial markets. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

At the outset, we think it's important for Members of Congress and the Administration to understand the existing regulatory framework under which the financial services industry functions.

II. The Existing Cybersecurity Infrastructure of the Financial Services Sector

The United States has embraced a sector-specific approach to data security and privacy regulation for decades. SIFMA urges Congress to consider the unique position of the U.S. financial services sector in connection with the ongoing examination of the national cybersecurity framework. As part of the financial services industry, SIFMA members are currently subject to stringent laws and regulations on the protection of personal data, including the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act (RFPA). These laws and regulations are reinforced by regular, pro-active review, and audited by highly specialized regulators that are supported by the Federal Financial Institutions Examination Council (FFIEC), an interagency entity that issues data privacy and cyber security guidance and monitoring procedures. As discussed below, financial services firms appreciate more than almost any other sector of the economy the importance of maintaining the confidentiality of customer information. The financial services industry is keenly aware of the consequences resulting from a privacy or security lapse, and has long played a leadership role in developing policies, procedures, and technology to protect customer data.

The financial services sector has had an effective and longstanding working relationship with the U.S. Treasury Department on cybersecurity since Presidential Decision Directive/NSC-63 was issued in May 1998. In response, the industry proactively formed the Financial Services Information Sharing and Analysis Center (FS-ISAC)[2] which began operations in October 1999. After September 11, 2001, and in response to Homeland Security Presidential Directive 7 (HSPD7) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to our sector that could impact business continuity and resiliency. Citi was one of the founding members of the FS-ISAC and I am currently on the FS-ISAC Board of Directors. A key factor in the success of the FS-ISAC is trust. And trust takes years to develop. The FS-ISAC has worked hard to facilitate the development of trust between its members, with other organizations in the financial services sector, with other sectors, and with government organizations such as law enforcement, regulators, and intelligence agencies for over a decade. We cannot afford to weaken that trust.

In addition to the work and success of the FS-ISAC the financial services industry is already one of if not the most highly regulated industries from a cybersecurity standpoint. SIFMA members are currently subject to the FCRA, GLBA and the examination guidelines of the FFEIC. Since 1970, the FCRA has promoted the accuracy, fairness, and privacy of personal data assembled by "consumer reporting agencies" (CRAs), including data provided by a majority of SIFMA member firms. The FCRA establishes a framework of fair information practices that include rights of data quality, data security, identity theft prevention, and use limitations, requirements for data destruction, notice, user consent, and accountability.

[2] For an overview of the FS-ISAC's responsibilities and functions, please visit: http://www.fsisac.com/files/FS-ISAC_Overview_2011_05_09.pdf

The GLBA provides data privacy rules applicable to "financial institutions," a term defined broadly to cover entities significantly engaged in financial activities such as banking, insurance, securities activities, and investment activities. The GLBA imposes data privacy obligations such as the obligation to securely store personal financial information, and provide data subjects with notice of the institution's privacy practices and the right to opt-out of some sharing of personal financial information. The GLBA regulations also provide guidelines to financial institutions on appropriate actions in response to a breach of security of sensitive data, including on investigation, containment, and remediation of the incident and notification of consumers and/or law enforcement authorities when warranted.

Finally, many SIFMA member firms also follow FFIEC guidance and monitoring procedures. The FFIEC is an interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

The FFIEC also makes recommendations to promote uniformity in the supervision of financial institutions. In the area of cybersecurity and data breach protection, the FFIEC has published the following standards: FFIEC Interagency Guidelines Establishing Standards for Safeguarding Customer Information; FFIEC Interagency Guidelines Establishing Information Security Standards; FFIEC Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice; FFIEC Information Technology Examination Handbook (includes guidance and audit provisions of many of the requirements identified in the guidance documents referenced above).

III. Proactive Sector Initiatives

FS-ISAC Account Takeover Task Force

In 2010, the FS-ISAC formed the Account Takeover Task Force (ATOTF) as a result of continued concern and need for additional tools to help financial institutions and their customers combat online account takeover attacks. The ATOTF consists of over 120 individuals from thirty-five financial services firms of all sizes and types, ten industry associations and processors and representatives from seven government agencies. The ATOTF focuses on deliverables in three areas of effective cyber defense: Prevention, Detection and Response.

Some example deliverables and products produced by the ATOTF include:

Prevention

- Fraud Advisory for Businesses: Corporate Account Take Over, co-branded with US Secret Service, FBI and Internet Crime Complaint Center (IC3). The advisory is available here: http://www.fsisac.com/files/public/db/p265.pdf

- Fraud Advisory for Consumers: Involvement in Criminal Activity through Work from Home Scams, co-branded with FBI and IC3. The advisory is available here: http://www.fsisac.com/files/public/db/p264.pdf
- J1-Visa Money Mule Advisory
- Internet Auto Fraud

Detection

- Detection Whitepaper for financial institutions – Document focused on detection of account takeover victims.
- Techniques for recovering customers from ZeuS or other keystroke logging/man-in-the-middle Trojan infections and the exploration of third-party services with the goal of gathering elements of intelligence to enable better detection methods.
- Document Standard Set of Requirements and enhancements for alerting and security requirements for core ACH/wire transfer software providers.

Response

- Contact List, Procedures - This list provides financial institutions the information they need to report account takeover attacks via online banking to the Secret Service, FBI and other agencies, and a process for keeping the contact lists current.
- Form for Reporting account takeovers, including what should be submitted in the incident report and used for metrics to measure the success of the ATOTF.
- Actions financial institutions can take after an incident, communicated via FS-ISAC advisory notices.
- Internet Fraud Alert service from the National Cyber-Forensics & Training Alliance (NCFTA). This provides financial institutions with information for recovered credentials from the takedown of botnet command and control servers.
- List of Resources currently available for cyber crime and broad education so that financial institutions can leverage existing resources.
- Malware Submission method provides a process for sharing identified new malware with government/law enforcement agencies and anti-virus vendors.
- Redesign Suspicious Activity Report (SAR) Submission and Analysis Process by working with the Financial Crimes Enforcement Network (FinCEN) to give financial institutions and regulators more actionable information.
- Recommendations for reporting an account take over attack via SARs.

Finally, the ATOTF implemented a survey and polled member organizations regarding commercial account takeover to establish a baseline for Commercial Account Takeover attempts and losses. The surveys collected data in 2009, 2010 and the first half of 2011. The results indicate that financial institutions are doing a better job of stopping fraudulent transactions.

Botnet Takedown Partnership with Microsoft

FS-ISAC, in partnership with Microsoft and NACHA, announced on March 26, 2012, that they successfully executed a coordinated global takedown operation against some of the most

notorious cybercrime operations responsible for online fraud and identity theft. The takedown was accomplished through coordinated legal and technical actions and disrupted massive botnets using the ZeuS and SpyEye malware families, striking a major blow against cybercriminal operators targeting the financial services sector's customers.

A video news release about the disruption, codenamed, "Operation B71", is located here at the Microsoft Digital Crimes Unit web page: http://www.microsoft.com/presspass/presskits/dcu/ . The takedown will help prevent online fraud and identity theft for consumers and businesses worldwide. Microsoft's investigation shows that approximately 3.6 million computers in the United States alone have been infected with the ZeuS malware.

This takedown was made possible through a successful pleading before the U.S. District Court for the Eastern District of New York on March 19, 2012, which allowed Microsoft, FS-ISAC and NACHA to sever the command and control structures of several of the most dangerous botnets running ZeuS, SpyEye and Ice IX malware. Because the botnet operators used ZeuS, SpyEye and Ice IX to steal victims' online banking credentials and transfer stolen funds, FS-ISAC and NACHA joined Microsoft as plaintiffs in the civil suit.

On March 23, 2012, Microsoft and co-plaintiffs FS-ISAC and NACHA, escorted by the U.S. Marshals Service, executed a coordinated physical seizure of servers in multiple hosting locations to preserve evidence for this case and seized hundreds of domain names used by the ZeuS, SpyEye and Ice IX malware to remotely command and control victim computers. Although it is not expected that this operation will completely destroy all botnets running ZeuS, SpyEye and Ice IX malware, or even that every botnet taken down in the operation will stay down permanently, this action is expected to significantly disrupt the cybercriminals' operations by increasing the risk and costs for its controllers to continue doing business.

Microsoft has stated that it will use the intelligence gained from this takedown to partner with Internet Service Providers and Computer Emergency Response Teams around the world to help remediate infected computers from the control of ZeuS, SpyEye and Ice IX, making the Internet safer for consumers and businesses worldwide.

Together, these aspects of the operation are expected to undermine the criminal infrastructure that relies on these botnets every day to make money and helps to provide new tools for the industry to work together to proactively fight cybercrime.

IV. The Threat - Hactivists, Organized Crime and Nation States.

Threats to the banking and finance sector come primarily from three groups – hacktivsts (on-line activists promoting a sociopolitical ideology), organized criminal gangs (committing cybercrime for financial gain), and foreign nation states / extremist groups (committing industrial espionage to gain competitive advantage or disrupt financial markets).

Hacktivism is a term used to describe motivated individuals and groups that use hacking techniques to promote a political ideology. While traditionally cyber based, in 2011, we witnessed hacktivist causes spill over into the physical world as well, causing disruptions and

complicating business operations for many government and businesses, including SIFMA members. Starting as far back as 1994, hacktivists were using Distributed Denial of Service (DDoS) attacks to make internet sites and services unavailable to intended users. DDoS attacks have since become a staple hacktivist technique, resulting in lost revenue and reputational damage. In the past year, hacktivist activity has exploded, with malicious actors bent on retaliation against organizations that do not support their cause. Hacktivist tactics continue to include DDoS attacks and also include public exposure of sensitive internal information.

Sophisticated criminal organizations continue to target individuals and organizations with sensitive financial information. Once they are able to compromise a victim, criminals are quickly turning the stolen data into financial gain. The criminals operate a sophisticated and mature business, with a complete operating model that includes outsourcing of each discrete component of the underground ecosystem to specialists and experts around the globe. Criminals cooperate through the development of malware to evade anti-virus protections, the delivery of malware via targeting phishing emails and/or infected websites, stealing customer credentials and answers to challenge questions, takeover of on-line banking accounts, and movement of stolen money through a network of unwitting and/or complicit professional "money-mules" to the criminal syndicate often outside the U.S. in places like Eastern Europe.

Technically advanced and adversarial Nation States and extremist groups represent the third major threat to the banking and finance sector. Foreign economic collection and industrial espionage against the United States and other nations are conducted, to a large degree, in Cyberspace. Virtually every business activity and the creation of new ideas take place on the Internet. Malicious actors, whether they are corrupted insiders or foreign intelligence operatives, can easily steal and transfer massive quantities of data while remaining anonymous and nearly impossible to detect. Foreign operatives with motivation to steal sensitive economic information are able to operate in cyberspace with relatively little risk of getting caught.

The use of sophisticated malware, along with highly cooperative hackers for hire, makes it difficult to attribute responsibility for the entities behind corporate computer network intrusions. Foreign adversaries perform industrial espionage to target proprietary (and sometimes non-proprietary) company information they can use for their own gain. For a SIFMA member firm, foreign adversaries could be interested in information like client lists, merger and acquisition data, company information on pricing, and financial data. High technology firms may be targeted for new design information. Extremist groups use the same techniques to gain system access, but go a step further by using that access to cause disruption and/or destruction. As an example, recent DDoS activity against large U.S. member firms has been orchestrated by extremist and terrorist groups associated with foreign nation states.

V. Information Sharing

Despite the robust cybersecurity infrastructure that the financial services sector has established and the current ability to share information with our peers and others, SIFMA recognizes the need for expanded information sharing with government agencies, including greater private sector access to threat data from Federal intelligence and law enforcement agencies. Access to threat information must be administered in a manner that can provide broader cybersecurity

protection without compromising ongoing investigations or the privacy of individual Americans. In addition, providing greater access to security clearances for private sector employees will increase the likelihood that cyber threat information will be distributed in a timely manner and handled properly.

While we support enhanced transparency and information sharing, we are concerned that if sensitive private sector information is shared with a government agency, it could be divulged to the public in response to a Freedom of Information Act (FOIA) request. Such disclosure could invite further attacks or create the perception that an institution is defending itself ineffectively. SIFMA believes that cybersecurity information shared with government agencies, including the identification of critical infrastructure, must be exempted from disclosure under FOIA.

Additionally, SIFMA believes government agencies should leverage ISACs and the United States Computer Emergency Readiness Team (US-CERT) to facilitate two-way and cross-sector public/private information sharing. We believe the ISACs should remain in place for mature sectors like financial services and we oppose any cybersecurity legislation that establishes a "National Information Sharing" clearinghouse, which will add layers of bureaucracy and delay information sharing with existing ISACs.

VI. Recent Cybersecurity Proposals

This past fall, the House Cybersecurity Task Force recognized that private-sector entities control the vast majority of U.S. information and communications technology and other critical infrastructure. These entities are in the best position to identify and defend against cyber-related threats. Owners and operators are, and should be, responsible for the protection, response, and recovery of private assets. Yet, there is widespread agreement that the public and private sectors need to work together, particularly when it comes to greater sharing of information in order to achieve enhanced situational awareness to detect, prevent, mitigate, and respond to emerging and rapidly changing threats – while at the same time ensuring that personal information is adequately protected.

In the spirit of enhancing public-private coordination, several members of Congress drafted proposals to combat cyber threats to critical infrastructure; increase public/private information sharing regimes; increase cyber research, development and education; and update federal network security practices.

SIFMA is especially encouraged by the information sharing provisions contained within CISPA, introduced by Reps. Mike Rogers (R-MI) and Dutch Ruppersberger (D-MD)

SIFMA believes the sharing of information from government to industry has immense value but we are also supportive of the voluntary approach to information sharing from the private sector to the government. CISPA provides a solid framework and useful legal protections to encourage and permit the timely flow of actionable information. Creating an environment where cyber threat intelligence is readily available and shared is fundamental to any long-term endeavor to defend our country and make our markets more resilient.

As the debate continues in Congress, in addition to information sharing, SIFMA asks that Members keep the following principles in mind with respect to the following issues:

1. **Critical Infrastructure:** Several of the recent cybersecurity proposals include provisions that grant DHS the ability to designate an organization as a critical infrastructure operator and then regulate that system or organization. SIFMA believes that the financial services sector's current regulator is best-suited for the role of designating or regulating a critical infrastructure operator because they have a long history and are familiar with the complex operations of financial services organizations. The Treasury Department, as the Sector Specific Agency for the financial services sector, and the regulatory agencies through the Financial and Banking Information Infrastructure Committee (FBIIC), should determine if an institution in the sector is considered critical. The financial industry, like many other industries in the United States, is far too complex to be managed and regulated via a one-size fits all solution.

   Furthermore, when determining what constitutes critical infrastructure within a firm, the scope of critical infrastructure should apply to specific capabilities, processes, functions or business units and not to an entire firm or institution. It must be recognized that critical infrastructure is built within an ecosystem that includes commercial vendors and suppliers that contribute to the overall resiliency of the capability, process or function that should be protected. SIFMA supports enhanced supervision over service providers on which financial institutions depend (e.g., hardware and software providers, Internet service providers, etc.); however, such coordination may be better achieved by building on some of the existing mechanisms that seek to address these issues (e.g., Partnership for Critical Infrastructure Security).

   Building on existing mechanisms and organizations within the sector, we feel it is essential that the private sector have a prominent voice in the criteria that will be used to designate critical infrastructure. By leveraging the established partnership between the Financial Services Sector Coordinating Council (FSSCC) and the FBIIC, the experts can come together and determine what the criteria, metrics and thresholds should be to determine if a specific capability, process, function or business unit within the financial services industry is critical. Once those systems are denoted, leveraging and updating the existing rules in place that we as an industry already adhere to would make implementation and assessment as seamless as possible.

2. **Supply Chain:** SIFMA supports federal cybersecurity supply chain management and promotion of cybersecurity as a priority in Federal procurement. Other efforts to defend against cybersecurity threats will be lessened without financial support for the infrastructure necessary to implement a defense strategy.

3. **Law Enforcement:** SIFMA supports the strengthening and clarification of criminal penalties for cybercrimes. These improvements further bolstered by an increase in budgets and personnel for these purposes at law enforcement agencies will provide additional protection for consumers and financial institutions.

4. **Research & Development:** The development of essential technologies and improving federal systems are important efforts which should be supported. As DHS and the National Institute of Standards and Technology (NIST) pursue their research and development agendas, we hope to see substantial resource commitments and advances in these areas. We also support the improvement of the resilience and security of federal systems to further prevent cybercrime.

5. **International Cooperation:** Because cybersecurity is a global problem and cyber crimes frequently occur across borders, cooperation with international partners is critical to preventing, investigating, and prosecuting cyber crime. The U.S. should seek strong cooperation with foreign governments, international law enforcement agencies and policy making bodies, to improve cybersecurity. The U.S. should pressure foreign governments to enact effective cyber security legislation and demonstrate they enforce those laws by prosecuting and punishing individuals convicted of such crimes. If we do not work across borders on this issue our ability to prevent, defend and deter cyber crimes will be severely limited.

6. **Safe Harbor for Disclosure:** SIFMA members believe that the safe harbor provisions for cybersecurity reporting will be helpful for SIFMA members and provide much-needed extra protections for sharing information beyond what is currently available under Protected Critical Infrastructure Information (PCII) provisions. Financial institutions that cooperate with the government in cyber-threat sharing should receive liability and confidentiality protections. We are in support of both strong liability and confidentially protections with strong preemption.

7. **Education & Awareness:** Public education and awareness campaigns have been a critical method of limiting cyber crimes in the financial services industry. Both the Securities and Exchange Commission (SEC) and SIFMA members have promoted public awareness of the risk of disclosure of personal information for many years, and SIFMA supports the expansion of any such campaigns and promotions.

8. **Breach Notification:** SIFMA members believe that a single, uniform federal breach notification standard that preempts state law would help reduce administrative oversight, establish clear notification guidelines, and reduce consumer confusion. We support a notification standard that is based on risk-based assessments of actual or likelihood of harm, and allows for a reasonable investigation and mitigation period.

VII. Conclusion

SIFMA supports the efforts of the Administration and Congress to further protect the American people, businesses, and government from the increasing threat of cyber attacks and cyber crimes. As you can see, the financial services sector faces a number of significant threats and is currently tracking several of them, with a concern that they may materialize in the future. We have outlined a number of the actions that the FS-ISAC has taken on behalf of the sector to identify and mitigate threats that we are facing. In addition, the financial services sector already has a strong regulatory regime in place with its existing regulators. This oversight, as well as

partnerships with industry bodies and software providers, allows us to proactively work to ensure that our systems are protected and that we maintain flexibility so that we can respond quickly when threats change.

Recent proposals are a good first step in addressing some of the issues and the four bills recently passed by the House address many of the principles we laid out earlier. The changes to the Federal Information Security Management Act (FISMA) that will drive improvements in federal systems, increase coordination between federal agencies around education, awareness, standards and talent development, and the reauthorization of the Networking and Information Technology Research and Development program (NITRD), will assist in helping America better protect its cyberspace. CISPA in particular will move us along the furthest by making the private sector aware of the threats that are out there and provide a framework within which we can confidently share information with the government.

The sharing of actionable and timely intelligence will allow the people with the greatest expertise in protecting their systems, many of them critical to properly functioning markets and the economy at large, the best chance of anticipating, protecting and defending their systems and networks from the individual criminals, criminal syndicates and nation states that seek to steal intellectual property, disrupt markets and do harm.

SIFMA members are accustomed to and fully supportive of protecting their customers' data, and, as partners and service providers, the data of customers of financial institutions worldwide. Encouraging effective data protection goes to the heart of SIFMA's mission of building trust and confidence in the financial services industry. Without effective protection of the personal data of our customers, financial institutions would lack the public trust that is so critical for their operation.

Booz Allen Hamilton Holding Corporation : Booz Allen Announces Top 10 Financial Services Cyber Risk Trends for 2013

11/29/2012| 08:05am US/Eastern

The New Cybersecurity "Rules of the Road" for the Financial Services Industry

Ask any customer what they expect from their bank or financial services firm today, and two words come through loudly and clearly: security and privacy. Commercial and institutional customers have come to expect seamless service, properly cleared transactions and fast, accurate information. But news about major cybersecurity breaches has alarmed consumers, causing banks to redouble their efforts to protect their technology infrastructure. This means the stakes have never been higher for banks and financial services firms, and there are clear trends for cyber risk and security protection in the financial services industry in 2013, according to the experts at Booz Allen Hamilton.

"When we think about the lethal daily threats to the globally integrated financial services industry from nation-states and individuals, it is imperative that Chief Information Security Officers begin looking around corners, talk with each other and better prioritize the real threats to their firms," said Mike McConnell, Booz Allen vice chairman and former Director of National Intelligence. "Self-evaluation and industry-wide conversations are the new 'rules of the road' to creating successful, integrated cyber defenses. The CISO can really drive organization-wide change while still championing efficiency and customer service."

McConnell is speaking today at Bloomberg's Enterprise Risk Conference (more information) where he will discuss the financial services industry's responses to state-based and state-sponsored cyber attacks. He added, "There are many cyber trends - including the sophistication and lethality of the attacks - that the financial industry should be aware of. Even though it is difficult to look into a crystal ball and predict the future, these events are happening now and could cause significant reputational, financial and infrastructure damage to any ill-prepared firm. Individual companies should not wait for legislation or an Executive Order to come together with their government counterparts to find dynamic solutions to these big issues."

Booz Allen works with financial services firms to identify and benchmark best practices and challenges for long-term cybersecurity prevention and protection. This process is part of Booz Allen's Cyber M3 (Measure, Manage, Mature) capability, which evaluates the maturity of a firm's cybersecurity programs. Both Cyber M3 and the benchmarking program incorporate technology, business process engineering, human capital development and risk management in developing a comprehensive picture of a firm's and industry's cyber readiness.

The Top 10 Financial Services Cybersecurity Trends for 2013:

1. **Business/Information Risk protection is not Just a Technology Issue** - Spending on new technology alone is not enough to protect a firm's information and business. Firms must also invest in people and in fine-tuning processes to ensure, not only the proper use of technology, but that the processes that require interfaces between organizations are well managed and executed flawlessly. No matter how good a technology is, if not used correctly by skilled employees who follow well-defined processes, vulnerabilities will surface that can be leveraged by both internal and external threat actors.
2. **Data disruption attacks may become data destruction attacks** - The potential of threat actors actually destroying data is a major concern among risk and security professionals. Over time, the financial services industry will face threats from extremist groups who, when denied access to weapons of mass destruction, will use cyber as a "weapon of mass disruption." Additionally, threat actors who mean to disrupt a firm's business operations to make a statement or prove what they consider a moral point will also utilize destruction of data to ensure they make an impact.
3. **Nation-states and threat actors are becoming more sophisticated** - We now have to face more sophisticated threat actors such as smaller nation-states and terrorist elements obtaining similar capabilities. The financial services industry must fully understand the entire threat landscape and what this means in terms of employing the right people, technology and processes to ensure business continuity and proper risk management.
4. **Legislation could push industry standards around cyber risks and improve threat intelligence information sharing** - Banks already share information, but they will need to do more in light of possible legislation to set standards for cyber protection. If Congress allows the sharing of important national security information, industry standards could become a benchmark requirement that firms must meet before they are given access to government information. Additionally, such legislation could help in reducing the valid fears of firms in sharing cyber incident information due to the threat of penalties and further regulation. The industry and government must acknowledge and treat firms as part of the nation's critical infrastructure because a breach at anyone bank or firm can have severe, cascading effects on the nation's stability.
5. **Predictive threat intelligence analytics will create a more effective risk management capability** - Financial services firms must begin to employ a more predictive threat intelligence capability to determine who might be trying to attack them and how. Focusing on understanding their own individual business risks (as well as industry risks) and combating real potential threats that could focus on such risks is much more effective than trying to create a defense that could cover any possible threat.
6. **Vendor Risk Management is becoming an increasingly important concern among firms** - Most firms buy much of their information technology and services from suppliers. Therefore, these suppliers' vulnerabilities become the vulnerabilities of the firms they provide products and services. Firms are becoming more focused on the security requirements for these suppliers and engaging independent third parties to evaluate the risks around such products and services.
7. **Cyber risk continues to be a board-level issue** - Information, legal documents, and communications with clients and employees are all becoming more and more electronic every day to include an even greater usage of mobile technologies and social media. The boards of financial institutions must create and embrace a culture that acknowledges the evolving risks and more openly shares incident information across the industry, with technology providers and with both law enforcement and the federal government.
8. **Firms must continue to embrace and adapt to the new "boundless network," and must also invest in training its workforce to properly access and protect corporate data** - Cloud, social and mobile technologies, including "Bring Your Own Device" (BYOD), are simply too cost efficient and effective for institutions to ignore them. Security and risk professionals need to better integrate these technology trends, which will require they embrace the fact that the corporate network now has extended beyond their control. Risk management and mitigation is evolving to better control how corporate data travels these boundless networks and ensuring the education of their employees on the responsibilities they have in securing such data.
9. **Identity and Access Management is becoming a key security control area in which firms will continue to invest heavily** - The days of focusing solely on perimeter defense have long since passed. Phishing and other social engineering strategies employed by threat actors have been very effective in allowing them to penetrate almost any network. Banking institutions must assume these actors can get in. Ensuring proper identity of an authorized individual is a key area that is being addressed by all firms in all industries to address this new paradigm. Most threat actors employ a strategy to gain access to networks and information by gaining access to valid authorized credentials of a firm's employee so that they can go undetected in their actions. Firms

will continue to invest heavily in ensuring that an authorized user is actually an authorized user. Additionally, firms will invest more heavily in tracking unusual activity of a user to detect stolen credentials or an insider threat.

10. **The Financial Services industry will rely more heavily on cyber benchmarking** - The FS industry is investing more and more in protecting its information assets and wisely spending these scarce dollars is becoming increasingly important, not only from an effectiveness standpoint, but to also be able to articulate to business leaders, the value of such an investment. The FS industry, therefore, will continue to use industry benchmarks to understand how their competitors and suppliers are investing in people processes and technology for cyber risk management.

For 2012 Booz Allen issued its first annual list of cybersecurity trends for the financial services industry (read the 2012 list). Since then, the industry has experienced a number of high-profile attacks, such as the DDoS attacks on U.S. commercial banks and the New York Stock Exchange.

"In the span of one year, we have seen a significant shift in the frequency and sophistication of cyber attacks on financial services firms. This is perhaps the biggest trend of them all," McConnell said.

Booz Allen Reports Top Ten Cyber Security Trends for Financial Services in 2012

November 29, 2011

MOBILE DEVICES, INSIDER THREATS AND ZERO-DAY MALWARE AMONG KEY CONCERNS

McLean, VA —Booz Allen Hamilton (NYSE: BAH) today cited increased cyber threats to senior executives, the impact of organized crime and mobile device security as among the Top 10 Financial Services Cyber Security Trends that will make 2012 a pivotal year for banks and investment firms as they try to stay ahead of the IT security curve. These threats have a trickle-down effect on every part of a financial services organization, with reputational and financial impacts that can be a huge risk to any organization.

"These trends highlight the fact that cyber security today is about living with and managing the risk in your network. It's more than just preventing security violations," said Bill Wansley, senior vice president at Booz Allen Hamilton. "Every day, it's essential that the financial services industry – from small community banks to large Wall Street institutions – know what cyber security threats are on the horizon, and how the cyber and technology industries are meeting these concerns. Today's business environment requires financial institutions to be more creative in meeting the demands of their customers, shareholders, and regulators," Wansley said.

The following list was developed from research by Booz Allen, which has years of experience in financial services consulting for federal, nonprofit and commercial clients:

Top 10 Financial Services Cyber Security Trends for 2012:

1. The exponential growth of mobile devices drives an exponential growth in security risks. Every new smart phone, tablet or other mobile device, opens another window for a cyber attack, as each creates another vulnerable access point to networks.
2. Increased C-suite targeting. Senior executives are no longer invisible online. Firms should assume that hackers already have a complete profile of their executive suite and the junior staff members who have access to them.
3. Growing use of social media will contribute to personal cyber threats. A profile or comment on a social media platform – even by the CEO's son or sister -- can help hackers build an information portfolio that could be used for a future attack.
4. Your company is already infected, and you'll have to learn to live with it – under control. Security should remain a priority, but today's risks and threats are so widespread that it will become impossible to have complete protection – the focus of cyber security tactics increasingly must be to analyze, detect and expunge threats inside your system.
5. Everything physical can be digital. The written notes on a piece of paper, the report binder and even the pictures on the wall can be copied in digital format and gleaned for the tools to allow a hacktivist-type of security violation, and increasingly this will be a problem.
6. More firms will use cloud computing. The significant cost savings and efficiencies of cloud computing are compelling companies to migrate to the cloud. A well designed architecture and operational security planning will enable organizations to effectively manage the risks of cloud computing.
7. Global systemic risk will include cyber risk. As banks and investment firms continue on the path to globalization, they will become increasingly inter-connected. A security breach at one firm can create negative ripple effects that greatly impact systemic risk in financial markets.
8. Zero-day malware (malicious software) and organized attacks will continue to increase. Like a vicious, insidious virus that mutates, the tools of cyber criminals adapt and change constantly, rendering the latest defenses useless. Firms need to be prepared to adapt quickly as well to zero-day malware and the tactics of organized crime and foreign adversaries that are increasingly used today.
9. Insider threats are real. The accidental insider breach will continue to be the primary source of compromise for the Advanced Persistent Threat (APT) and other attacks. Organizations need to focus on security awareness training and internal monitoring to detect intentional and accidental insider access.
10. Increased regulatory scrutiny. Recently, the Securities and Exchange Commission introduced guidelines that require companies to report incidents that result, or could possibly result in, cyber theft or a risk of compromised data considered material.

More information on these trends is available here.

In its 2011 U.S. Cost of a Data Breach, the Ponemon Institute reported that the financial impact of hacks continues to rise, with the cost per compromised record now at $214 (up from $204 in 2009) and the total price tag for each data breach event averaging around $7.2 million. In August 2011, hackers were able to steal $2.7 million from 3,400 customers of a major financial institution, which contributed to the $48 billion in identity fraud losses in the United States each year.

"As the list of companies victimized by hacking grows, it is clear that no network is completely impenetrable, but there are effective solutions that can help" said Wansley. "To thwart these attacks, one must embrace a dynamic defense that embodies the same aggressive, nimble, and methodical approach as our cyber adversaries use against us today. As the daily headlines remind us, cyber security isn't something on which anyone can declare victory. Cyber security is now a relentless operational risk issue for every organization that develops or delivers value."

[redacted]

Reducing the Delta Between New Regulations and Cost-Effective Practices Within the Financial Services Industry

A Study Sponsored By BITS/Financial Services Roundtable

September 2009

Table of Contents

Executive Summary 3
Objectives, Scope, and Approach 7
- Objectives 7
- Scope 7
  - Case Studies 7
  - Participants 8
- Approach 8

Analysis and Observations 10
- Summary Observations 10
- Case Study Analysis 16
  1. FFIEC Authentication in an Internet Banking Environment (2005) 16
  2. FACTA Identity Theft Red Flags (2007) 19
  3. Interpretive Guidance on Customer Breach Notification in the Gramm-Leach-Bliley Act (2005) 21

Recommendations and Implementation Steps 23
- Strategic Initiatives 23
- Tactical Improvements 30

Appendix 31
  1. Interview Detail on FFIEC Authentication in an Internet Banking Environment (2005) 31
  2. Interview Detail on FACTA Identity Theft Red Flags (2007) 36
  3. Interview Detail on Interpretive Guidance on Customer Breach Notification in the Gramm-Leach-Bliley Act (2005) 39
  - Interview Detail on Additional Observations 40

Executive Summary

BACKGROUND

The purpose of this study is to identify opportunities for financial services industry participants—financial institutions, service providers, industry associations, and regulators—to work more efficiently to achieve timely, practical, and commercially reasonable practices for complying with new regulations and supervisory guidance for technology, security and privacy topics.

This paper was commissioned in December 2008 by BITS, the technology and operations division of the Financial Services Roundtable, and The Financial Services Roundtable's Anthony T. Cluff Fund. It was conducted by Deloitte & Touche LLP.

To support our analysis, we selected three regulations or guidance to serve as representative examples of the process by which rules are disseminated and addressed by industry participants. These "case studies" include FFIEC Authentication Guidance (2005), FACTA's Identify Theft Red Flag Regulation (2007), and Interpretive Guidance on Customer Breach Notification in the Gramm-Leach-Bliley Act (2005).

BITS and Deloitte[1] jointly identified three medium to large financial institutions and three "brand name" service providers that would be interviewed by Deloitte. One large insurance company was also identified to provide additional insights from a non-banking perspective. In total we met with approximately twenty-two individuals in fifteen meetings. The conversations were held "on background" and as such the identity of each participant is not being released. The financial services regulatory agencies declined to participate in the study in an official capacity, and as such we were unable to obtain their perspectives on the perceptions shared with us by the industry participants and on the feasibility of the recommendations.

Although we cannot publicly recognize the names of those who participated in this study, we extend our sincere thanks to them for their expertise and candor.

KEY OBSERVATIONS

Through the course of the interviews with financial institutions and service providers, we heard literally hundreds of perspectives on the regulatory process. Different institutions have had different experiences, and different people within the same institution sometimes hold different perspectives. In analyzing the results of the interviews, six themes emerge on the regulatory and supervisory process:

1. Some aspects of the regulatory process appear to be working adequately: These include regulators selectively obtaining industry insight, and collaboration that resulted in guidance being risk-focused and not technology-specific or overly prescriptive.

[1] As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

2. The industry could benefit from changing how field examiners[2] support implementation: Some respondents appear to have achieved effective and open working relationships with the local field examiners. However, the more common feedback was that field examiners do not adequately support the rollout of new regulation and guidance.

3. The process could benefit from crisp and clear communication of new regulation and guidance: The participating financial institutions do not believe new regulations and guidance are communicated as effectively as they could be—both verbally and in writing.

4. Collaboration among participants to form regulation and guidance exists but can be improved: Financial institutions and service providers interviewed believe that the process to form regulation and guidance could be much more collaborative among industry participants.

5. Service providers and regulators can benefit from symposiums that enable communication on regulatory matters: Unlike financial institutions, service providers do not have an industry association to facilitate interactions with regulatory agencies or to support an understanding of how new regulations and guidance impact them.

6. Industry associations drive valuable communications among the participants, but there is an opportunity for them to further harness the perspectives of their members: Financial institutions in the study believe that industry associations can provide additional services, enhance their capabilities, and structure the participation of their members to better harness the perspectives of the industry

RECOMMENDED STRATEGIC INITIATIVES

The results of the interviews with the financial institutions and service providers indicate that there are opportunities for all participants to take some action to improve the regulatory lifecycle. It is not simply a matter of the regulatory agencies changing their processes.

While some of the strategic initiatives are fundamental changes to the current process, the extent of this change should not necessarily deter industry participants from exploring them further. In many cases the proposed initiatives (or components of them) can be piloted so their impact is better understood. From there, where successful, they can be further implemented. And where not successful, they can be modified or discontinued.

The interviews with the financial institutions and service providers point to six strategic initiatives to help improve the regulatory process:

1. Use a centralized project management model to implement new regulation and guidance; better support the field examiner's role in the process: To achieve a more consistent dissemination of new regulation and guidance, regulators should consider adopting a centralized "project management" model, rather than relying predominantly on field examiners. This can be conducted in a manner that preserves

[2] Within this study we use the term "field examiner" to refer both to field examiners (who visit institutions on a set schedule) and on-site regulators (who are generally staffed full-time at financial institutions).

flexible, risk-based approaches. The recommendation also emphasizes training, communication, and information sharing.

2. Improve collaboration on draft regulation and guidance: Regulators should expand their efforts to gather industry feedback prior to the issuance of new regulations and guidance; the industry and regulators can function much more collaboratively.

3. Industry associations should strengthen efforts to better harness the knowledge of their members: Industry associations could undertake efforts to better structure their interactions with their memberships to better harness the knowledge and perspectives from across the industry.

4. The industry should lead with a proactive agenda on operational regulation: Financial institutions and industry associations should develop a proactive agenda that can be pursued by the industry and communicated to the regulatory agencies.

5. Institutions should organize internally to better respond to regulations and guidance: Institutions can pursue more effective operating models to more effectively navigate the regulatory environment—driving an agenda, responding to proposed requirements, and mobilizing to implement.

6. Continue to engage service providers through regulatory agency-sponsored symposiums, but make sure service providers are aware of the opportunity: There may be an opportunity for the regulators to improve communications with the service providers (and vice versa), so service providers are aware that this resource is available.

Opportunities by Participant

In summary, these interviews indicate that there are a number of strategic and tactical initiatives that can be undertaken across the financial services industry participants to improve the regulatory lifecycle.

Regulators can:

- Better support the field examiner's role in the process, emphasizing training and communications; use a centralized project management model to implement new rules
- Expand efforts to gather industry feedback prior to the issuance of new regulations and guidance
- Communicate consistently; use standard terminology
- View technology from newer service providers with skepticism

Financial Institutions can:

- Lead with a proactive agenda; don't be on the defensive
- Organize internally to best respond to regulations and guidance
- Use the formal process such as comment letters
- Contact the regulatory agencies when it believes its field examiners are not appropriately interpreting regulation or guidance

Service Providers can:

- Engage with regulators through symposiums

Industry Associations can:

- Restructure efforts to engage participation from members
- Facilitate achieving many of the above recommendations

Objectives, Scope, and Approach

Objectives

The purpose of this study is to identify opportunities for financial services industry participants—financial institutions, service providers, industry associations, and regulators—to work more efficiently to achieve timely, practical, and commercially reasonable practices for complying with new regulations and supervisory guidance for technology, security and privacy topics.

The genesis of this study lies in a series of hypotheses developed by BITS:

- **Costly inefficiencies:** The current system by which new laws, with resulting new regulations and supervisory guidance, are developed and implemented is fraught with costly inefficiencies
- **Long duration and trial and error:** The period between the issuance of new regulations and supervisory guidance and industry agreement on leading practices tends to take a long period of time and involves costly trial and error among financial institutions, service providers, and regulatory agency examiners
- **Interagency complexity:** When multiple regulatory agencies are involved in the issuance of new regulations and supervisory guidance, they frequently seek different—and sometimes inconsistent or conflicting—levels of compliance in a series of "one-off" visits to financial institutions, particularly in the early stages of implementation. This process is inefficient and costly to the financial institutions as well as to the regulators
- **Opportunity to shorten duration:** Enhancements to the regulatory process can be developed that will result in achieving agreed-upon reasonable practices in a shorter period of time
- **Improvements to safety and soundness:** Enhancements to the regulatory process can be done in a manner that improves the safety, soundness, and cost effectiveness of the regulatory process

Scope

This paper was commissioned in December 2008 by BITS, the technology and operations division of the Financial Services Roundtable, and The Financial Services Roundtable's Anthony T. Cluff Fund. It was conducted by Deloitte & Touche LLP.

Case Studies

To help manage the potentially large breadth of the study, BITS and Deloitte jointly defined the scope. They selected three regulations or guidance to serve as representative examples of the process by which regulations (or supervisory guidance) are disseminated and addressed by industry participants. These "case studies" consisted of:

- **2005 FFIEC Authentication Guidance:** The requirement for risk management controls to authenticate the identity of customers accessing Internet-based financial services

- **2007 FACTA's Identify Theft Red Flag Regulation:** The requirement to develop and implement a preventative program to mitigate the risk of identity theft for both new and existing accounts
- **2005 Interpretive Guidance on Customer Breach Notification in the Gramm-Leach-Bliley Act:** The requirement to notify customers when sensitive data is breached. This case study is focused on understanding the implications of regulation originating in both the Federal and state domains, sometimes with significant inconsistencies.

Participants

BITS and Deloitte jointly identified three medium to large financial institutions and three "brand name" service providers that would be interviewed by Deloitte. One large insurance company was also identified to provide additional insights from a non-banking perspective. Deloitte made contact with each organization; all agreed to participate. In total we met with approximately 22 individuals in 15 meetings.

The conversations were held "on background" and as such the identity of each participant is not being released. Any identifying information has been removed to maintain their anonymity.

BITS shared a number of documents that outlined efforts of the industry to understand issues and educate industry participants on new regulation and guidance.

The financial services regulatory agencies declined to participate in the study in an official capacity. As such we were unable to obtain their perspectives on the perceptions shared with us by financial institutions and service providers. In addition, we were unable to include their insights into the feasibility of the recommendations, or to what extent some of them may be planned or in place.

Although we cannot publicly recognize the names of those who participated in this study, we extend our sincere thanks to them for their expertise and candor.

Approach

For financial institutions, the proposed approach was to interview five to seven representatives, generally from the following groups: Risk, Information Security, Privacy, Fraud, Compliance, and Legal.

For each service provider, the proposed approach was to interview one to three representatives, generally from the Government Relations or Regulatory Affairs areas, or who interact with legislators, regulators, or industry associations on regulatory and compliance matters.

While the focus of each individual discussion was slightly different, the objective was to gain a perspective on:

- **How the organization worked with industry participants** (e.g. regulators, financial institutions, industry associations, and other service providers) across the regulatory lifecycle—from the time where regulations or supervisory guidance were formed to the point where industry leading practices were developed

- **What approaches were successful or unsuccessful** in the process to educate regulators and the industry on the necessity of regulation or guidance, industry capabilities, potential solutions, and leading or commercially reasonable practices
- **Ideas for improving the process and interactions** so that a) the industry can achieve timely, practical and commercially reasonable practices for complying with new regulations and supervisory guidance prior to the compliance date and b) regulators have comfort that the industry is adequately addressing the risks or consumer protections that are the focus of the regulation or supervisory guidance

Representative questions included:

- Please walk us through how you participated in the lifecycle for each of the three case studies. How did you interact with industry participants throughout? What worked well in the process? What did not work well? What role did industry forums (e.g. conferences, conference calls) play?
- Are there points in the regulatory lifecycle where you would have liked to have had a greater voice, or you think the process or communication could have been improved and may have resulted in a better solution?
- Are there components of the regulatory process that are too long or too short?
- In the case studies, were there situations where the underlying issues to be addressed were within the purview of multiple regulatory agencies? Does there need to be better coordination among agencies in interacting with the industry on a particular topic, or is this coordination effective today?
- How aligned in the pursuit of a common objective are regulators, institutions, industry associations, and service providers? If they are not aligned, is there an opportunity to better align them?
- Is there an established, consistent method for participating in the regulatory lifecycle, or does it change from regulation to regulation? Is this good or bad?
- How effective have industry associations been at creating channels of communication among leading thinkers in the industry and with regulators? What could associations do differently to be more effective?
- Do you see opportunities to better educate regulators on industry capabilities, technological maturity? What would need to change?
- What improvements to the regulatory process would make it more efficient to achieve cost effective, commercially reasonable processes much earlier in the regulatory lifecycle?

Analysis and Observations

Summary Observations

INTRODUCTION

The Analysis and Observations section is structured with a subsection devoted to each case study regulation or guidance. Key takeaways are summarized at the beginning of each case study; more detailed observations are included in the appendix and are organized by interviewee.

Before presenting the summary observations, we would like to share some perspectives on the data and its implications.

- **Facts and perceptions:** Interviews yield two types of information: facts and perceptions. Facts are those pieces of information that actually happened, e.g. a conversation that took place, or how an organization responded to the guidance. Perceptions are those opinions that are "true" in the mind of the interviewee. An example might be a belief that something didn't happen, simply because that person did not participate in it. For the purposes of this study, both facts and perceptions are the "data set" from which we draw our conclusions. In the recommendations section, we will address not only a set of solutions to improve the regulatory process, but also ideas on what can be done to increase "transparency" and address perceptions
- **Operational versus business-impacting rules:** Institutions view regulation and guidance as falling into two categories: operational or business-impacting. We heard that the general response to operational regulation and guidance (e.g. IT security, consumer privacy, fraud) is to "get it done." Institutions may respond to business-impacting regulation and guidance (e.g. credit card interest rates and terms and conditions) much differently and with much more vigor. As this study deals with operational aspects, the application of its findings may not be appropriate in business impacting situations
- **Number of regulators:** Reducing the number of regulatory agencies was a topic that we heard on several occasions. This is a topic that has been brought up with increasing frequency in the press and in debate in the US Congress. As an option for improving the regulatory process, it is out of scope for the purposes of this study

KEY OBSERVATIONS

Through the course of the interviews with financial institutions and service providers, we heard literally hundreds of perspectives on the regulatory process. Different institutions have had different experiences, and different people within the same institution sometimes hold different perspectives. In analyzing the results of the interviews, six themes emerge on the regulatory and supervisory process:

1. Some aspects of the regulatory process appear to be working adequately
2. The industry could benefit from changing how field examiners support implementation

3. The process could benefit from crisp and clear communication of new regulation and guidance
4. Collaboration among participants to form regulation and guidance exists but can be improved
5. Service providers and regulators can benefit from symposiums that enable communication on regulatory matters
6. Industry associations drive valuable communications among the participants, but there is an opportunity for them to further harness the perspectives of their members

Further detail on these six conclusions is provided below:

1. Some aspects of the regulatory process appear to be working adequately

While we gathered a diverse set of opinions, a number of interviewees provided positive views of the regulatory process. Examples include:

- **Regulators obtaining insights:** Regulatory agencies appear to be selectively obtaining insight from institutions and thought-leading vendors prior to releasing guidance (This process is not entirely "transparent" or visible to other participants)
- **Effective results:** The communication and interaction among financial institutions, service providers, industry associations and regulators is generally effective in recommending that guidance be risk-focused and not technology-specific or overly prescriptive, especially in the case of FFIEC Authentication guidance
- **Training of field examiners:** The regulators pursue efforts to train their field examiners on topics such as authentication, and have worked with major vendors to obtain education and awareness (through webinars) from vendors
- **Good relationships with field examiners:** Some institutions have a great deal of respect for their field examiners and have developed collaborative and effective approaches to implementing new regulation and guidance. (However, some other institutions have not met with the same success.)
- **Outreach efforts:** Regulators have conducted outreach efforts such as a webinar on Red Flags to help institutions understand the regulation

2. The industry could benefit from changing how field examiners support implementation

Some respondents appear to have achieved effective and open working relationships with the local field examiners. However, the more common feedback was that field examiners do not adequately support the rollout of new regulation and guidance.

Local field examiners have primary oversight of financial institutions and are furthermore responsible for the oversight of each institution's response to new regulation and guidance.

Some respondents appear to have achieved effective and open working relationships with the local field examiners. However, the more common feedback was that field examiners do not adequately support the rollout of new regulation and guidance. Perspectives include:

- **One way conversations:** Conversations with regulators are "one way", meaning that financial institutions and service providers provide interpretations and plans, but field examiners do not provide any meaningful feedback. Comments provided include:
  - Insight is withheld because field examiners want financial institutions to solve their own problems
  - A perception that field examiners are reluctant to offer insights because they do not receive appropriate training and communication from Washington
  - Insight is not provided because field examiners do not want to be held accountable for setting the bar too low
  - While the regulators in Washington are comfortable with a risk based approach, field examiners are not
- **Sharing successes:** Insights into how other institutions are addressing requirements are generally not shared
- **Inconsistent interpretations:** A belief that examiners are not consistently interpreting guidance across financial institutions
  - Field examiners monitoring compliance at a service provider did not raise concerns with the service provider's platform during its development/ enhancement (to comply with new regulation). After the platform was built and deployed to customers, a field examiner at one of the customer sites cited it for not being fully compliant
- **Need for new examiners:** The belief that the training of field examiners is not as much of an issue as the need for higher quality field examiners, which will only happen if Congress and the regulatory agencies increase their pay scales
- **Disconnect between authors and implementers:** A view that the regulators who write guidance are different from those who enforce it, which leads to different interpretations
- **Rewards system:** A perception that the reward system for field examiners measures who has the "best" financial institution (e.g. safest, most compliant) drives stronger interpretation of regulations by the field examiners
- **Recommendation to implement a specific technology:** A belief that field examiners wanted a financial institution to simply implement a specific technology that was being implemented at another large institution

In contrast to this, one service provider said that, in response to a request from the regulators, it provided training to examiners to help them become more knowledgeable on authentication topics and enforce compliance more consistently.

3. The process could benefit from crisp and clear communication of new regulation and guidance

The participating financial institutions do not believe new regulations and guidance are communicated as effectively as they could be—both verbally and in writing

A number of interviewees provided perspective on how regulation and guidance are communicated to the industry. These include how it is written, how it is disseminated, and at what point in the regulatory cycle it is produced. This is separate from the comments made previously that were related specifically to field examiners.

Related to written guidance:

- **Lack of consistent terminology:** A belief that there is a lack of clear and consistent terminology in written guidance, which causes confusion in interpretation
  - Terms such as security breach, identify theft, privacy, information security, and application have very specific meaning
  - One interviewee pointed out that the regulators did a good job in clearly defining "application" in the May 2008 Application Security bulletin[3]
- **Expansion of scope:** A perception that in cases where terminology has not been defined, the scope of regulation expanded based on questions asked by the financial institutions. One financial institution believes that if they had not asked if Interactive Voice Response (IVR)[4] was included in FFIEC Authentication in an Internet Banking Environment, it may not have been
- **Cognizance of downstream implications:** A desire among some financial institutions for regulation to be written with an understanding of the downstream implications. For example:
  - When the final identity theft red flags regulation was published with 26 "illustrative examples", there was some confusion among participants over whether the red flags were requirements
  - Some institutions are still addressing the ramifications of this situation in the education of their internal auditors, who are questioning why each red flag was not implemented

Related to how it is disseminated:

- **Interagency challenges:** A belief that there are special challenges for institutions in trying to comply with interagency guidance. The view from some financial institutions is that when guidance is explained by regulators in Washington, each agency tends to emphasize its own particular perspective, rather than the agreed upon interagency guidance

Related to timing:

- **FAQ timing:** Some financial institutions commented that Frequently Asked Questions (FAQs) are issued too closely to or after compliance dates. In the situation of Red Flags, the compliance date was November 2008, and FAQs were not issued until June 2009. If FAQs cause meaningful changes to interpretation of regulation or guidance, then a late release date may not allow sufficient time to implement revised approaches for compliance

[3] *OCC Bulletin 2008-16*, May 8, 2008.

[4] Interactive Voice Response (IVR) is an interactive telephone technology that accepts voice and keypad inputs to interact with callers, gather information, provide information, and route calls. In the financial services industry it is traditionally used, for example, to provide balance and transaction information, and to help route calls to specific operators based on the purpose of the call.

4. Collaboration among participants to form regulation and guidance exists but can be improved

Financial institutions and service providers interviewed believe that the process to form regulation and guidance could be much more collaborative among industry participants

Based on these particular case studies, the general perspective from both financial institutions and service providers is that the communication and interaction among participants was generally effective in making recommendations to improve regulations and guidance. However, a number of interviewees provided feedback on the process to form guidance.

- **Regulators seek perspectives:** Appreciation for those situations where the regulators sought perspectives from the industry prior to the issuance of guidance
- **More collaboration before draft issuance:** Belief that there is an opportunity for more collaboration between regulators and the industry before draft regulation or guidance is issued, as both groups have similar objectives such as protecting customers and combating fraud
- **Need to escalate internally:** A belief that the internal Government Affairs departments at financial institutions are not knowledgeable about security and privacy issues, and they could be made more so to help drive the agenda
- **Concern with traditional response mechanisms:** Some concern that the "traditional" industry response mechanisms such as comment letters and some industry mobilization efforts may result in adversarial relationships between financial institutions and regulators. A view that the process goes back 50 years, and is largely the same, while the world has changed over that time
- **"Black Box" view of the regulatory process:** A belief by some that the regulatory process is a "black box" and that financial institutions do not know if feedback on proposed guidance matters. Moreover, a belief that if financial institutions knew that feedback mattered, they would participate more actively
- **Small service providers have had too much influence:** A concern that service providers—especially smaller ones with untested solutions—have exerted excessive influence in shaping regulations and guidance, and that the regulators are overly receptive to their technology "solutions." In addition, an acknowledgement that service providers are effectively using the comment letter

process to make their views known, and are responding in greater numbers than financial institutions

5. Service providers and regulators can benefit from symposiums that enable communication on regulatory matters

Unlike financial institutions, service providers do not have an industry association to facilitate interactions with regulatory agencies or to support an understanding of how new regulations and guidance impact them.

Regulatory agencies have sponsored various symposiums for service providers, but one service provider pointed out that the last one was held in 1993. As the regulatory agencies have held several service provider symposiums since this date on topics such as pandemics and authentication, this statement indicates that there may not be adequate communication and awareness among service providers that this resource is available.

6. Industry associations drive valuable communications among the participants, but there is an opportunity for them to further harness the perspectives of their members

Financial institutions in the study believe that industry associations can provide additional services, enhance their capabilities, and structure the participation of their members to better harness the perspectives of the industry

Industry participants generally believe that industry associations such as BITS add value by bringing industry participants (e.g. financial institutions and regulatory agencies) together to discuss issues and solutions, enabling a network of experts and peers across institutions, and voicing opinions that financial institutions do not want to individually or publicly voice.

Participants also provided feedback that industry associations such as BITS can enhance their capabilities to address risk topics, can provide additional services of value to the industry, and need to reorganize participation in forums and conference calls to better gain perspectives from its members.

Related to improving capabilities:

- **Great facilitators, but need risk managers:** Belief that while industry associations such as BITS have strong facilitators, they could be strengthened (and more responsive) if they had strong risk managers on their staff

Related to providing additional services:

- **Insights into metrics and response strategies:** Additional value could be added by disseminating hard-to-obtain metrics that would be valuable in responding to regulators (e.g. how many AML people are on staff), and real time insights into how other financial institutions are complying with regulation and guidelines
- **Reframing positions:** A belief that in an environment in which increased regulation is likely, BITS should take on a more aggressive advocacy role and reframe the way in which it frames its positions. For example, considering the large infusion of government funds into financial institutions, BITS could take the

position that taxpayer money would be better invested in an environment that is more efficient, and costs can be lowered by reducing overlapping regulation

Related to industry participation:

- **Need for increased participation:** A view that there is sometimes very little participation and input by institutions on calls, which reduces the value of the conversation. Participants on calls may range from senior executives to project managers, and not knowing who is on the line causes attendees to remain silent
- **Identifying participants:** Belief that BITS needs to take a more structured approach to identifying resources from each institution who should be participating in various initiatives and on calls. Belief that broad communications from BITS asking for participation can create confusion within a financial institution
- **Segment participation:** Belief that industry association forums need to be segmented by financial institution size, as different types of institutions face different issues including organizational complexity, legacy environment, and maturity

Case Study Analysis

1. FFIEC Authentication in an Internet Banking Environment (2005)

BACKGROUND

In October 2005 the Federal Financial Institutions Examination Council (made up of the Federal Deposit Insurance Corporation, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration) released updated guidance on the risks and risk management controls necessary to authenticate the identity of customers accessing Internet-based financial services. The guidance, *Authentication in an Internet Banking Environment* was issued—in the words of the FFIEC—"to reflect the many significant legal and technical challenges with respect to the protection of customer information, increasing incident of identity theft and fraud, and the introduction of improved authentication technologies and other risk management strategies."[5] The guidance replaced the FFIEC's *Authentication in an Electronic Banking Environment*, which had been issued in 2001 and had been nonbinding.

The interagency guidance was a significant change from the technology-specific direction guidance appeared to have been taking as reflected in the FDIC's study *Putting an End to Account-Hijacking Identity Theft*, issued in December 2004.

On August 15, 2006, the FFIEC agencies released a FAQs document on the guidance. The compliance date was set for the end of December 2006.

Prior to the release of the guidance, BITS developed a policy statement that articulated the Financial Services Roundtable's position on authentication mandates. Policy statements are reviewed and approved by member company CEOs of the Roundtable

[5] See *Authentication in an Electronic Banking Environment,* August 8, 2001 (http://www.ffiec.gov/pdf/pr080801.pdf).

and serve as the primary means of outlining the association's advocacy views. Once the guidelines were released, BITS convened and facilitated multiple information-sharing sessions between BITS members and representatives of the Federal regulatory agencies that comprise the FFIEC.

Summary Perspective

The three financial institutions and two service providers interviewed on authentication guidance identified a number of positive perspectives, challenges, and specific recommendations to improve the regulatory process.

Positive Feedback

- **Regulatory feedback cycle worked:** The general perspective from both financial institutions and service providers is that the communication and interaction among participants was effective in recommending that the guidance be risk-focused and not technology-specific or overly prescriptive. Participants also voiced their belief that authentication is something necessary to protect customers and institutions; the guidance as it stands is not something they are opposed to
- **Regulators sought feedback:** Regulators actively sought out institutions and service providers to get perspectives on authentication prior to the finalization of the guidance
- **Good working relationships:** One institution in particular cited good, open working relationships with its onsite regulators as important in developing a common sense solution

Neutral Feedback

- **Operational regulation:** Two financial institutions viewed regulation and guidance as falling into two categories: "operational" or "business impacting." Operational refers to topics such as IT security, consumer privacy, safety and soundness, and fraud prevention. The general philosophy for responding to operational regulation is to simply "get it done." Business impacting refers to regulation and guidance that would change the business model. An example is the regulation of credit card interest rates, late fees, and other terms and conditions. Institutions may respond to business impacting regulation and guidance much differently and with much more vigor

Challenges

- **Service provider influence:** All three financial institutions cited concerns with service providers exerting excessive influence in shaping the guidance. This comment was predominantly aimed at smaller untested firms but one interviewee called out a number of large firms. There was a general view that regulators were overly receptive to the smaller firms with "solutions" that were too technology-specific. (As a counterpoint, a large service provider noted that it advocated on behalf of its customers for the regulators to pursue a risk-based approach and that the regulators were receptive to the feedback.)
- **Service providers use comment letters:** Service providers are effectively using the comment letter process to make their views known, and are responding in greater numbers than financial institutions. According to one interviewee, in the case of

FFIEC Authentication, out of thousands of banks perhaps only seventeen wrote a comment letter, while more than twice as many service providers did so

- **Lack of clarity in the guidance:** There is a perception that interagency guidance is challenging because even though it is agreed upon among agencies, each agency tends to pursue (or explain) it based on its own perspective. A lack of clear and consistent terminology in the guidance was cited for causing confusion. Lastly, there is a perspective that the regulators did not know exactly what they wanted when the guidance was issued, and the scope expanded as institutions asked additional questions
- **Training/calibration of examiners:** The interviewees generally spoke with their peers at other institutions to share perspectives on the guidance and gain insight on complying with its requirements. There is a perception that local field examiners are not adequately trained on guidance, and therefore interpret it inconsistently. This means that what is acceptable to one regulator at one financial institution may not be allowed by another regulator at another. A service provider expressed frustration that it communicated with its regulators frequently as it developed a solution, but after the solution was built and deployed, a field examiner at one of the customer sites cited a module within it for not being compliant. In contrast to this, one service provider said it was asked for and provided training to regulatory examiners so they could become knowledgeable on authentication topics and enforce compliance more consistently. Finally, there were views that the regulators who write guidance are different from those who enforce it, which leads to different interpretations
- **Pressure to use solutions in place at other financial institutions:** Financial institutions cited pressure from field examiners to implement approaches that were implemented at other institutions. This seemed to contradict the individual risk based approach set forth in the guidance
- **Tight compliance deadlines:** One large financial institution stated that the compliance deadline was too short for an institution of its size, and that it created an unnecessary burden

Recommendations

- **Opportunity to be proactive.** There is an opportunity for financial institutions to escalate industry issues and emerging threats more formally to their executive management and regulatory affairs groups—and proactively address these issues with legislative bodies and regulators. A specific topic the industry could rally around is the currently unregulated financial aggregation websites which provide risk to authentication methods by having customers reveal their login credentials. Finally, there is a general belief that industry participants have the opportunity to work much more closely to achieve good outcomes for the industry

Additional recommendations to improve the process that were not raised by the interviewees themselves are detailed in the "Recommendations and Implementation Steps" section.

2. FACTA Identity Theft Red Flags (2007)

BACKGROUND

The impetus for FACTA Identity Theft Red Flags was the belief that identity thieves were using people's personally identifying information to open new accounts and misuse existing accounts. The final rules[6] were issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. Under the Rule, financial institutions and creditors with covered accounts must have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft. The final rules became effective on January 1, 2008; the compliance deadline was November 1, 2008. (The FTC is delaying enforcement for entities under its jurisdiction until August 1, 2009. The financial regulators did not extend the deadline.)

A financial institution's program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft. The program must also help a financial institution to:

- Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the program
- Detect red flags that have been incorporated into the program
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft, and
- Update the program periodically to reflect changes in risks from identity theft

The agencies also issued guidelines to assist financial institutions and creditors in developing and implementing a program, including a supplement that provides examples of 26 "red flags" which give the requirements their common name. These red flags are not a checklist, but rather are examples that financial institutions and creditors may want to use as a starting point. The final rules also require credit and debit card issuers to develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card. In addition, the final rules require users of consumer reports to develop reasonable policies and procedures to apply when they receive a notice of address discrepancy from a consumer reporting agency.

SUMMARY PERSPECTIVE

The three financial institutions and two service providers interviewed on identify theft red flags note a number of positive perspectives, challenges, and specific recommendations to improve the regulatory process.

---

[6] See *Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule*, November 9, 2007 (http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf)

Positive

- **Effective operating and governance models may ease the response and implementation process:** Financial institutions that have effective models to address regulatory issues seem to have a more successful experience in achieving compliance than those that need to navigate a traditionally "decentralized" environment. Two of the financial institutions interviewed had relatively positive views of the regulatory process and achieving compliance. One in particular considers itself to have a very open and collaborative working relationship with the regulators, and a Compliance organization structure that can quickly assess the impact of regulation across the business and understand implications. The other has each of its attorneys dedicated to a particular regulatory topic (e.g. fraud); he or she works closely with the various lines of business and understands the implication of regulations on the business. A third financial institution, which had a generally less positive view of the regulatory process, also appeared to be more decentralized in its response

Challenges

- **Prescriptive regulation:** Although the regulation was finalized with the 26 red flags termed as "illustrative examples", there was some level of confusion among participants during the process over whether the red flags were requirements. One institution is still addressing the ramifications of this situation in the education of its internal auditors, who are questioning why each red flag was not implemented. This speaks to the need to issue proposed regulations with a view to the downstream implications. Some institutions on the other hand believed instantly that the 26 were only examples
- **Long time period from issuance to implementation:** Almost all interviewees commented on the long duration from issuance of the regulation to its implementation. One financial institution noted that they have had turnover in the people who were originally focused on this; long durations require additional investment in getting people up to speed on the situation
- **Concern over traditional industry response mechanisms:** One financial institution in particular voiced concerns over the "traditional" comment letter process, noting that they believe it tends to result in an adversarial relationship between financial institutions and regulators. One participant noted that the process goes back 50 years, and is largely the same, while the world has changed over that time. Another perspective was that the industry response was overblown. One financial institution relayed that on an industry association call another institution said that it had dozens of people on taskforces to address red flags. The view of the first institution was that the industry tends to stereotypically jump to worst case interpretations
- **Communication:** There was continued feedback that communication and insight from the field examiners is not where it needs to be. There is a view that communication with the regulators is "one way." The regulators are not providing perspective, guidance, or insights into how others are addressing the regulation. There was also a perspective that the field examiners are not receiving appropriate training, guidance and communication from Washington, and that this adds to their reluctance to offer insights and opinions. One interviewee stated that the issue is not training so much as the need for Congress and the

regulatory agencies to increase their pay scale so they can recruit higher quality people

- **Some desire for industry standards:** There was some desire to see standard industry practices and consistency, especially in operational regulation that is based on a risk management framework. The view is that when an industry standard isn't set, there is a tendency to implement a solution much greater than necessary

Recommendations

- **Need for service provider forum:** One service provider stated that the last symposium for service providers was in 1993. It believes these forums should be resurrected to provide clear and consistent information to service providers. This is necessary because there is no organization for service providers; they need the regulatory agencies to provide the structure to bring them together. (The regulatory agencies have held several service provider symposiums since 1993 on topics such as pandemics and authentication, which indicates that there may not be enough communication and awareness in the industry that this resource is available.)
- **Early perspectives from industry participants:** One financial institution noted that there is an opportunity for more collaboration before draft regulations are issued; regulators should get the perspective of institutions earlier in the process. The view is that both entities have the desire to protect customers, and they can share perspectives on the topic earlier

3. Interpretive Guidance on Customer Breach Notification in the Gramm-Leach-Bliley Act (2005)

BACKGROUND

The FFIEC agencies jointly issued *Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (FIL-27-2005) on April 1, 2005. The guidance is an interpretation of section 501(b) of the Gramm-Leach-Bliley Act and the Interagency Guidelines Establishing Information Security Standards (12 CFR 364, Appendix B). The Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) was signed into law in 1999. The interpretive guidance states that financial institutions should develop and implement a response program designed to address incidents of unauthorized access to sensitive customer information maintained by the financial institution or its service provider. The interpretive guidance describes the appropriate elements of a financial institution's response program, including customer notification procedures.[7]

At a minimum, an institution's response program must have procedures to address:

[7] *Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, April 1, 2005 (http://www.fdic.gov/news/news/financial/2005/fil2705.pdf)

- Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused
- Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information
- Consistent with the agencies' Suspicious Activity Report (SAR) regulations, filing a timely SAR, and in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, promptly notifying appropriate law enforcement authorities
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information
- Notifying customers when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it

Because the guidance was merely an interpretation of 501(b), it had no effective date.

Since the issuance of this guidance, most states have issued much more stringent and prescriptive regulation on data breach notification.

This case study is focused on understanding the implications of regulation originating in both the Federal and state domains, sometimes with significant inconsistencies.

SUMMARY PERSPECTIVE

The general view on the breach notifications section of the Gramm-Leach-Bliley Act and the implications on future regulation are mixed.

No interviewees identified breach notification requirements coming from the states as a significant burden. The majority of those we interviewed implemented solutions that "raise the bar" and address across all states the standards put forward by the toughest state.

One institution commented that meeting the individual state requirements is a normal cost of doing business in the United States.

Some institutions commented that addressing fewer sources of standards is certainly easier than addressing more. To this end, they suggested that the federal government should put forward regulation that is more comprehensive, and which preempts states governments from having to act on their own.

Recommendations and Implementation Steps

INTRODUCTION

The results of the interviews with the financial institutions and service providers indicate that there are opportunities for all participants to take some action to improve the regulatory lifecycle. It is not simply a matter of the regulatory agencies changing their processes.

The recommendations are divided into two types: "strategic initiatives" and "tactical improvements." Strategic initiatives are undertakings that require detailed planning and structured execution. These should have a medium to large impact on the regulatory lifecycle. Tactical improvements are undertakings that are more basic in nature and should require less planning and effort to implement. Individually a tactical improvement may have a low impact, but a number of them taken in concert could have a more significant result.

For each strategic initiative we have outlined a number of activities. In some cases these are visions of the future process, and in others they are the major work steps to begin implementation.

While some of the strategic initiatives are fundamental changes to the current process, the extent of this change should not necessarily deter industry participants from exploring them further. In many cases the proposed initiatives (or components of them) can be piloted so their impact is better understood. From there, where successful, they can be further implemented. And where not successful, they can be modified or discontinued.

The interviews with the financial institutions and service providers point to six strategic initiatives to help improve the regulatory process:

1. Use a centralized project management model to implement new regulation and guidance; better support the field examiner's role in the process.
2. Improve collaboration on draft regulation and guidance
3. Industry associations should strengthen efforts to better harness the knowledge of their members
4. The industry should lead with a proactive agenda on operational regulation
5. Institutions should organize internally to better respond to regulations and guidance
6. Continue to engage service providers through regulatory agency-sponsored symposiums, but make sure service providers are aware of the opportunity

Strategic Initiatives

1. Use a centralized project management model to implement new regulation and guidance; better support the field examiner's role in the process.

To achieve a more consistent dissemination of new regulation and guidance, regulators should consider adopting a centralized "project management" model, rather than relying predominantly on field examiners. This can be conducted in a manner that preserves flexible, risk-based approaches.

With few exceptions, one of the greatest challenges voiced in the interviews was that field examiners are not adequately supporting the roll-out of new regulation and guidance. Financial institutions and service providers alike expressed concern that field examiners are not forthcoming with information, might not be adequately trained, are providing inconsistent information from institution to institution, and are too far removed from understanding the original intent of regulation or guidance.

To achieve a greater level of consistency and better address the needs of the financial institutions, regulators could build on traditional program and project management principles, used frequently to effectively and consistently manage large implementation efforts. Some concepts include:

- **Steering committee:** Convene a steering committee that is responsible for overseeing the successful rollout of a particular regulation or guidance, and determining what changes may be required to draft rules. In the event of interagency guidance, the steering committee could be made up of representatives from each of the participating agencies
- **Program manager and core team:** Select a program manager who is responsible for the day-to-day management of the rollout. Build a "core team" of resources to support the program manager with communications, tracking questions, issues, etc. For continuity, include an expert who participated in forming the regulation or guidance. (This could be a part time or advisory role.)
- **Create implementation teams, if necessary:** Depending on scope or complexity of a particular regulation or guidance, create one or more "implementation teams" that report directly to the program manager. These teams could be structured by financial institution size, region, or other attribute (possibly building on an existing structure already in use by the regulatory agencies). They would manage the rollout to a smaller set of financial institutions
- **Define role of field examiner:** Define and manage the responsibilities of the field examiners with respect to the rollout of new guidance, especially in the early stages of rollout. Their responsibilities could range from actively overseeing the financial institution's development of an approach (particularly at medium to larger institutions), to simply having knowledge of it based on participation in meetings with the financial institution and implementation teams. Field examiners can be an asset to the process, and there is an opportunity to better integrate them into it
- **Comprehensive training:** Develop training manuals and conduct training of regulators to promote consistent enforcement
- **Communications strategy:** Follow a communications strategy and protocol that drives consistent messages to financial institutions and appropriate service providers
- **Regular communications:** Hold regular conference calls and meetings designed to consistently and comprehensively answer questions from institutions. Invite both industry participants and field examiners so they hear the same messages

- **Share insights** into how different institutions have proposed implementing the guidance
- **Gather questions:** Oversee efforts to gather questions from across the industry, and provide consistent answers (e.g. questions are routed to the core program management team)
- **Manage issues and risks:** Actively manage issues and risks (e.g. such as the need to revise draft guidance) and escalate to the Steering Committee for decisions
- **Gather data to understand success:** Conduct some level of data gathering and reporting to understand the level of understanding or adoption across the financial system

While a centralized team approach may appear to be more resource intensive, it may actually enable financial institutions and regulators to remove inefficient iterations from the process, and do more with less.

Some institutions have very effective and collaborative working relationships with their field examiners. Others do not. The skill set, communication style, and personality traits of a particular field examiner or banking representative is likely a factor in the effectiveness of these relationships. This means that while the regulatory agencies could institute more rigorous training for field examiners on new regulations and guidance, it may not achieve the desired level of consistency. A program such as the one outlined above would better integrate field examiners into a larger process and help drive consistency across the banking system.

2. Improve collaboration on draft regulation and guidance.

Regulators should expand their efforts to gather industry feedback prior to the issuance of new regulations and guidance; the industry and regulators can function much more collaboratively.

Regulators and financial institutions appear to agree on the need to address "operational" issues such as IT security, consumer privacy, and fraud. The difference often appears to be in perspectives on "how" to address them.

Many interviewees stated that they appreciated those situations where the regulators sought perspectives from the industry prior to the issuance of guidance, or where there were industry association symposiums held on a particular issue. There is an opportunity to expand this effort, not only in gaining industry perspectives, but also in providing some level of transparency into the efforts of the regulators so the industry knows it is happening.

This recommendation is made with the understanding that the regulatory proposal and rulemaking process is driven by the legal infrastructure in which the regulators operate. Thus, process change may need to be preceded by legal changes to that rulemaking process.

A framework for a collaborative initiative might function as follows:

- **Select an issue:** The regulators could select an issue that is under consideration for guidance and agree to pilot a more collaborative approach

- **Determine legal framework:** Develop a strategy to make activities comply with any "open hearings" type laws
- **Sample institutions:** Regulators could gauge true interest by speaking with a sample of financial institutions and thought-leading service providers
- **Shore up support:** Announce that some guidance will be issued and the objective is to gain early feedback into it. This will help shore up support from the institutions (i.e. this is not about creating new regulation, but about providing early feedback into regulation that will be issued)
- **Convene a working group:** Based on interest from financial institutions, regulators could convene a working group of engaged, constructive, thought-leading participants
- **Define the issue, explore options:** Work through defining the core issue to be resolved, then options on how to resolve it
- **Engage industry associations** for subject matter expertise and in communicating efforts of the pilot initiative
- **Merge into normal process:** Proceed with normal rule making process (e.g. comment letters, etc.)
- **Evaluate success:** Create metrics and evaluate the process against the more traditional process (e.g. is the process a black box, is it adversarial, is the comment period shorter, are significant revisions necessary, is implementation satisfactory)

This effort could be a first step in addressing the feedback from the industry that the regulatory process is a "black box" and that the traditional industry response mechanisms may result in more adversarial relationships between financial institutions and regulators. Moreover, it could also help to shorten the traditional comment period, define more effective solutions, and achieve faster implementation of new guidance.

3. Industry associations should strengthen efforts to better harness the knowledge of their members.

Industry associations could undertake additional efforts to strengthen their interactions with their memberships to better harness the knowledge and perspectives from across the industry.

One of the success factors in working collaboratively across financial institutions and the regulators is making sure that the leading thinking from the industry is presented. The feedback from many financial institutions is that industry associations such as BITS can strengthen efforts to structure the participation of its members to better harness the perspective of the industry.

To this end, BITS could consider:

- **Strategy for obtaining participants:** Reevaluate how it secures participants from the institutions, working closely with its advisory council and board on strategy, and working exclusively through a key liaison at each back to identify participants

- **Define roles:** Clearly defining roles, responsibilities, and attributes of ideal participants—paying special attention to the level of person that should attend (e.g. executive or project manager)
- **Discontinuing broad communications** to each bank seeking participation
- **Consider segmentation:** Develop a strategy to determine if committees, phone calls, forums, and other venues for communication should be segmented (by an attribute such as financial institution size), so the conversation is more valuable to each group of participants
  - **Subcommittees:** BITS could consider the use of subcommittees to gather the perspectives from each group and an overarching committee to synthesize these perspectives
  - **Segregate beginners:** Consider holding a series of "beginners" calls throughout the response efforts, so those financial institutions who are late to the process do not hold back the other institutions
- **Define expectations:** Define the expectations for participants on calls (e.g. talk or listen) both to change behavior and to set expectations. For example, if the purpose of a call is for the audience to listen, people should not leave with the impression that participation was low
- **Use participation strategies:** Incorporate strategies to improve participation. For example, if institutions are not asking questions because they do not want to be identified, enable them to send real time questions via email

4. The industry should lead with a proactive agenda on operational regulation

Financial institutions and industry associations should develop a proactive agenda that can be pursued by the industry and communicated to the regulatory agencies.

There is some belief among financial institutions and service providers that the industry is in a defensive or reactive mode when it comes to responding to and implementing new regulation and guidance. The industry can be much more proactive in identifying a platform of operational issues, which in turn can help collaboratively drive the regulators' agendas. This aligns with what we heard about the shared objectives of the regulators and industry (e.g. prevention of fraud, protection of customers, etc.) and the belief that the industry is facing regulation and guidance because it did not effectively communicate that many of the components of new regulation or guidance were already in place.

There is also a view that much regulation in the security and privacy space is overlapping. The specifics of this were out of scope for this study, but a number of participants believe that mapping new regulation or guidance to a framework or standard (e.g. ISO) would be effective at communicating where new regulation already exists and where it may be needed.

Developing a proactive agenda could be led by an industry association such as BITS which could:

- **Convene a group** of thought-leading financial institutions who have the pulse on operational issues that need to be addressed

- **Develop guiding principles** for how financial institutions can more proactively drive an agenda of operational issues
- **Collect suggestions** for specific initiatives that the industry and/or regulators could pursue. Some suggestions provided included:
  - Oversight of personal finance management websites which provide aggregated views of a consumer's financial position, but also pose a risk to authentication methods by having customers reveal their login credentials
  - Federated ID
- **Select an industry framework** or standard (e.g. ISO) and map existing regulation or guidance it to identify where regulation already exists and where it does not
- **Service providers:** Invite thought-leading service providers to the discussion
- **Prioritize and develop positions:** Create an inventory of operational issues, prioritize the list though discussions with a broader group of financial institutions, and begin to develop positions on each
- **Initiate discussions with regulators** to share perspectives and collaborate on an agenda

5. Institutions should organize internally to better respond to regulations and guidance.

Institutions can pursue more effective operating models to more effectively navigate the regulatory environment—driving an agenda, responding to proposed requirements, and mobilizing to implement.

To more effectively navigate the regulatory lifecycle, financial institutions can consider changes to their operating models. These changes could help drive the regulatory agenda, support responding to proposed regulation or draft guidance, and successfully mobilize to implement new regulation and guidance.

Throughout this paper we have commented on effective practices in place at financial institutions, as well as opportunities to improve those practices. These include:

- **Escalate perspectives** to executives and Government Relations/Regulatory Affairs departments on operational issues that have the potential to become future regulatory initiatives
- **View the pipeline:** Have an effective mechanism is in place to spot and understand regulations and guidance that is in the pipeline
- **Create specialists on regulatory topics:** Consider aligning individuals in Legal or Compliance with particular regulatory topics (e.g. authentication, privacy) so one person can quickly coordinate and understand implications, overlaps, and who from the organization needs to become involved
- **Effective internal communication channels:** Where a financial institution has a number of business lines, have a structure in place that can quickly assess implications across the business lines and business units—including Information

Technology. Make sure there is clear communication between the group making commitments to the field examiners, and those groups who will need to perform the work (e.g. IT)

- **Build risk management capabilities:** Put less focus on building "compliance oriented" structures, and more on building risk management perspectives and capabilities.
- **Build risk management capabilities, rather than Enable honest conversations:** Where there are already regular risk management and compliance meetings in place, consider adding, if communication needs to be more honest and direct, a less frequent risk and compliance meeting with a smaller audience
- **Meet regularly with regulators** to share progress and obtain feedback

6. Continue to engage service providers through regulatory agency-sponsored symposiums, but make sure service providers are aware of the opportunity.

There may be an opportunity for the regulators to improve communications with the service providers (and vice versa), so service providers are aware that this resource is available.

The regulatory agencies should continue to sponsor service provider symposiums that provide clear and consistent information on regulatory matters to service providers. These symposiums can be especially valuable because service providers do not have an industry association to facilitate interactions with regulatory agencies or to support an understanding of how new regulations and guidance impact them.

There may be an opportunity for the regulators to improve communications with the service providers (and vice versa), so service providers are aware that this resource is available.

- For service providers with regulated operations, each field examiner should confirm the point of contacts within the company that should be made aware of service provider symposiums
- For service providers without regulated operations, the regulatory agencies could expand their database of service provider contacts by
  - enabling enrollment or sign-up on regulatory agency websites
  - obtaining contact names from previously submitted comment letters
  - allowing service providers to sign-up at various industry events
  - working with financial industry associations who may be able to provide additional contacts
  - using its network of field examiners at financial institutions to submit the names of active service providers who should be made aware of service provider symposiums

On a regular basis, the regulatory agencies could ask each service provider to identify the individual(s) who should receive communications on upcoming events.

Tactical Improvements

Tactical improvements are undertakings that are more basic in nature and should require less planning and effort to implement. Individually a tactical improvement may have a low impact, but a number of them taken in concert could have a more significant result. As these recommendations are fairly straight-forward, they are not described in great detail. Based on the interviews, opportunities include:

1. Until other mechanisms are put in place, financial institutions should continue to take advantage of using comment letters to voice their perspectives and help educate the regulatory agencies
2. In situations where a financial institution believes that its field examiners are not appropriately interpreting regulation or guidance, the institution should confer with the regulatory agency contact listed on the regulation or guidance
3. When issuing rules, regulators should include a section on terminology and define terms
4. Regulators could make an effort to be cognizant that that technology "solutions" from smaller service providers may be untested
5. If there are delays in issuing documents (such as FAQs) related to a regulation or guidance, regulators should attempt to communicate some insight into when they might be issued

Appendix

1. Interview Detail on FFIEC Authentication in an Internet Banking Environment (2005)

Detailed Perspectives by Institution/Service Provider

Financial Institution A

Financial Institution A provided perspectives on the challenges of interagency guidance, a disconnect between those writing guidance and those implementing it, the "calibration" or training of examiners to drive consistent application of regulation across institutions, consistent terminology, and the role of service providers in influencing guidance.

At the time of this guidance, Financial Institution A stated that it did not have a mature operating model in place to monitor the regulatory landscape and coordinate its response across the organization. The predominant method of responding through this regulation was through BITS.

Financial Institution A believes that interagency guidance is "inherently bad" and that there are special challenges for institutions trying to comply with it. Their view is that there are conflicting interests among the regulatory agencies, and through a negotiation process the agencies present a mutually agreed upon written document.[8] However, when the guidance is explained verbally, the regulators appear to revert to the original opinions or perspectives of their own agencies. This causes confusion among the financial institutions.

The example cited for this is the three two-hour calls BITS hosted on FFIEC authentication guidance. Over the course of the three calls, the regulators explained the guidance first as "authentication", then as "not authentication but layered security", and finally as "layered security with good authentication."

Financial Institution A believes that regulators do not conduct training necessary to "calibrate" their examiners so that rules are consistently applied across institutions. Financial Institution A cited that a regulatory agency admitted this on a BITS call. This is important because examiners provide input to institutions as they develop plans to comply with regulation. Institutions communicate with each other to determine appropriate practices to comply with regulation. It is frustrating to institutions when they see a competitor achieve compliance with an approach that their own examiner does not agree with, or when they are not able to pursue a solution that they have seen accepted among their peers.

Financial Institution A perceives that something is lost in the handoff between those crafting rules and those overseeing the implementation of them. In this case both the institution and the field examiners are interpreting guidance for the first time, which leads

[8] Financial Institution A cited an agency's decision to issue guidance on application security in May 2008 (OCC Bulletin 2008-16) as another example of conflicting interests across regulatory agencies. The guidance was not interagency, but solely through one agency. According to the institution, at a BITS forum on the topic, the regulatory representatives announced that they "agree to disagree."

to confusion. They believe that someone who crafted the rules should help lead the implementation of those rules, rather than moving on to craft the next set of guidance.

Financial Institution A commented that the guidance is mistitled and this caused confusion. While the official title is *Authentication in an Internet Banking Environment*, the guidance is also applicable to ATMs and call centers. Their view is that the regulators create confusion when they loosely use terms such as security breach, identify theft, privacy, information security. To them, each of these terms has a very specific meaning. (They also pointed out that the regulators did a good job in clearly defining "application" in the May 2008 Application Security guidance.)

A final comment from Financial Institution A is that service providers—regardless of size—hold too much sway over the regulatory process, and overly influence regulators by touting untested "solutions." While there is no way to prevent service providers from talking to the regulators, Financial Institution A felt that industry associations should try to avoid creating environments where service providers can easily access regulators. They cited that when BITS held a forum on authentication guidance, the service provider session was scheduled just after the examiner roundtable, and that created an environment for both groups to interact.

Financial Institution B

Financial Institution B generally found the regulatory process to address authentication a positive experience, though they did provide some perspectives on service provider influence and the consistency of implementation across financial institutions over time.

Financial Institution B holds a particular philosophy on regulation that helps shape its perspective. First, it differentiates between "operational regulation" (e.g. safety and soundness, IT security) and "business-impacting regulation" (e.g. credit card interest rates and terms and conditions). Business impacting regulation may be addressed very assertively. The general response to operational regulation is: "let's just figure out a way to get it done." The Financial Institution's view is that much of the Federal regulation in security and privacy is not innovative, and should be in place anyway.

Second, Financial Institution B's perspective from Compliance and Risk Management is that they have developed very strong working relationships with the regulators, and they have a good organizational structure to support responsiveness. This operating model has led, in their view, to common sense approaches for complying with regulation and guidance.

Financial Institution B views the regulatory process for authentication as a positive experience. The Information Technology group remarked that one regulatory agency called from Washington to gather perspectives on the issue before guidance was released. They commented that the efforts of BITS, especially in bringing the industry and regulators together on conference calls to share information, serve as a good model. The Financial Institution also views BITS as successful in structuring a dialog that showed the regulators that they need not dictate what technology financial services companies should use, and in showing the effectiveness of incorporating compensating controls.

Financial Institution B believes that service providers had a larger voice in driving the regulation than the industry. Financial Institution B believes that service providers are effectively using the comment letter process to make their views known, and are

responding in greater numbers than financial institutions. According to this institution, for FFIEC Authentication, out of thousands of banks only perhaps seventeen wrote a comment letter, while more than twice as many service providers did so. Financial Institution B also perceived that many of the service providers were smaller ("fly-by-night") and did not have credible solutions, yet their perspective was taken seriously by the regulators.

Finally, Financial Institution B perceived that those institutions who implemented solutions later "did better" than those institutions that implemented solutions earlier. More specifically, the regulatory agencies embraced the risk management aspects more fully as time progressed.

Financial Institution C

Financial Institution C provided perspectives on the overall objectives of the regulators and clarity of guidance, the influence of service providers, tight compliance dates, and being compared to other financial institutions by the regulators. The Financial Institution also shared perspectives on emerging issues in the authentication domain.

Financial Institution C believes the authentication guidance was not well defined (had "a lot of grey areas") and that the regulators didn't know exactly what they wanted. An example cited is that when the financial institution asked if Interactive Voice Response (IVR) was included, the regulators responded "um, ye...yes!" Two issues emerge. The first is that the regulation could have been clearer, and specific terms could have been defined. The second is that the financial institution now feels hesitant to ask questions, believing that if they had not asked about IVR, it may not have been in scope.

Financial Institution C believes that service providers had too much voice in influencing the regulators, and that the regulators were overly receptive to claims made by service providers. The Financial Institution viewed many of the service providers as "brand new" with untested solutions. They also commented that as regulators assessed the technology landscape, they should have also considered that there was not enough technology capacity or scale across the service providers to support specific technology solutions for the entire industry. According to this institution, this serves as further support for a risk based model.

While Financial Institution C believes the final guidance was correct, they feel strongly that the compressed timeline was not. Once guidance was issued, they had fourteen months to interpret and implement a solution across a large company with many electronic channels.

Of particular concern to Financial Institution C was the continued pressure from the examiners to implement a technology that was being implemented by another large financial institution. The Financial Institution had a number of contentious conversations with its examiners, because the institution did not want its response to be tied to one particular tool. One perspective outlined is that while regulators in Washington may be open to a risk based assessment, the local field examiners are held accountable, and lean toward tactical solutions. The Financial Institution also feels that the guidance provided by field examiners was not consistent.

The Financial Institution also shared perspectives on emerging issues in the authentication domain. The Financial Institution is concerned about the proliferation of financial account aggregation websites. Customers are giving away their login

credentials to have simplified access to many of their accounts. The Financial Institution expressed concern about security levels at these firms, and wondered what would happen to the data and servers should one of these firms go out of business. The Financial Institution believes that these companies/sites should be regulated—not only should the playing field be level, but also there is a need for customers to be protected. There is an opportunity for the financial services industry to champion this issue with the regulators.

Service Provider A

Service Provider A provided a positive perspective on the regulatory process—especially with respect to the regulators gathering information on authentication and pursuing training for its examiners. Service Provider A shared insights into service provider/regulator interactions, and the perception of industry participants on this interaction. Finally, Service Provider A shared opinions on how the financial industry can better educate legislators and regulators on industry issues and perspectives, and how the industry can work more collaboratively on industry issues.

Service Provider A stated that when the FDIC issued its 2004 study *Putting an End to Account- Hijacking Identity Theft*, it talked to different experts in the field. Because Service Provider A understood the landscape of authentication and had experts in this area, our interviewee put the FDIC in touch with technical experts in the company. These experts spoke to the FDIC not only about what existed in authentication, but also about what was coming. Service Provider A encouraged the FDIC to not be technology-specific, as a specific technology would only have supported a short-term solution until threats or technology evolved.

Service Provider A believes that its foresight into authentication technology helped to shape the broader risk-based and layered approach that was put forward in the authentication guidelines.

Service Provider A's view of the regulatory process is that the regulators came to "a pretty good place" with FFIEC authentication. Service Provider A would support more guidance being developed in this manner.

Service Provider A noted that some financial institutions were caught off guard when the study was circulated and their first reaction was to simply say "kill this" and push back. Service Provider A believes that now that the guidance has been largely implemented, people generally say that it works.

Service Provider A believes that the regulators did a good job in getting the examiners trained uniformly across the FFIEC as the regulation was implemented. In addition, the regulators asked Service Provider A to conduct a webinar for its examiners on emerging fraud trends, including cross-channel fraud, after the FFIEC guidance deadline had passed, in order to stay informed of evolving threats. Service Provider A believes that the regulators try to consistently understand the threats, the practices and technologies that can help mitigate those threats, and that they conduct ongoing training across the FFIEC institutions for the examiners.

Service Provider A shared its perspective on the perception some industry participants may have on its interaction with the regulators. Service Provider A stated that there was some mistrust by the financial industry associations on what companies such as his tell the regulators. Service Provider A stated that it advocated on behalf of its customers to

help them address their risks. Service Provider A stated that many customers knew it was having discussions with the regulators and were grateful. Service Provider A also said that the leading voices at the financial industry associations weren't focused on the authentication topic and the regulators knew that Service Provider A was. Finally, Service Provider A stated that the financial services industry is an important customer. It does not advise the regulators to be prescriptive or advocate for additional regulation on the financial industry.

Service Provider A also stated that the regulators came to them because they knew the content and because service providers are generally collaborative. An overly defensive stance by the financial industry prompts the regulators to go to the service providers for information.

Service Provider A commented that at the time, the lobbyists for financial institutions knew very little about issues such as authentication. While Chief Information Security Officers (CISOs) talked to other CISOs, they were not escalating issues to more senior executives, lobbyists, or industry associations. Service Provider A believes that the industry needs to escalate and get in front of issues earlier, rather than defensively react to proposed regulation.

With regard to industry associations, Service Provider A believes that BITS had some good representatives focused on this topic, but that they didn't have anyone who could talk technically about authentication at the time the FDIC report was issued.

Finally, Service Provider A stated that there is and will be some dynamic tension between the regulators and the industry. However, if regulators, institutions and service providers worked more closely, they could accomplish a lot. There is a great deal of expertise at the CISO level and with the financial services regulators who are eager to learn.

Service Provider B

Service Provider B stated that it has very good relationships with its examiners and has worked hard to achieve this state. However, Service Provider B shared its perspective on inconsistency across examiners.

Service Provider B worked closely with the regulators to develop solutions for multifactor authentication, sharing its interpretations of the guidance and plans for its work to achieve compliance. Service Provider B updated its products by the deadline of December 2006. However, in mid-2007 a field examiner at a client using Service Provider B's technology cited the client for not having multifactor authentication for administration in place. When Service Provider B was developing its solution, sharing plans and progress with the regulators, none of the regulators provided any feedback that authentication was needed for this component. Service Provider B does not think there is consistency among the agencies in what the field examiners are examining. Moreover, Service Provider B was told that guidance on authentication for administration was forthcoming; it has been over a year and has yet to be issued. Service Provider B stated that it wants to--and is in its best interest to—comply with regulation, but regulators need to communicate better so it can do so.

2. Interview Detail on FACTA Identity Theft Red Flags (2007)

DETAILED PERSPECTIVES BY INSTITUTION/SERVICE PROVIDER

Financial Institution A

Financial Institution A's perspective on FACTA Red Flags called out the difference between "business" and "operational" regulation, some concern over the potentially prescriptive nature of the regulation, the length of time to implement, and the view that a good organizational structure can make compliance easier.

Financial Institution A prefaced its comments on FACTA Red Flags by noting that when regulatory issues may affect its core business—such as regulation on credit card late fees—it will vigorously and proactively communicate its position. But on "operational" regulation, while they submit comment letters and convey their opinions, their primary focus is on achieving compliance. They take the perspective that they can only be passionate about so many things, and because many of the operational regulations are "motherhood and apple pie", they cannot really be opposed anyway.

When the proposed rule came out in July 2006, Financial Institution A attended multiple forums and also submitted a comment letter. They stated that in situations where they feel strongly about an issue, they try to coordinate the content in their comment letters with those of other institutions. In this case they did not.

Financial Institution A had some concerns with the 26 red flags being interpreted as prescriptive rather than serving as examples. External counsel advised them to proceed as if they were examples.

The "jury is still out" on getting a view from the regulators on whether they interpreted and implemented their solution adequately, as Financial Institution A has not yet had the regulatory examination that covers Red Flags. Financial Institution A added, however, that its own internal audit group is having some difficulty in not considering the 26 flags as prescriptive requirements.

Financial Institution A commented that the implementation of FACTA has taken an extremely long time, as the legislation was originally passed in the early 1990's, though amended in 2003. Their perspective is that organizations (both financial institutions and regulators) lose focus over time, and this creates inefficiencies. Each time the regulation is resurrected, people have to invest time in getting up to speed again. Moreover, people who originally provided feedback have since left the organization, and this creates a disconnect.

Finally, Financial Institution A provided some perspective on their organizational structure which they believe makes compliance easier. They have aligned their attorneys in the Legal department with specific issues (e.g. authentication). The assigned attorney follows the end-to-end process from regulatory monitoring, to response, to implementation. The attorney understands how regulations on the topic overlap, how the business operates, and with whom to work in the various business units to determine implications and response. By having a point person on a topic who serves the enterprise, Financial Institution A is able to understand not only the regulation, but also the implications to the business. From a regulatory response perspective, this organizational structure enables the organization to quickly understand implications and how it should respond.

Financial Institution B

Financial Institution B's perspective is that FACTA Red Flags made sense. They believed that it was aligned with its anti-money laundering program and how the financial institution manages a central view of customers. Moreover, they came to the conclusion that they may be better situated to respond than some of their competitors. Hence, they did not participate in the process to provide a different perspective to the regulators. They took a passive role with the industry, and participated in various CIO groups and industry association discussions—mostly in a "listening" capacity.

Financial Institution B has a strong relationship with its regulators and believes that they can be very open and transparent with them on their perspectives and plans. They view their interactions as collaborative, not defensive. In this case the financial institution met with the regulators and came up with a common sense solution that met both of their objectives and was cost effective. Financial Institution B believes that involving regulators early and putting forward a proposed solution are keys to success.

Financial Institution B shared that they viewed the 26 red flags as examples, not mandates or prescriptive regulation.

Financial Institution B provided some perspective that they thought the industry response was "overblown." Specifically they said that some of the financial institutions had dozens of people on taskforces. They believe the industry tends to jump to worst case interpretations.

Financial Institution B put forward the view that comment letters and traditional responses tend to result in an adversarial relationship between financial institutions and regulators. They believe that extreme positions get plugged into comment letters (because there are "too many cooks in the kitchen"). They also believe that comment letters seem to be formulaic, i.e. "we strongly disagree with the proposed regulations...we have this in place already...nobody cares about the consumers more than we do...this regulation will add an unacceptable burden and cost to the banking system." The implication is that the response to proposed regulation has become routine.

While Financial Institution B made an early decision to move forward quickly because the regulation was aligned with its capabilities and competitive position, it simultaneously voiced an interest in seeing standard industry practices and consistency. Their view is that when an industry standard isn't set, there is a tendency to implement a solution much more stringent than necessary.

Financial Institution C

Financial Institution C views the regulatory comment period as a "black box." After it received the draft regulation, it provided a comment letter. It believes that Regulators had already decided what they wanted the rules to be and were not going to make significant changes in response to input from Institutions or Service Providers. When the final regulation (and preamble) was issued, many of the comments it made were not included.

Financial Institution C believed that problems with definitions (e.g. what is a "covered account") and lack of clarity around whether the Red Flags that appeared in the rule were mandatory or merely examples, complicated the process.

From a timing perspective, Financial Institution C believed the rules were long on development and short on implementation time. To meet deadlines, Financial Institution C started implementation of Red Flags several months before the final rules were issued. Moreover, the FAQ document (at the time of this interview) had not been issued by the Regulators. (It was issued in June 2009.) In general if FAQs cause meaningful changes to interpretation of regulation or guidance, then a late release date may not allow sufficient time to implement revised approaches for compliance.

Financial Institution C expressed frustration that its conversations with regulators were "one way." It met with its field examiners on a quarterly basis to discuss interpretation and progress, but did not receive any meaningful feedback from them. On one occasion, the feedback from the field examiners was that "we haven't gotten our heads around it."

Financial Institution C also has the sense that poor communications from the regulators affects not only financial institutions but also the regulatory community. The institution said that after the regulators delivered a webinar on Red Flags to financial institutions, the local field examiners approached their institution, said they had heard a webinar had been conducted, and asked for copies of the materials. The Financial Institution believes that regulators in Washington did not take the time to raise awareness among its own field examiners before engaging in industry outreach.

Financial Institution C believes that industry associations were not out in front on interpretation of Red Flags. One interviewee voiced a perspective that some of the BITS conference calls focused on foundational elements and introductory material rather than more advanced or substantial insights.

In the end, Financial Institution C concluded it was already fulfilling the intent of the FACTA Identity Theft Red Flags and, for the most part, found the implementation to be a documentation exercise.

The exam to test the financial institution's compliance with Red Flags has not yet been conducted. A concern is that the examiners conducting the review will rely on a different interpretation to judge compliance.

In discussing this regulation, the financial institution stressed that it would be a good idea for the regulators to get the perspective from institutions earlier, before it issues draft regulations. It said that they are in general agreement with the objectives of the regulators, and they both want to protect customers. There is an opportunity for more collaboration.

The Financial Institution also said that the agencies need to be put in a position to hire more of the "best and brightest." It views training as a bandage. The top salary for regulators is too low and the agencies need more good people and sufficient staff to do the work.

Service Provider A

The interviewee at Service Provider A did not take an active role the regulatory life cycle for FACTA Identity Theft Red Flags. He stated that the time period of three to four years to achieve a final rule seemed excessive and that he was not sure how effective the rule would be given the delayed implementation by the FTC covered entities.

Service Provider B

Service Provider B considers itself to have strong relationships with its regulators. However, it stated that Regulators were less forthcoming than usual with insight, encouraging Service Provider B to read the Examiner's handbook for additional perspective and insight.

The service provider believes that Regulators do not like to "consult" or otherwise provide advice about "how" to comply with requirements. The regulators would not provide any insight into how other firms were achieving compliance. The service provider stated that it wants to comply, and would like more cooperation and insight from the regulators. On the flip side, however, it understands that the regulators likely do not want to risk sacrificing market creativity and objectivity, an essential part of risk management. Nevertheless, more collaboration and insights from the regulators were desired.

The service provider suggested that the regulators hold a FFIEC Risk Assessment 101 class to better explain requirements and expectations. Their view is that "risk assessment" is esoteric and academic, and there are no specifics on how to conduct it.

Service Provider B relies on its own staff to identify and track legislation and regulation on the horizon. It participated in forums on the topic with industry associations such as BITS, but its status as a service provider precludes it from membership.

The service provider stated that the last symposium for service providers was in 1993. It believes these forums should be resurrected to provide clear and consistent information to service providers. This is necessary because there is no organization for service providers; they need the regulatory agencies to provide the structure to bring them together. (Note: The regulatory agencies have held several service provider symposiums since 1993 on topics such as pandemics and authentication. This indicates that there may not be enough communication and awareness in the industry that this resource is available.)

3. Interview Detail on Interpretive Guidance on Customer Breach Notification in the Gramm-Leach-Bliley Act (2005)

Detailed Perspectives by Institution/Service Provider

Financial Institution A

In regulation that is state-specific, Financial Institution A usually raises the bar to meet the requirements of the toughest state and applies it equally across all states. This reduces the complexity of having to customize a response state by state. However, Financial Institution A believes that regulations such as GLBA should more comprehensively address customer and other information it seeks to protect and remove the imperative for states to fill any perceived gaps with state-specific regulation.

Financial Institution B

Financial Institution B recognizes Federal breach notification requirements as a baseline. Financial Institution B acknowledged that state-specific notification requirements increase the complexity that financial institutions have to manage. However, Financial Institution B also said that it has to deal with different state laws for other business

processes as well, such as real estate secured lending. Financial Institution B believed it was just the nature of doing business in the United States.

Financial Institution C

Financial Institution C said it would be much easier to comply with breach notification requirements if there was a single national standard. Financial Institution C believes that customers should be notified in the event of a breach, but cautioned that the many breach notification laws in place results in too many notifications that unnecessarily scare customers (i.e. the real potential for identity theft or fraud is low) or overload them with confusing information.

Service Provider A

When it came to implementing requirements, Service Provider A believed the fewer the number of potentially conflicting standards the better.

Service Provider A believes that the key to a successful national standard is to draft requirements that adequately address the various industry concerns so that the states do not have a reason to take action on their own.

Service Provider B

Service Provider B did not have any comments on breach notification.

Interview Detail on Additional Observations

Through the course of our interviews, the participants provided additional perspectives on the regulatory process that were outside of the case study framework. These observations are summarized in this section.

Perspectives by Institution/Service Provider

Financial Institution A

More communication between industry and regulators prior to issuance of draft guidance: Financial Institution A stated that once a draft regulation is issued, it is too late to address the regulation itself. The focus becomes primarily on how to comply. Communication between the industry and regulators needs to take place before draft regulations are issued. Financial Institution A said that in some cases (e.g. such as the Risk-Based Pricing Rule) regulators are interested in talking to them, initiate a conversation, and share advance proposals—and this type of communication should happen more often.

Being organized internally to respond to proposed rules is important: One area for improvement Financial Institution A identified for itself is the process to identify stakeholders when trying to *comment* on proposed rules. Financial Institution A considers itself better at responding to regulation than monitoring and responding to proposed rules.

Outside counsel is instrumental to understanding regulations: Financial Institution A's Legal department speaks with outside counsel weekly to understand the regulatory pipeline and the implications of both proposed and issued guidelines. Financial

Institution A considers outside counsel the primary provider of updates on regulatory happenings.

Mixed view of value of industry groups: Financial Institution A stated that it perceives other participants in industry forums to not be as knowledgeable on the subject matter as it is, and this makes industry forums a less valuable source from which to get information. Financial Institution A considers industry forums a useful environment in which to push opinions. Moreover, through industry associations, they can make contact easily with the right people to address regulatory questions.

Need to educate Congress on the amount of regulatory oversight: Financial Institution A believes a key challenge is educating Congress and legislators on the amount of regulatory oversight that already exists within the financial services industry. Financial Institution A believes that legislative bodies tend to write legislation on an industry by industry basis, that it overlaps, and there is no real appreciation of the cost burden it drives.

New approach for BITS: Financial Institution A believes that in an environment in which increased regulation is likely and in which there may be some challenges in educating regulators on industry perspectives, BITS should consider changing the way in which it frames its arguments. BITS should take on a more aggressive advocacy role and reframe the way in which it frames its positions. For example, considering the large infusion of government funds into financial institutions, BITS could take the position that taxpayer money would be better invested in an environment that is more efficient, and costs can be lowered by reducing overlapping regulation. Also, TARP funds need to be addressed as there is an inherent conflict between the pressures to loan the money while keeping credit standards high.

Financial Institution B

Perception that the reward system for field examiners drives increased requirements: Financial Institution B voiced the view that each field examiner team is in competition with the field examiner teams at other financial institutions. They are measured on who has the "best" (e.g. safest, most compliant) financial institution. Therefore, each team pushes for the most stringent interpretation of regulations.

No collaboration between financial institutions / Need for secure forums: Although financial institutions are being attacked by the same groups of criminals, they are not collaborating on response strategies and solutions. The barrier to cooperation is anti-trust laws and concerns over revealing information to competitors. There is a lot of room in the industry to collaborate on this topic. Moreover, financial institutions need a secure environment to talk about security and privacy concerns in the industry. The IT department is invited to present at various industry events, but declines to do so to keep its strategy and tactics confidential (and more secure) and to avoid becoming more of a target for criminals.

Need for industry association to segment membership: Perception that industry association forums need to be stratified by financial institution size, as different groups of financial institutions are facing different issues based on size, legacy environment, and maturity.

View of industry association value: Industry groups add value by voicing opinions that the financial institutions do not want to voice, bringing industry players together (e.g.

financial institutions and regulatory agencies), and enabling a network of experts and peers across institutions.

Belief the industry is on the defensive: The industry is reactive to the regulatory environment. The industry should be on the offensive, not the defensive, but the timing may be bad now. It would be good to advance a security agenda through an industry association. The industry could also consider pushing for federated identity (Federal ID) to support consumer banking security.

Need to involve government affairs: The Government Affairs department is not knowledgeable about security and privacy, and they could be made more so to help drive the agenda.

Regulator should focus on the big picture: In general, the regulators tend to focus on the small "nits and gnats." They should work with the financial institution more on the big picture view to make sure "we aren't leaving the barn door open."

Need to control the messages: The banking industry needs to take further measures to educate consumers and legislators on security and privacy and related topics. In actuality, the financial institution's losses to electronic fraud are less than $250,000 per year; the financial institution absorbs this cost, not the consumer. The risk message is being controlled and distorted by vocal and biased parties.

Use an enterprise risk management framework: There is an opportunity to drive the risk agenda by taking risk topics and breaking them down into an enterprise risk management framework. When regulations are proposed, they can be mapped to the framework to avoid duplication and promote the right solutions.

Industry associations need risk managers: While industry associations such as BITS have strong facilitators, they could be strengthened (and more responsive) if they had strong risk managers on their staff.

Current Successes of Industry Associations: Industry associations such as BITS are viewed as successful in bringing industry players together to discuss issues and solutions, and in voicing opinions when the company does not want to be the public voice.

Needs from Industry Associations: Industry associations such as BITS could add additional value by disseminating hard-to-obtain metrics that would be valuable in responding to regulators (e.g. how many AML people are on staff), and in providing real time insights in to how other financial institutions are responding to comply with regulation and guidelines.

Financial Institution C

Regulatory Process as a "Black Box": Financial Institution C commented that the regulatory process is a "black box" and they didn't know if feedback on proposed guidance matters. Financial Institution C believes that institutions need to know that their input matters, and if they know that, they will participate more actively and do more.

BITS Participants: Financial Institution C believes that BITS needs to take a more structured approach to identifying resources from each institution who should be participating in various initiatives and calls. There is a belief that the broad communications from BITS asking for participation creates confusion within the financial institution, because the institution does not know who is participating from its

organization. One interviewee recommended that BITS address this by working more closely with its advisory council and board—and to use a key liaison at the financial institution, not broad communications, to get involvement.

BITS Calls: Financial Institution C commented that there is still very little participation and input by institutions on calls, which reduces the value of the conversation. One interviewee commented that the level of audience on calls may range from senior executives to project managers, and not knowing who is on the call causes attendees to remain silent.

Service Provider A

Service Provider A did not have any additional observations.

Service Provider B

Service Provider B did not have any additional observations.

Authors

Walter Hoogmoed	John Graetz	Edward Appert
Principal	Principal	Senior Manager
Financial Services	Financial Services	Financial Services
Deloitte & Touche LLP	Deloitte & Touche LLP	Deloitte & Touche LLP
whoogmoed@deloitte.com	jgraetz@deloitte.com	eappert@deloitte.com
+1 973 602 5840	+1 415 783 4242	+1 212 436 7511

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2009 Deloitte Development LLC. All rights reserved.

Member of Deloitte Touch Tohmatsu

STATEMENT OF

BITS PRESIDENT PAUL SMOCER
ON BEHALF OF THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

SUBCOMMITTEE ON CAPITAL MARKETS AND
GOVERNMENT SPONSORED ENTITIES
OF
THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON FINANCIAL SERVICES

CYBER THREATS TO CAPITAL MARKETS AND CORPORATE ACCOUNTS

JUNE 1, 2012

TESTIMONY OF PAUL SMOCER, BITS PRESIDENT

Thank you Chairman Garrett, Ranking Member Waters, and Members of the Committee for the opportunity to testify before you today.

My name is Paul Smocer and I am president of BITS, the technology policy division of The Financial Services Roundtable. BITS addresses issues at the intersection of financial services, technology and public policy, on behalf of its one hundred member institutions, their millions of customers, and all of the stakeholders in the U.S. financial system.

First, I would like to recognize the Members for their focus on cybersecurity as illustrated by the House's recent Cyber Week and, more importantly, by its passage of legislation that will enhance public/private information sharing, augment funding for cybersecurity research and development, and provide for broader citizen awareness and education regarding cybersecurity. These bills address three key issues in our collective effort to secure cyberspace and fight cybercrime.

The financial services industry recognizes the serious and constantly evolving nature of cyber threats to its customers, its institutions, and the broader economic wellbeing of the United States. The industry and its institutions have historically had and continue to have a strong focus on this subject and we have been leaders in partnering with others to address the challenges.

Today, I will address cybersecurity efforts at both the institutional and industry levels, collaborations within and beyond the industry, and efforts underway to improve information sharing, and discuss how both industry and government can be supportive in protecting key economic infrastructures, such as capital markets, and in protecting customers.

At the individual institution level, every new or developing product is subject to a risk assessment that the institution uses to identify potential institutional and customer threats and risks as well as to identify mitigations to limit these risks. Likewise, when institutions consider new product delivery channels, they too are subject to an in-depth risk review. The risk management practices and processes institutions use to conduct such reviews and their general efficacy is also the subject of

reviews by numerous regulatory agencies that are part of the Federal Financial Institutions Examination Council.[1]

Individual institutions also bear a serious responsibility for understanding the cyber risks and controls of their key service providers. This is an important consideration as we consider cyber threats to both the capital markets and, to a more limited extent, commercial customers. In the context of capital markets, individual institutions often rely on external providers for many of the services that support this market such as clearings, settlements and accounting services. Institutions, both because of their innate risk management policies and regulatory expectations under the federal regulators' guidelines, regularly either examine the cyber and resiliency risks and controls of these providers or request the providers supply them with independently produced evaluations such as those produced under the American Institute of CPA's Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. These reviews both help assure that the underlying infrastructure that supports capital market security remains intact by forcing providers of services to employ effective cybersecurity protections and assures those using the services that they will remain available. Interestingly, many of the providers of those services are, in fact, themselves, financial institutions. As both a service provider and a financial institution, those institutions are both internally focused and externally focused on cyber issues.

Institutions recognize, however, that in the battle over cybersecurity, no one institution can fight alone. Consequently, at the sector level, a number of collaborative efforts exist. Through associations such as BITS and others such as the Financial Services – Information Sharing and Analysis Center (FS-ISAC) and the Securities Industry and Financial Markets Association (SIFMA) represented today on this panel, member companies band together to identify collectively institutional and customer risks in emerging areas such as mobile financial services, cloud computing and social media usage, as well as identify and share information on new threats and threat methods. They develop best practices guidelines for the industry to improve cybersecurity and reduce fraud. In many cases, these associations band together and work with all of their members on key issues. Two recent examples of these efforts include the work led by the FS-ISAC to address fraud occurring against commercial accounts through the Account Take Over Task Force and the work of

[1] See FFIEC IT Examination Handbook "Risk Management of E-Banking Activities" at http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities.aspx

the American Bankers Association and BITS toward building a more secure Internet environment in which to conduct financial services.

The largest of these industry collaborations is perhaps the sector's Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). This group consists of over 20 financial trade associations, ten of the largest US-based financial institutions (many of whom are integral to providing services within the capital markets infrastructure) and ten key participants operating in the financial infrastructure such as the Depository Trust and Clearing Corporation (DTCC). Through the Council, these organizations come together to focus on key policy areas, threat and vulnerability, research and development and resiliency. One current focus of the group is a pilot program underway between the Council and the DHS Science and Technology Directorate's Cyber Security Division to utilize available government agency data to enhance customer identity verification – an effort that would be helpful in protecting consumers.

In the spirit of public-private partnerships, this Council works closely with the public sector partner Financial and Banking Information Infrastructure Committee (FBIIC), which was chartered under the President's Working Group on Financial Markets, and is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. Chaired by the Treasury Department, this Committee includes sixteen government agencies with oversight for the entire financial sector including regulators within the capital markets. Working together, the Council and the Committee members focus on key cybersecurity issues affecting the industry and how to address them. This focus includes the critical question of the industry's ability to recover from an incident – whether cyber or physical – that might affect the availability of vital industry infrastructure. Under their leadership, the two groups have sponsored numerous industry-wide resiliency exercises. The latest of these, called "Quantum Dawn," had as one of its two objectives to exercise operational risk practices across the equities clearing and trading processes. The cybersecurity scenarios tested by this exercise included corruption of publicly reported stock prices, corruption of trades (changing of *buys* to *sells),* and substantial loss of availability of the National Market System and resulted in identifying both effective processes and areas for improvement.

While the industry and its regulators are investing significant effort to work symbiotically to improve cybersecurity for financial services, the effort continues even beyond those groups. Recognizing that our ability to maintain confidence in financial services relies on other key constituencies, the industry has formed collaborations with other key parties. One example is the development of the Cyber Operational Resiliency Review (CORR) currently being piloted. This pilot, organized by BITS, allows financial institutions to request, through The Department of the Treasury, a review by a team of specialists supplied by The Department of Homeland Security of an institution's cyber practices and networks. In addition, BITS, FS-ISAC and other associations have formed collaborative relationships with various law enforcement agencies including the Federal Bureau of Investigation, United States Secret Service and US Postal Inspectors to coordinate industry and law enforcement efforts to prevent and prosecute cybercrime. Law enforcement was a key participant in the efforts led by the FS-ISAC toward mitigating issues with commercial account takeover.

Understanding that it is important to strengthen every link in the infrastructure chain, the industry has also affected outreach efforts to other key sectors. One recent example was showcased this past Wednesday in a White House-sponsored event that announced the Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace developed by the Industry Botnet Group. This multi-industry group, committed to working together to combat cyber threats, is a voluntary group of corporations, trade associations, and non-profit organizations, led by a steering committee composed of BITS, Business Software Alliance, Online Trust Alliance, Software Information Industry Association, National Cyber Security Alliance / StaySafeOnline, StopBadWare, TechAmerica, U.S. Internet Service Provider Association, and the U.S. Telecommunications Association. Recognizing that botnets have a serious impact to the security and privacy of both individuals and businesses as they facilitate the delivery of malicious software by the cybercrime community, this multi-stakeholder group is acting collaboratively to mitigate the problem. Another recent example was the successful effort undertaken by Microsoft's Digital Crimes Unit – in collaboration with the FS-ISAC and NACHA – The Electronic Payments Association, to take down the command and control center of a major botnet ring operating within the US.

These types of efforts recognize a key factor – today's Internet and electronic world is highly integrated and relies on multiple organizations and providers to effectively mitigate security risks. That is why the industry has been and continues to be supportive of efforts to assure a more

consistent level of security within other critical sectors in the cyber environment. That is also why the industry has invested in educating consumers on cybersecurity. Consumers and businesses play a key role in cybersecurity and have a responsibility to protect themselves as well. The financial services industry and others have recognized that consumers and businesses often lack the skills and awareness to fully protect themselves. As a result, significant investments have been made in education efforts by financial institutions and associations and we applaud the House's passage of H.R. 2096 The Cybersecurity Enhancement Act of 2012 sponsored by Representative Michael McCaul, which will help with this effort.

The industry's efforts start with individual institutions that provide educational materials via websites, mailings and community educational events. Financial associations also publish educational material and offer education directly to their communities through community outreach efforts. These efforts have often been done in collaboration with other parties such as law enforcement, as was the case with educating businesses about account takeovers, or with entities focused on citizen education such as the National Cyber Security Alliance and its StaySafeOnline campaign.

As these efforts show, the financial services industry understands cybersecurity is a critical issue, and that the best success in improving security comes from collaborative efforts and not just the work of financial institutions. Clearly financial institution work is significant in terms of resources, cost and commitment. Institutions willingly undertake these security and awareness efforts and recognize their necessity to safeguarding customers and their accounts, and the overall financial system. These protections are critical to maintaining customer trust and confidence in the industry, and are a highly important investment. Individual institutions also recognize success depends on investing in broader, collaborative efforts beyond financial services to ensure a resilient economic system.

I would be remiss, however, if I did not mention one other key area of collaboration – that is, the area of threat information sharing. Like all cybersecurity defenses, information sharing exists at multiple levels. Individual institutions monitor their own threats and in the financial services sector, we do an effective job of sharing threats through the FS-ISAC. But, there remains much opportunity to exchange threat information more broadly. Most of the efforts to date have involved intra-industry efforts in the financial services sector and in the defense industry sector, through its

Defense Cyber Information Sharing Environment (DCISE) program. Inter-industry and public/private information sharing opportunities remain to be developed. BITS, in cooperation with the FSSCC and the FS-ISAC, is nearing the end of a study to assess existing and potential collaboration programs between the US Government's national security agencies and the financial services sector. The study focuses on threat information sharing, cyber security capacity building and cyber-related crisis management.

Threat data and threat analysis are very often industry agnostic. Viruses, Trojans and other malicious software are sometimes written to attack the users of a particular sector, such as those that attempt to steal login credentials from banking customers. In many cases, however, they are not aimed at a particular sector. For example, malicious software that attempts to take over a user's computer or other device to make it part of a botnet[2] that will be subsequently used by cybercriminals simply does not care who or for what purpose one is using their device. Botnets, however, create the risk of establishing large numbers of endpoints available to criminals to commit cybercrime. Likewise, cyber anarchists who use denial of service attacks in attempts to disrupt the availability of systems, websites and other technology resources use these techniques to target entities in virtually all private and public sectors. The more information shared across a broad swath of sectors about the sources of attacks, the nature of attacks and the pattern of attacks, the more ultimate improvement will occur in the responsiveness and the defense of all sectors. Frankly, however, organizations are often hesitant to share this type of information. Some are concerned that information exchanged will not be protected and will subsequently be revealed. While true even with private-to-private sharing, this is especially true with private companies sharing information with public entities. Private organizations are concerned that revelation of the information will impact their reputation and the confidence of their customers – regardless of their industry. That is why the financial services industry along with other industries was supportive of the passage of HR 3523, the Cyber Intelligence Sharing and Protection Act, which, if enacted, offers additional protections and assurances to the confidentiality of shared information.

[2] The term *bot* is short for robot. Criminals distribute malicious software (also known as malware) that can turn your computer into a bot (also known as a zombie). When this occurs, your computer can perform automated tasks over the Internet, without you knowing it. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a *botnet*. Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. (As defined by Microsoft ® Safety & Security Center at http://www.microsoft.com/security/resources/botnet-whatis.aspx)

It is important to recognize that the information sharing generally done with regard to cyber attacks seldom involves non-public, private information regarding individuals. We recognize that as HR 3523 was debated, the concern about protecting individuals' information and privacy was a legitimate concern raised by several Members of the House. As you consider future cybersecurity legislation, however, we do urge you to consider solutions to allow sharing of this type of information under certain circumstances in a manner that protects the rights of individuals, but facilitates their protection as well. There are legitimate reasons to share this information that benefits citizens. For example, a breach occurring at a payroll processor can result in cybercriminals obtaining the checking account information of individuals. Today, sharing that information with the financial institutions that hold those accounts is difficult at best. Sharing it, however, and sharing it quickly, would allow those institutions to take action to prevent fraud against their commercial and retail customers.

In closing, please accept my thanks for the opportunity to testify to the Committee. Cybersecurity is a vitally important issue for both the private and public sectors. Protecting companies, and more so, protecting their customers and our citizenry in general must remain key imperatives for us all. Further, protecting the infrastructures that support our economy is crucial to maintaining confidence and an operating global financial system. We commend the Committee for recognizing the importance of this subject and for your attention in supporting the strongest cyber defense for our nation.

###

Testimony of

Michele B. Cantley

Chief Information Security Officer

Regions Bank

On Behalf of the

The Financial Services Information Sharing & Analysis Center

Before the

United States House of Representatives

Capital Markets and Government Sponsored Enterprises Subcommittee

June 1, 2012

FS-ISAC BACKGROUND

Chairman Garret, Ranking Member Waters, and members of the Subcommittee, my name is Michele Cantley. I am the Chief Information Security Officer for Regions Bank and I am appearing today for the Financial Services Information Sharing & Analysis Center (FS-ISAC). I want to thank you for this opportunity to address the U.S. House of Representatives Financial Services Capital Markets and Government Sponsored Enterprises Subcommittee on the important issue of corporate account takeover and its impact to the financial services industry. In addition, my written testimony includes other recommendations for improving communication between the public and private sector about cyber threats as well as the efforts that our financial services sector can take to improve our defenses and educate our customers.

First, let me provide some background on Regions and FS-ISAC. Regions Financial Corporation, with $127 billion in assets, is a multi-state regional bank and is one of the nation's largest full-service providers of consumer and commercial banking, wealth management, mortgage, and insurance products and services. Regions is the 12th largest U.S. bank by deposits and loans and serves customers in 16 states across the South, Midwest and Texas, and operates approximately 1,700 banking offices and 2,100 ATMs. Regions is a member of the FS-ISAC.

The FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (PDD63) that called for the public and private sector to work together to address cyber threats to the Nation's critical infrastructures. After 9/11, and in response Homeland Security Presidential

Directive 7 (HSPD7) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to our sector.

The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial services firms. Since that time the membership has expanded to over 4,400 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, exchanges and clearing houses, payments' processors, and over 30 trade associations representing the majority of the U.S. financial services sector.

The FS-ISAC works closely with various government agencies including the U.S. Department of Treasury, Department of Homeland Security (DHS), Federal Reserve, Federal Financial Institutions Examination Council (FFIEC), United States Secret Service, Federal Bureau of Investigation (FBI), National Security Agency (NSA), Central Intelligence Agency (CIA), and state and local governments.

With respect to cooperation within the financial services sector, the FS-ISAC is a member of, and partner to, the Financial Services Sector Coordinating Council (FSSCC) for Homeland Security and Critical Infrastructure Protection established under HSPD7. We also work closely with other industry groups and trade associations that are members of the FS-ISAC including the American Bankers Association (ABA), Securities Industry and Financial Markets Association (SIFMA), Independent Community Bankers Association (ICBA), and the BITS division of the Financial Services Roundtable. In addition, our membership includes various clearing houses

and exchanges such as the National Automated Clearing House Association (NACHA), Depository Trust and Clearing Corporation (DTCC), New York Stock Exchange, NASDAQ, The Clearing House (TCH), all of the payment card brands and most of the card payment processors in the U.S.

The overall objective of the FS-ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that provides anonymity to allow members to submit threat, vulnerability and incident information in a non-attributable and trusted manner so information that would normally not be shared is instead provided for the good of the sector, the membership and the nation. FS-ISAC information sharing services and activities include:

- delivery of timely, relevant and actionable cyber and physical email alerts from various sources distributed through the 24x7x365 FS-ISAC Security Operations Center (SOC);
- an anonymous online submission capability to facilitate member sharing of threat, vulnerability and incident information in a non-attributable and trusted manner
- presenting cyber security briefings and white papers;
- operation of email list servers supporting attributable information exchange by various special interest groups including the FSSCC, the FS-ISAC Threat Intelligence Committee, threat intelligence sharing open to the membership, the Payment Processors Information Sharing Council (PPISC), the Clearing House and Exchange Forum (CHEF), the Business Resilience Committee, Compliance and Audit Council, Insurance Risk Council, and the Payments Risk Council;

- anonymous surveys that allow members to request information regarding security best practices at other organizations;
- bi-weekly threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities and incidents affecting the sector;
- emergency threat or incident notifications to all members using the Critical Infrastructure Notification System (CINS);
- emergency conference calls to share information with the membership and solicit input and collaboration;
- engagement with private security companies to identify threat information of relevance to the membership and the sector;
- development of risk mitigation best practices, threat view points and toolkits;
- Subject Matter Expert (SME) committees including the Threat Intelligence Committee and Business Resilience Committee that provide in-depth analyses of risks to the sector, provide technical, business and operational impact assessments and recommend mitigation and remediation strategies and tactics;
- special projects to address specific risk issues such as the Account Takeover Task Force (see pages 10-13);
- document repositories for members to share information and documentation with other members;
- development and testing of crisis management procedures for the sector in collaboration with the FSSCC and other industry bodies;

- participation in sector, cross-sector and national exercises such as the Cyber Attacks Against Payment Processes (CAPP), National Level Exercise 2012, and the Cyber Storm series;
- semi-annual member meetings and conferences; and
- online webinar presentations and regional outreach programs to educate small to medium sized regional financial services firms on threats, risks and best practices.

A key factor in all of these activities is trust. The FS-ISAC works to facilitate development of trust between its members, with other organizations in the financial services sector, with other sectors, and with government organizations such as law enforcement, regulators, and intelligence agencies. The FS-ISAC, for example, uses a traffic light protocol (red, yellow, green) to indicate to its members how information may be disseminated to FS-ISAC members, partners, and other ISACS. This protocol has been a key component in developing a clear means for trusted distribution of information. The FS-ISAC has also built a model for sharing information without attribution to a specific institution and also uses non-disclosure agreements (NDAs) to ensure that confidentiality of non-public and sensitive information is maintained.

The FS-ISAC is an active participant in cross-sector information sharing and has engaged in a number of cross-sector information sharing programs such as the Joint ISAC BOTNET Mitigation Process Working Group and the Cross Sector Information Sharing Framework, a vehicle for real-time cyber information sharing between the sectors. FS-ISAC currently also has a leadership role in the National Council of ISACs.

The FS-ISAC has implemented a number of programs in partnership with the Department of Homeland Security (DHS) and other government agencies. As part of this partnership, the FS-ISAC set up an email listserv with U.S. CERT where actionable incident, threat and vulnerability information is shared in real-time. This listserv also allows FS-ISAC members to share directly with U.S. CERT. In June 2011, the FS-ISAC, in partnership with DHS became the third ISAC to participate in the National Cybersecurity and Communications Integration Center (NCCIC) watch floor. FS-ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the financial services sector. Over the course of a year, our presence on the NCCIC floor has largely greatly enhanced situational awareness and information sharing between the financial services sector and the government. The FS-ISAC recently obtained funding from a member to have full-time staff on the NCCIC floor in addition to the part-time resources that are currently deployed.

In addition, FS-ISAC representatives sit on the Cyber Unified Coordination Group (Cyber UCG). This group was set up under authority of the National Cyber Incident Response Plan (NCIRP) and has been actively engaged in incident response. Cyber UCG's handling and communications with various sectors following the RSA attack in March of 2011 is one example of how this group is effective in facilitating relevant and actionable information sharing.

Finally, it should be noted that the FS-ISAC and FSSCC have worked closely with DHS, the U.S. Department of Treasury, FBI, U.S Secret Service and other government partners to obtain over 250 Secret level clearances and a number of TS/SCI clearances for key financial services

sector personnel. These clearances have been used to brief the sector on new information security threats and have provided useful information for the sector to implement effective risk controls to combat these threats. The FS-ISAC would like to see this process updated to efficiently and effectively provide more clearances to the private sector.

PUBLIC / PRIVATE SECTOR RESPONSE TO THE CYBER CRIME ISSUE

The FS-ISAC is aware through its information sharing arrangements with both public and private sector organizations that criminal threats are targeting US financial institutions, capital markets exchanges, clearing houses, payment processors, businesses and consumers.

I want to thank you for the opportunity to address the issue of corporate account takeover. Corporate account takeover is the unauthorized use of valid online banking credentials, typically obtained via malicious software ("malware") that infect customers' workstations, laptops or computer networks. Cyber criminals use a variety of methods to infect business customers' computers and they are constantly updating their methods to match customers' uses of technology.

In order to get account information, cyber criminals continue to attack business customers' computers by phishing (attempting to acquire information (and sometimes, indirectly, money) such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication), malicious advertisements (or "malvertisements") and fraudulent messages on social media sites.

Phishing remains the most popular attack method that criminals use to infect victims' machines. Nonetheless, emails that purport to be from a victim's bank are no longer the primary type of phishing email. Criminals now send emails purporting to be from NACHA (The National Automated Clearing House Association), EFTPS (the Electronic Federal Tax Payment System), the US Postal Service, private delivery firms, telecommunications' companies, social media providers and others in order to trick their victims into opening the email and clicking on a link. Once the user clicks on such a link, it redirects the unknowing user to a server that then downloads malicious software onto the victim's computer. This malicious software includes a key logger (a program that can record a user's keystrokes) that captures the user's online banking credentials as he types them.

Another method of attack is malicious advertisements or "malvertising." In this case, criminals have put advertisements on search engines and other prominent news-sites. Victims, believing that it is a legitimate ad, click on the link, and the malware gets downloaded on their computer(s) and fraud can occur. A more recent method involves fraudulent messages sent from social media sites. These may include bogus friend requests, for example, that include links to malicious sites.

Once the criminals have the valid online banking credentials, they can impersonate the customer by logging onto the online banking site. They then create fraudulent ACH and/or wire transactions which they submit to the bank. The fraudulent transactions are generally directed to people who have been recruited to serve as intermediaries or "mules." The mules receive

instructions from the criminals regarding how to handle the funds. The mules might be instructed to withdraw the funds in cash and then send them elsewhere via legitimate money transfer or wire methods. The mules get to keep a percentage of the funds as payment for his/her services.

However, research shows that losses due to cyber crime currently only account for a small percentage of the overall fraud losses incurred by financial institutions. Over the past two years, actual losses experienced by financial institutions and their customers as a result of cyber-related fraud has actually declined in spite of the fact that the number of attacks has increased. The FS-ISAC and its members recognize the online criminal threat both to the affected institutions and to consumer confidence posed by these criminal activities and we are taking steps to address areas of concern.

The FS-ISAC has been active in its efforts to counteract the spread of corporate account takeover. In 2010, the FS-ISAC formed the Account Takeover Task Force (ATOTF) as a result of continued concern and need for additional tools to help financial institutions and their customers combat online account takeover attacks. The ATOTF consists of over 120 individuals from thirty-five financial services firms of all sizes and types, ten industry associations and processors and representatives from seven government agencies. The ATOTF recently completed a report that includes recommendations to focus on three main areas—prevention, detection and responsiveness—in order to ensure an improved and effective defense against cyber crimes, including account takeover.

For each area, the ATOTF created work products whose purposes were to assist financial institutions of all sizes with dealing with account takeover by educating them and their customers on how account takeover works, what techniques can be used to detect and prevent account takeover, and lastly, in the event of an account takeover event, what steps financial institutions and customers should take to respond.

Examples of the work products include:

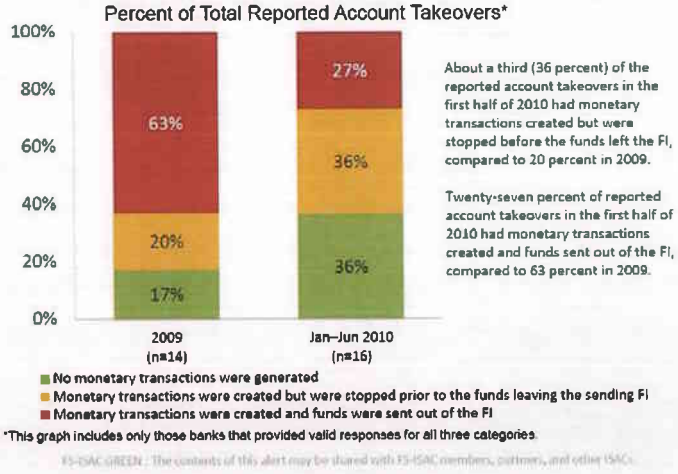
- Industry Advisories for Corporate & Small Business Customers and Financial Institutions
  - Fraud Advisory for Businesses: Corporate Account Take Over, co-branded with US Secret Service, FBI and Internet Crime Complaint Center (IC3). The advisory is available here: http://www.fsisac.com/files/public/db/p265.pdf
- J1-visa Mule Advisory (many mules from abroad are recruited via J1-Visas)
- Fraud Advisory for consumers about Work from Home Scams (where mules are often recruited)
  - Fraud Advisory for Consumers: Involvement in Criminal Activity through Work from Home Scams, co-branded with FBI and IC3. The advisory is available here: http://www.fsisac.com/files/public/db/p264.pdf
- Detailed white papers on Detection, Prevention and Response Techniques
- A contact list and procedures which provide financial institutions with the information they need to report account takeover attacks to the Secret Service, FBI, and other law enforcement agencies

- A recommendation to FINCEN (since adopted) to redesign the Suspicious Activity Report (SAR) in order to appropriately capture account takeover events

Lastly, the ATOTF has undertaken, with the assistance of the FS-ISAC and the American Bankers Association, surveys of the FS-ISAC members about the scope and impact of the account takeover problem. Survey data has been obtained for 2009, 2010 and the first half of 2011. The chart which follows includes a portion of the survey data for 2009 and 2010. This chart reflects the collective work of the ATOTF and FS-ISAC members in working effectively to reduce monetary losses associated with account takeover.

Monetary Transactions (ACH or Wire Transactions) Associated with Commercial Account Takeovers

Based on valid responses from FIs that reported experiencing account takeovers in 2009 and/or Jan-June 2010.



*This graph includes only those banks that provided valid responses for all three categories.

FS-ISAC GREEN - The contents of this alert may be shared with FS-ISAC members, partners, and other ISACs.

In the most recent survey, members were asked about the most effective step they had taken to reduce corporate account takeover. The answer may surprise you. It was not technology or legislation; rather, it was customer education. As trusted partners, financial institutions are in the best position to educate our customers about the vectors of attack for corporate account takeover and how customers can protect themselves. This is why customer education was such an integral part of each ATOTF deliverable.

As noted above, the FS-ISAC and its membership have taken tremendous steps to limit cyber crime and corporate account takeover. Nonetheless, it is important to note that corporate account takeover attempts cannot be stopped solely by the actions of financial institutions. Beyond financial firms, our customers and participants in the broader electronic ecosystem all have roles to play to improve security.

Banks, for instance, have no direct control over the end customers' computers, nor can banks control what emails bank customers open or what websites they visit prior to accessing their online banking system(s). Nonetheless, to increase the security of our customers' accounts, we must educate our customers on the risks and monitor for anomalous transactions. Banks must continue to detect fraudulent transactions and stop them. Customers have a role to play in learning about these threats and practicing safe internet habits. Customers can also reconcile their accounts daily and review their electronic transactions for accuracy.

Others have roles to play as well. Law enforcement can assist by seeking out and arresting the criminals behind these attacks. Internet Service Providers (ISPs) can monitor traffic on their

network for much of this malicious software and alert their customers to these infections. (Collaboration is already underway with the government, ISPs, and others to reduce the number of servers and computers used to disseminate the malware and phishing emails that target financial institution customers.) ISPs and email service providers can create electronic security measures that "interrogate" phishing emails. If the senders don't authenticate the messages, they should be dumped into spam folders so they are less likely to fool users. Also, these companies can pursue civil actions to take down servers that send the phishing emails and malicious software. Finally, continued work on international legal and diplomatic levels is needed so that all countries recognize this type of cyber-crime and that there are some forms of sanctions for those countries that harbor the criminals who perpetuate the problem.

Another example of industry collaboration is the BITS / FSISAC Trusted Email Registry project, which is designed to strengthen the email delivery channel through better authentication and encryption.

Let me highlight one example of cooperation. Law enforcement and a number of government agencies have taken a lead role working with the FS-ISAC, its member organizations, payments processors, and the financial services sector as a whole to combat these types of attacks. An example of a successful instance of government/financial services sector information sharing occurred on August 24, 2009, when the FBI, FS-ISAC and NACHA released a joint bulletin concerning account takeover activities targeting business and corporate customers. The bulletin described the methods and tools employed in recent fraud activities perpetrated against small to medium-size businesses that had been reported to the FBI. The objective of the bulletin was to

employ FS-ISAC and NACHA subject matter expertise and apply it to the FBI case information to identify detailed threat detection, prevention, and risk mitigation strategies for financial institutions and their business customers, while preserving the integrity of the FBI's ongoing investigations. The FS-ISAC and NACHA developed a comprehensive list of recommendations for financial institutions to educate their business customers on the need to use online banking services in a secure manner. The bulletin was distributed through the FS-ISAC to its over 4,400 members, which includes over 30 member associations such as NACHA, ABA, and ICBA. Subsequent releases of the bulletin were shared with the press in 2010, redacting sensitive information about the ongoing investigations.

The risk mitigation tactics that are outlined in the joint FBI/FS-ISAC/NACHA bulletin include information security best practices that are consistent with the 2005 Federal Financial Institutions Examination Council's (FFIEC's) Guidance on Authentication in an Internet Banking Environment. The joint FBI/FS-ISAC/NACHA bulletin actually moved further than the 2005 FFIEC Guidance in its recommendations. Specifically, the bulletin recommended that financial institutions implement a layered "defense in-depth" approach to information security to protect financial institutions and their customers.

FFIEC SUPPLEMENTAL GUIDANCE ON INTERNET BANKING AUTHENTICATION

The FFIEC Supplemental Guidance on Internet Banking Authentication released on June 28, 2011 incorporates many "defense in-depth" recommendations and includes a number of very important new regulatory provisions that fit into the larger and detailed regulatory landscape. To highlight, the financial services sector is highly regulated by international, Federal and state

authorities. Through numerous laws enacted by Congress over the past 150 years, federal financial regulators have implemented a complex regime that includes supervision of the financial institutions' operational, financial and technological systems. Regulators, such as the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency and Securities and Exchange Commission, conduct examinations to assess the adequacy of controls to address financial and other risks. These examinations focus on information security, business continuity, vendor management and other operational risks. In addition to these public sector entities, self-regulatory organizations (SROs), such as the Municipal Securities Rulemaking Board (MSRB), the Financial Industry Regulatory Authority (FINRA), the National Futures Association (NFA), and exchanges, such as the Chicago Mercantile Exchange (CME), and the New York Stock Exchange (NYSE), also play an important role in industry oversight.

The following is a summary of some of the Supplemental Guidance's key provisions. The Guidance reinforces existing supervisory expectations for annual risk assessments by financial institutions. These risk assessments should consider changes in the internal/external threat environment, changes in the financial institution's customer base, changes in functionality to online Internet services, and the financial institution's actual fraud experiences. Authentication controls should be upgraded in response to risk assessments.

For the first time, the FFIEC distinguishes between retail and commercial accounts. It raises the bar for minimum controls for all accounts and recognizes that commercial accounts pose a higher level of risk. The Guidance notes that banks must educate their customers on both the security

and protections provided to both retail and commercial clients. In doing so, it creates a regimen of clear disclosures. Commercial account controls should be consistent with increased levels of risk and stronger than the controls for consumer accounts.

The FFIEC Supplemental Guidance now requires financial institutions to have layered security for consumer accounts. "Layered security" is defined as having different controls at different points in a process, so that weakness in one control is compensated by strength in another control. At a minimum, layered security should include anomaly detection and response at initial customer login, and at initiation of funds transfers to other parties. Layered security for commercial accounts should be stronger than those implemented for consumer accounts. The Guidance specifies enhanced controls for system administrators of commercial accounts. Examples of these enhanced controls include additional authentication/verification of new payees, creation of new wire templates, added wire approvers, and changes to established value threshold or time windows.

Layered security should now include anomaly detection. Changes in consumer or commercial account activity should be detected and steps taken (such as triggering incremental client authentication to validate questionable transactions) to ensure that additional controls are in place if such activity is discovered. Such efforts must protect customers' privacy yet should not interfere with efforts to detect fraud. However, according to the FFIEC Supplemental Guidance, "simple" device identification and challenge questions are no longer deemed effective as a primary control. Instead, financial institutions will be required to implement "*Complex Device*

Identification." An example of complex device ID includes use of a one-time cookie, in conjunction with other factors, such as the PC's configuration, IP address, and geo-location, to create a digital "fingerprint" of the customer's personal computer. The Guidance also calls for more "*Complex Challenge Questions*" not easily found by cyber criminals on the Internet. These "out of wallet" questions should not rely on publicly available information and there should be more than one question, potentially even including a "red herring" question that only the account holder will recognize as false, requiring a potentially fabricated answer.

Lastly, the FFIEC Supplemental Guidance calls for increased customer awareness/education efforts by financial institutions. The Guidance recognizes that customers have an important role to play in online banking security, and that consumers' and small businesses' financial institutions are likely more knowledgeable about online security. Financial institutions have an obligation to help customers practice good online banking security and to clarify, via customer education, the protections provided under Regulation E. Financial institutions should also educate their commercial account holders, especially small businesses, on use of security controls that are available for their online banking services.

FFIEC regulatory agencies have begun examinations to assess conformance with these new FFIEC Supplemental Guidance.

As a result of the 2009 joint FBI/FS-ISAC/NACHA bulletin, the FFIEC Supplemental Guidance and the many deliverables of the ATOTF, financial services firms and their business customers,

government, and consumer customers have become more aware of the online risks facing them and of the many effective layered defense practices to mitigate those risks. As a result, more financial institutions are now aware of how to detect, prevent and respond to malicious and criminal activities resulting from online attacks.

FS-ISAC believes that the private sector and government can continue to work together to improve account security. Several areas of cooperation are outlined below.

1. IMPROVE CYBER CRIME LAW ENFORCEMENT

a. There needs to be better and more domestic and international collaboration regarding investigations and prosecutions given the origins of a significant portion of cyber crime. Countries that have not adopted the Council of Europe's Convention on Cyber Crime should be encouraged to do so. The Convention is an international, multilateral treaty specifically addressing the need for cooperation in the investigation and prosecution of computer network crimes.

b. Sufficient funding is needed for cyber crime investigations and forensics. Currently, private sector firms report that some local law enforcement agencies require minimum thresholds before they will take the case. However, evidence indicates that most of these types of attacks are directed at many firms and their customers, so the cumulative dollar value of the crime committed may be many times the amount of any individual loss.

c. Law enforcement must be more responsive to cyber crimes reported by financial services firms. There needs to be improved communications at a local level between financial

services firms and their cyber crime law enforcement contacts and an understanding of how to report these crimes so that action will be taken.

d. After a compromise is reported to law enforcement, law enforcement must allow the threat indicators from the attack to be shared with financial institutions. There are a number of instance where those indicators have not been shared and thus other financial institutions are exposed to similar attacks. We understand the sensitivity around nation state attacks and around preserving evidence for criminal cases. However, the actions of some law enforcement agencies to restrict information sharing is hampering the financial services' sector's ability to protect itself and its customers from similar attacks. This issue speaks clearly for the need for greater trust between the public and private sector.

e. In keeping with our commitment to education, it is also important for law enforcement, prosecutors and judges to have substantial cyber education and knowledge so that they can prosecute cyber criminals effectively.

2. CONTINUE TO IMPROVE FINANCIAL INSTITUTION INFORMATION SECURITY PROGRAMS

Regulators and industry need to have a flexible and dynamic approach to cyber security so that individual financial institutions can continue to improve information security programs based on their size, scope of activities, and structure. Financial institutions have comprehensive security regulations already in place. This approach builds on the foundation embodied in the Gramm-Leach-Bliley Act framework and opposes prescriptive, one-size-fits-all or technology-specific approaches.

3. IMPLEMENTATION OF DEFENSE IN-DEPTH SECURITY

Financial services firms and payment processors need to implement defense in-depth security in order to protect their customers and their institutions from cyber criminal attacks. These security solutions must take into account the evolution of the changing threat landscape and will need to be updated over time. Commercially reasonable security procedures must achieve an appropriate balance between security, risk and usability. The June 28, 2011 FFIEC Supplemental Guidance on Internet Banking Authentication goes a long way towards achieving that balance without dictating any single solution which may prove to be untenable over time.

4. IMPROVE PUBLIC/PRIVATE SECTOR COLLABORATION

Expanded information sharing between government agencies and the financial services industry is one of the FS-ISAC's primary goals. There have been improvements made but there needs to be greater private sector access to threat and intelligence from Federal intelligence and law enforcement agencies. The House-backed Cyber Intelligence Sharing and Protection Act is a good example of strengthening information sharing in order ultimately to protect customers. This access must be administered in a manner that can provide broader protection without providing undue market advantage to a select group or that would compromise ongoing investigations. Specific recommendations include:

a. Provide financial institutions, networks and processors with timely, relevant and actionable information on threats, vulnerabilities, and exploits.
b. Provide the financial services industry with analysis of trends using existing data reporting requirements (e.g., FinCEN's data of Suspicious Activity Reports which includes computer crimes).

c. Support the existing National Infrastructure Protection Plan (NIPP) and its supporting organizations such as the National Council of ISACs of which the FS-ISAC belongs and the sector coordinating councils, such as the FSSCC. Also support the FSSCC's public sector partner, the Financial and Banking Information Infrastructure Committee (FBIIC) and support their joint initiatives.
d. Compile and share data on payment system fraud and security trends.
e. Fund top R&D priorities, such as the FSSCC's priority project on identity assurance.
f. Support industry exercises that relate to cyber threats. By routinely engaging in exercises and training, public and private sector participants build relationships and establish trust that is essential for sharing information.
g. Continue towards the goal of a fully integrated Joint Coordination Center for sharing cyber threat information between the public and private sectors. The embedding of financial sector personnel in the NCCIC is a positive step in that engagement process and is an essential building block towards a stronger trust model.

5. IMPROVE THE INTERNET INFRASTRUCTURE

Use Federal procurement power to improve the security of software, hardware and services that support the Internet business infrastructure and applications (i.e., enhanced technology that is implementable and cost appropriate for the market.)

6. EDUCATION

More public/private sector collaboration is needed to support educational efforts to increase consumer and business awareness of cyber threats and risk mitigation best practices. One

example of such an effort has been undertaken by the National Cyber Security Alliance in promoting a "Stay Safe Online" campaign as part of the October Cyber Security Awareness month (http://www.staysafeonline.org/).

As a result of these types of programs and the efforts of the FS-ISAC Account Takeover Task Force, financial institutions have educated their customers regarding phishing and other social engineering attacks with information on their websites, mailers and in their bank lobbies regarding safe and secure online banking practices. Corporate and government users of online financial services products can now take advantage of these educational tools that are available.

Thank you for the opportunity to present this testimony.

BITS

FINANCIAL SERVICES ROUNDTABLE

SOFTWARE ASSURANCE FRAMEWORK

January 2012

BITS
A DIVISION OF THE FINANCIAL SERVICES ROUNDTABLE
1001 PENNSYLVANIA AVENUE, NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
202-289-4322
WWW.BITS.ORG

Executive Summary

Software is the critical underpinning to virtually all of the products and services offered by financial institutions. It processes information that is sensitive both to financial institutions' customers and to the institutions themselves. Developing that software is a complicated process involving many steps including idea conception, design, coding and testing. Implementing software is also often complicated given that virtually all developed software operates within a broader ecosystem. These complexities can give rise to improperly designed or insecure software that exposes an organization to a variety of risks. The risks associated with insecure software include:

- Increased likelihood of attack on financial institution software,
- Theft of customer information such as account and credit card data,
- Theft of corporate information and intellectual property,
- Increased maintenance costs and lost opportunity costs, and
- Reduced system availability and negative client reputational impact.

These risks can lead to both direct costs as well as indirect costs (such as those associated with reputational risk losses). Developing software in a secure fashion can do more than avoid costs though – it can also have a positive return on the investment associated with software. A January 2011 study commissioned by Microsoft and conducted by Forrester Consulting found that those organizations that utilize a secure development process experience more positive ROIs in various areas including time to market, post-development maintenance, and the amount of time devoted to testing.[1] Generally speaking, it is far less expensive to build secure software than to fix security issues once the software is deployed. In addition, if a breach occurs, the costs can increase dramatically based on the type of compromise and remediation efforts involved. Secure coding practices are critical for developing secure code.

Today, there are numerous methodologies that address various aspects of software development. While most are good for their purpose, they tend to be very detailed, focus on specific components of the software development process, and are often very focused on the development of software using specific techniques or software languages. These methodologies have their place in developing secure software, but generally fail to outline an overall process, or framework, of practices. In addition, they generally do not focus specifically on the needs of the financial services industry.

The BITS Software Assurance Framework provides a higher level outline of the various components of a mature, strategic program for secure software development for software used within the financial services industry. The Framework was developed by subject matter experts in software development primarily in the financial services industry. It can be applied to software developed directly by financial institutions or developed by third parties for the benefit of financial institutions.

[1] Forrester Consulting Thought Leadership Commissioned by Microsoft, State of Application Security, Immature Practices Fuel Inefficiencies, But Positive ROI Is Attainable, (Microsoft, http://go.microsoft.com/?linkid=9762340, 2011).

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Table of Contents

Executive Summary i
Introduction 1
Chapter 1: Education & Training 2
Chapter 2: Security Software Assurance Development Standard 5
Chapter 3: Threat Modeling 9
Chapter 4: Coding Practices 14
Chapter 5: Security Testing 18
Chapter 6: Pre-Implementation Practices 28
Chapter 7: Software Assurance Documentation Archive Best Practices 30
Chapter 8: Post Implementation Phase Controls 35
Acknowledgements 38
Appendix A – Education & Training 40
Additional Resources 50

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Introduction

The BITS Software Assurance Framework represents a set of common practices within financial services firms to improve software security for customer- and employee-facing applications. This framework leverages the maturity of software assurance controls that were adopted by financial services firms in recent years and is intended to provide guidance and serve as a reference tool for financial services firms interested in improving software security controls and practices.

The framework is based on the following principles:

1. Software security is an essential dimension of software quality and should be part of an overall effort to consistently measure and improve the quality of the software development and integration practices for financial service firms.
2. IT risk controls are most effective when they are imbedded within core business processes during the software development process as opposed to being subsequently added or "bolted on" during risk assessment processes outside of software development activities.
3. Security vulnerabilities in software should be treated as defects (bugs) that require remediation to the application architecture, design, or application code within the software development lifecycle.
4. The use of techniques, practices, and tools that identify security vulnerabilities should be applied as early in the lifecycle as feasible to improve software quality and reduce the increased cost associated with subsequent fixing of defects.
5. Building and integrating software from third parties is a common and efficient practice for financial service firms. The practices discussed in this Framework are appropriate whether software is developed internally, developed by a third party, or purchased through a third party.
6. Investment in the development of resilient software components that are shared across applications within an enterprise represents an example of an *application architectural framework* that both improves quality and is a vital source of preventative software security controls.

These principles have emerged over time from the practical experience of many software security program implementation efforts in major financial services organizations. They represent the collective experiences from each implementation effort. This Framework identifies practices and essential controls for a successful software security program implementation by a financial services organization. The above six principles should be considered design principles when developing or enhancing an existing software security assurance program.

The Framework addresses the following key component areas:

- Education & Training
- Security Software Assurance Development Standard
- Threat Modeling
- Coding Practices
- Security Testing
- Pre-Implementation Practices
- Software Assurance Documentation Archive Best Practices
- Post-Implementation Phase Controls

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Chapter 1: Education & Training

The BITS Software Assurance Framework identifies the essential components and principles of a mature software security program. A primary criterion for a successful program rests with the level of influence and change in behavior of application developers and systems integrators. There are many complex technical challenges in deploying vulnerability detection and management capabilities within a software security program for medium and large organizations, but all successful programs share a common commitment to education and training. An effective measurement of program maturity is to poll application developers to determine if they know the difference between a software vulnerability and a software defect. If the majority of developers answer that vulnerabilities and defects are one in the same, then the education program can be considered successful. In fact, this is the single moment of truth for developers embracing secure development practices.

Software development, whether commercial or not, involves the constant removal of defects from application code through iterative testing and modifications until the software reaches acceptable quality for the investment made. Developers know how to deal with defects in a development process. Developers that defer or delegate security vulnerabilities need to understand that the vulnerabilities are nothing less than defects that need to be prioritized and fixed. This sounds straight-forward but it actually represents a significant challenge. The education and training program in a mature software security program represents the "lubricant" to behavior change in developers and as a result, is an essential ingredient in the change process.

In addition, a mature software security program also helps developers understand that while minimizing the impacts of security vulnerability defects is a key component of secure development, utilizing effective architectural features, such as memory protection techniques, can serve to minimize the impact of unknown vulnerabilities.

For example, in early 2008, Dan Kaminsky discovered a critical vulnerability in the domain name service (DNS) system. The DNS system translates domain names that people understand, like www.blah.com, to IP addresses that computers understand, like 204.11.200.1. This creates an entire family of vulnerabilities—for example, the DNS system on PCs can be fooled into thinking that the IP address for www.badsite.com is really the IP address for www.goodsite.com, and there is no way for users to tell the difference. This flaw allows cyber criminals at www.badsite.com to trick a user into doing all sorts of things when their browser takes them to their site, like giving up bank account details. Kaminsky had discovered a particularly nasty variant of this DNS cache-poisoning attack. This vulnerability was unknown in the original design and testing of the DNS system.

What is important in this example, however, is how *good design decisions* can make software secure and resilient from vulnerabilities and attacks yet to come. Years ago, cryptographer Daniel J. Bernstein looked at DNS security and decided that source port randomization was a smart design choice. Bernstein did not know about the specific vulnerability or of Kaminsky's eventual attack design, but he saw a general class of attacks and realized that this enhancement could protect against them. Consequently, the DNS program he wrote in 2000, "djbdns", did not need to be patched—it was already immune to Kaminsky's attack. It is a very good example of how teaching techniques of good

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

design and their subsequent use can result in software secure not just against known attacks, but also against unknown attacks and attacks yet to come[2].

Two fundamental constructs of a software security education and training program have emerged in recent years in recognition of the evolution of educational content and the significance of education as an essential ingredient in a successful implementation:

1. While many consider application developers to be the primary, critical constituency for education, that single constituency is not enough to reinforce appropriate behaviors within an organization. Education is essential for all of the key roles within the software development and integration process including:

   - DBAs
   - Project Leads
   - Project Managers
   - Architects
   - Quality Assurance Testers
   - Information Risk Professionals
   - Business and IT Management
   - Business Systems Analysts (BSAs)

   In addition, distinct application developer curricula, depending on the development platforms, are necessary. For example, here are several different groups of developers who require a separate curriculum:

   - Java developers
   - .NET developers
   - COBOL developers
   - Mobile application developers
   - SQL developers

2. Educational content for software security today is available from many different vendors and can be tailored to the specific groups of stakeholders that need it. The content can be delivered via e-learning, through workshops, and through traditional classroom settings. In addition, integrating this education into corporate Learning Management Systems (LMSs) is common and practical given recent adoption of standards. Some customization of the material specific to an organization's Software Development Life Cycle (SDLC) may be required along with specific workshops, but the majority of the educational content is already available from 3rd parties today.

[2] Merkow, M. S., & Raghavan, L., Secure and resilient software, requirements, test cases, and testing methods. (Auerbach Publishers, 2011).

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

One common approach includes defining the various stakeholder groups up front (Java developers, architects, project managers, Q/A staff, etc.) and assigning owners of each stakeholder group the responsibility for defining the mandatory and optional curriculum for their respective group. The owners evaluate and adjust the education and training content as the needs evolve. A formal review can be conducted annually to assure that the content remains current and relevant. In addition, the curriculum can be separated into awareness sessions and hands-on training for more in-depth content. Specific examples of awareness education for three stakeholder groups from an existing program are provided in Appendix A.

A sample description of stakeholder groups and specific curriculum is also available in Appendix A. By no means is this list exhaustive, but is illustrative of key items one should consider a baseline when evaluating an education program.

Integrating IT risk controls within the software development process as a part of a software security program requires on-going education for key stakeholders since the techniques and approaches are continually evolving. For example, this is clearly evident with the recent growth in developing applications for deployment on mobile platforms. Another model gaining traction is the development of an architectural construct, designed to take Java applications and port them to different mobile platforms so that developers can focus on Java development and this component will adapt the code to the targeted mobile platform. This allows the development teams to integrate Web development tools (e.g., static analysis) in the development process and leverage dynamic scanning capabilities (e.g., application penetration testing) in the Quality Assurance phase prior to configuring the applications for the target mobile platform. Dealing with the differences and complexities in security capabilities across mobile devices is indeed a challenge. A few organizations have taken steps to separate the responsibilities of development teams from software release teams that approve the distribution of mobile applications for both internal and external use. Final testing then includes manual penetration testing and/or using automated testing tools to test security and quality attributes of the program.

As development processes continue to evolve, on-going education for all stakeholders involved in the application development process is a must.

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Chapter 2: Security Software Assurance Development Standard

A holistic, process-based approach to implementing secure application development techniques has been proven to lead to substantially better outcomes in terms of designing security into the application and creating mitigations for potential future vulnerabilities. One of the crucial early steps for this process is to conduct a risk analysis and to define a ***minimum standard of security and privacy*** attribute for the particular application. This process of considering these requirements early on sets the stage for decisions later in the process to classify issues and to make judgments about the quality of the security and privacy process. Creating this standard helps improve the efficiency of the entire development process - not just the security aspects. Noting the work done by Forrester[3] and Aberdeen Research[4], implementing a holistic secure development program with this type of requirement setting and early security design work can result in a significant return on investment in terms of resource time and schedule.

Minimum Development Standards

All application software must have a documented risk analysis performed before design begins with clearly identified areas where security practices, such as threat modeling, design reviews and scope of dynamic testing are defined. This risk analysis should also highlight specific security requirements relative to the intended use scenarios and environment. Outcomes from this process include quality gates that define the required security and privacy standards. The quality gates also provide a mechanism to assess progress and to provide a sense of overall risk mitigation maturity of the application. Bug bars are one type of quality gate that set thresholds for classifying security and privacy vulnerabilities. As developed by Microsoft for use in its Security Development Lifecycle, bug bars provide a tool to complete the critical steps of both classifying vulnerabilities and the severity of vulnerabilities that are permissible.[5]

Examples of Security Bug Bars

Severity	Example Issues
Critical	Remote elevation of privilege
Important	Denial of Service
Low	Spoofing (As part of bigger attack scenario)

[3] Forrester Consulting Thought Leadership Commissioned by Microsoft, State of Application Security, Immature Practices Fuel Inefficiencies, But Positive ROI Is Attainable (http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=2629, 2011).
[4] Aberdeen Group; Securing Your Applications: Three Ways To Play, Part Three (http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6968, 2010).
[5] Bryan Sullivan, Add a Security Bug Bar to Microsoft Team Foundation Server 2010 (MSDN Magazine, 2010).

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Examples of Privacy Bug Bars

Severity	Example Issues
Critical	Lack of notice & consent
Important	Lack of data protection
Moderate	Data minimization

Components of a Secure Application Development Standard

The following is a high level list of the components needed for an effective secure development standard:

1. The development standard must be consistent with and reflect the institution's regulatory obligations and internal policies.
2. The development standard must address the key elements of privacy and data collection minimization. These issues need to be addressed early in the design process.
3. Applications must be mapped to the standard risk classification criteria so that all stakeholders understand what controls are required in all subsequent development phases.
4. The standard must be unambiguous and well documented to enable meaningful decisions during design, coding, testing and final security review.
5. The standard must explicitly map out the expected quality gates with exit criteria that provide a clear and unambiguous indication of the results for each quality gate, thereby creating a body of evidence that can be used in the final security review prior to application deployment.
6. Privacy and data governance requirements must be incorporated into the standard to assure these important issues are considered along with software security.
7. A tracking mechanism is also needed to enable tracking of all vulnerabilities, work items and quality gate completions.
8. The standard must produce, on a project-by-project basis, consistent artifacts that validate compliance with the standard. These artifacts must be retained for use by third-parties (e.g., auditors, regulators, software purchasers) who may wish to validate the process.

A critical consideration of all of the listed requirements is to assure that the development standard is well-defined and unambiguous so that clear quality decisions can be reached during the development and testing phases.

Quality of the Development Standard

The practical applicability of any development standard comes down to the quality and clarity of its construction. The key to that, is assuring that all of the components enumerated in the previous section are covered. The standard must also be practical relative to development and test phases being able to meet the risk mitigation criteria. The standard must be clear and implementable and must provide the ability to make clear choices about the severity and required remediation of bugs that are identified by the process. The usefulness of a development standard is derived from the ability for everyone to use it, consistency in the standard and its application. An example is that a developer when running a static analysis tool discovers a bug. Based on the criteria identified in the secure application development standard, the developer should be able to rate the severity of the issue and take the appropriate steps to mitigate without outside advice or assistance. Only when all

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

of the issues that do not meet the development standard or bug bar have been met can the gate be passed and the process can move to the next step. This allows an organization to see great efficiencies since the best, easiest and least expensive place to fix issues is at development time rather than fixing them later based on input from subsequent stages in the process. Testing can then be focused on other, more complex issues since many of the bugs would have already been identified and remediated. Before any application can be moved to production, it needs to demonstrate that it has met the application development standard at **every** quality gate and that there are no remaining issues.

It is also helpful to consider engaging internal or external resources who are security and privacy experts to help at this stage. Involving this type of expertise early can help identify issues earlier and help set the appropriate context for the subsequent development and testing. This can result in significant savings compared to having these issues arise later or even worse, missing key issues.

As the development standard, and more broadly the Framework, is applied, the following key questions should be considered to help identify where deep assessments need to be undertaken to identify the security and privacy functional aspects of the applications:

1. (Security) Which portions of the project will require threat models before release?
2. (Security) Which portions of the project will require security design reviews before release?
3. (Security) Which portions of the project (if any) will require penetration testing by a mutually agreed upon group that is external to the project team?
4. (Security) Are there any additional testing or analysis requirements that critical outside constituencies (e.g., auditors, regulators, third party assessors) deems necessary to mitigate security risks?
5. (Security) What is the specific scope of the fuzz testing requirements?
6. (Privacy) What is the Privacy Impact Rating? The answer to this question could be based on the following example guidelines:
   - P1 High Privacy Risk. The feature, product, or service stores or transfers PII, changes settings or file type associations, or installs software.
   - P2 Moderate Privacy Risk. The sole behavior that affects privacy in the feature, product, or service is a one-time, user-initiated, anonymous data transfer (for example, the user clicks on a link and the software goes out to a Web site).
   - P3 Low Privacy Risk. No behaviors exist within the feature, product, or service that affect privacy. No anonymous or personal data is transferred, no PII is stored on the machine, no settings are changed on the user's behalf, and no software is installed.

Improving the Secure Application Development Standard

As organizations exercise the Secure Application Development Standard through their application development projects, they have an opportunity to learn lessons from those activities. How that learning occurs is primarily dependent on both the size of the organization and the number of development projects it undertakes.

In smaller organizations, or those with fewer development projects, it may be possible to perform a post-project lessons learned exercise after every application development project. In larger

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

BITS Software Assurance Framework
Security Software Assurance Development Standard

organizations, or those with many development projects, individual post-project exercises may not be feasible. These organizations might consider post-project exercises for select projects (e.g., those of higher criticality or investment). Larger organizations often use other options, which are also useful tools for smaller organizations, such as measuring defect results across projects at various phases and monitoring production environments for defects that they track back to specific projects. Regardless of approach, there needs to be a robust process for measuring the effectiveness of the overall secure development lifecycle that serves to identify the need for improvements.

In addition to measuring effectiveness, institutions should consider other methods to improve their process. For example, as new use cases emerge, institutions should use them to expand both the risk profile for the particular application for which it emerged and the applicability to other applications' risk profiles. Likewise, organizations should monitor changes to regulatory or compliance requirements and integrate those changes into their risk profiles. The key though is that, for a given risk profile, the development standard should stay relatively consistent within an organization.

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Chapter 3: Threat Modeling

Threat modeling is essential for resilient software design and development and is defined as:

> *Threat is anything that can act against an asset resulting in a potential loss. Risk is the magnitude of a loss and the frequency or probability of that loss. Threats act on or exploit a vulnerability in an asset resulting in a risk of loss. Threat modeling is the process of introducing threats into the application design phase of a software development lifecycle with the explicit purpose of influencing the design to address the most likely threats to the application's security and resiliency. Threat Modeling is often one part of a security requirements phase or architecture review phase that is part of application design.*

Threat modeling is one of the most important components for addressing risk in the development of software yet it remains one of the more elusive controls to implement consistently within an organization. There are several reasons for this elusiveness in consistently applying threat modeling in the design of software including:

- Confusion on what constitutes a threat vs. a vulnerability vs. a risk
- Lack of guidance on methods to identify assets
- Requiring participants with requisite expertise and training in threat analysis, a strong understanding of application design and a well-structured process
- Security experts often learn from different risk profiles and use different techniques for modeling
- Teaching threat modeling requires an apprentice-based approach that involves an appropriate curricula, adequate investment in effective education tools and a process for educating appropriate constituencies
- Different types of applications have very different risk profiles meaning the threats will vary depending factors such as the application architecture

The basic components of a threat model typically include:

- **Threat Actor**- the "who" that wishes to attack an application
- **Threat Vector (or Attack Surface)** - applies to the approach and opportunity a threat actor has to execute a specific attack. A large attack surface means there are many opportunities for a threat actor to find and exploit vulnerabilities. A small attack surfaces means there are limited opportunities for the threat actor to succeed.
- **Use Case** – A specific, often important, intended action taken by the system or the end users of the system, such as logging into the application or querying a database.
- **Abuse Case**- this is similar to a use but identifies a specific attack approach and how the application may be compromised. These are sometimes referred to as misuse cases.
- **Trust Zone**- This refers to aspects of the application where imbedded controls (e.g., authentication) protect against malicious attacks or threats and those with access to the trust zone can be trusted at a higher level than users of public sites.

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Threat modeling is most effective as part of an architecture or design review process where technical considerations are addressed along with the threats and risks of a specific design option. The most significant aspect of the introduction of threat modeling into an architecture review process is the recognition that making design changes to accommodate improved risk management is far less expensive versus changing application code that has already been designed, developed and implemented, and can reduce remediation costs by a factor of 100[6].

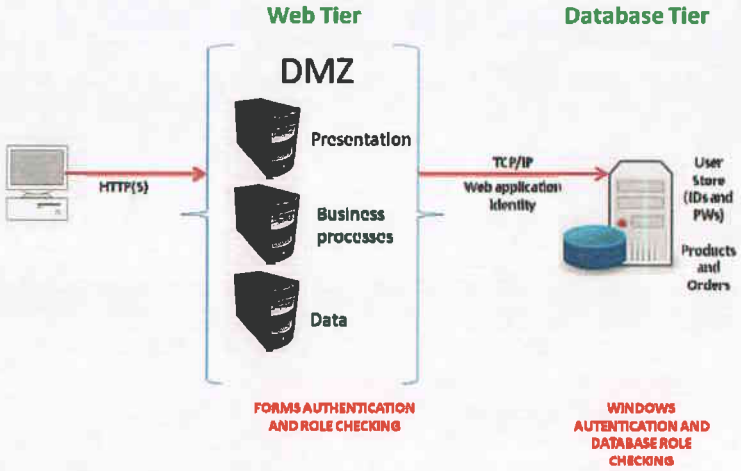
One of the key benefits of threat modeling is that the models should be developed in collaboration with the architects, developers and the QA/Test personnel. In doing threat modeling collaboratively, everyone can agree on the relative risk of different areas of an application so that when a developer has an issue he knows what severity a particular bug might be assigned and can fix it at the most efficient point - when it is being written. The QA/Test personnel benefit from threat modeling by virtue of the fact that they now have insights into how an attacker might target this application so that will be taken into consideration when exercising the threat models as part of the testing cycle. Architects can benefit since they can see where additional features or design changes could have a significant impact on the relative security of an application.

Threat modeling outputs should include identification of all relevant assets (e.g. databases, servers, applications, Web services, etc.), architectural diagrams, dataflow diagrams and trust boundaries (identified either in the architectural diagram or dataflow diagram). A mature threat modeling process will include a library of threats and attack patterns that can be applied to various scenarios. This ensures that all threats are considered and taken into account during the modeling phase. Any new threats/attack patterns identified as part of threat modeling are added to the library for future use. Some organizations choose to develop specific threat models for different architecture types or archetypes (e.g., ATM threat model, consumer on-line banking threat model, business-to-business institutional trading threat model, etc.).

Threat modeling should include creating a diagram for the application designed. A simple example of such a diagram follows.

[6] Boehm, Barry W., and Richard Turner, Balancing Agility and Discipline: a Guide for the Perplexed (Boston, MA: Addison-Wesley, 2006)

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.



Threat modeling should also include a data flow diagram (DFD) since data should be clearly classified and managed accordingly. Data flow diagrams are used to graphically represent the application using a standard set of elements including: data flows, data stores, processes and interactors. Microsoft recommends including trust boundaries in the data flow diagram. DFDs can be drawn using these symbols according to Shawn Herman, Scott Lambert and Tomasz Ostwald and Adam Shostack from Microsoft.[7]

Item	Symbol
Data flow	One way arrow
Data store	Two parallel horizontal lines
Process	Circle
Multi-process	Two concentric circles
Interactors	Rectangle
Trust Boundary	Dotted line

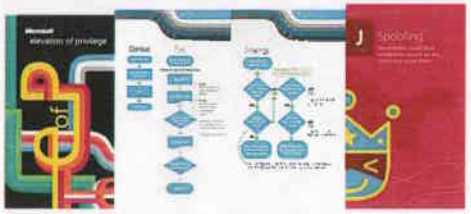
[7] Shawn Herman, Scott Lambert, Tomasz Ostwald and Adam Shostack, Uncover Security Design Flaws Using The STRIDE Approach (MSDN Magazine http://msdn.microsoft.com/en-us/magazine/cc163519.aspx, 2006)

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

This group recommends the use of the STRIDE approach:

Threat	Security Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

Adam Shostack of Microsoft produced a highly creative way to teach software development teams using a card game called Elevation of Privilege[8], which is fun to play and makes it easy to learn threat modeling. A sample of a card is shown below:



One of the more challenging aspects of threat modeling is recognizing that an Internet-facing money movement banking application for retail consumers carries a very different risk profile from a business to business money movement application behind a VPN with two factor authentication. There are indeed risks for both applications but they differ and determining the actual risk for any given application architecture is essential to leverage threat modeling effectively. An Internet-facing application that requires detailed customer personal information will have an inherently higher risk than an application that offers marketing collateral to prospective customers without a registration process.

Many organizations will classify the application risk of a given project to develop a new application during the design or requirements phase using a simple High, Medium, or Low risk designation. The advantage of classifying applications early in the lifecycle is that it yields the opportunity to apply controls to the development process that are commensurate with the level of risk. Applications that process sensitive customer information gathered over the Internet will have a higher risk classification than Websites with public information. The corresponding risk classification informs which appropriate controls must be applied for the remainder of the SDLC. As an example, an application classified as high risk may require approval from a security architect

[8] Microsoft® Security Development Life Cycle, Announcing Elevation of Privilege: The Threat Modeling Game (Microsoft, http://blogs.msdn.com/sdl/archive/2010/03/02/announcing-elevation-of-privilege-the-threat-modeling-game.aspx, 2010)

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

before IT Management approves funding for the development of the application as a way to assure appropriate understanding and managing of risk in the application design phase.

Many organizations will use threat modeling to apply a risk score to a given application along with the classification. There are several advantages to using a risk score in addition to the risk classification of high, medium and low including:

- Makes it easier to determine the relative risk of one development project from another across application portfolios or business units
- Implements standards that require specific controls based on either the classification and/or the risk score
- Measures the risk at multiple points in the development process to better define residual risk throughout the lifecycle leading to production of the application
- Measures risk trends over a period of time across an application portfolio

The most effective use of threat modeling in financial services organizations integrates a security requirement or architecture review with a governance process. An example of this is when funding approval requires a specific architecture review that includes a risk assessment based on threat modeling in the design phase. In most organizations, application enhancements or development of new applications to support business needs represents a core business process that is essential to the success of the financial services organization. Therefore, the integration of IT risk controls within the software development process as part of IT Governance represents a high level of maturity for an organization.

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Chapter 4: Coding Practices

Mature coding practices help to assure that the code being developed protects the confidentiality, integrity and availability of the data, business processes and informational assets necessary for successful operations. Often, developers do not account for security validation of the code as part of the code review or development process. There are several reasons for the absence of security as part of software coding practices including:

- Developers lack of understanding of security vulnerabilities
- Lack of secure coding process
- Lack of developer training and education on secure coding practices
- Insufficient architectural and design knowledge to identify security controls provided by the environment/frameworks as opposed to those that have to be coded
- Absence of a central repository of approved security software libraries

It is far less expensive to build secure software than to fix security issues once the software is deployed. In addition, if a breach occurs, the costs can increase dramatically based on the type of compromise and remediation efforts involved. Secure coding practices are **critical** for developing secure code.

Several secure coding practices processes are available in the marketplace (e.g., OWASP Secure Coding Practices Guide, Department of Homeland Security Build Security In Portal, CERT Secure Coding, MSDN Security Developer Center). Common recommended practices include:

- General Principles:
  - Principle of least privilege, late privilege (grant elevated privileges as late as possible in processing), and minimum duration privilege (drop elevated privileges as soon as possible)
  - Reducing the attack surface, i.e., expose the least number of services/functions necessary for satisfying requirements
  - Confirm the integrity of all third-party code using crypto (e.g. hash sums, digital signatures)
  - Consider timing and race conditions
  - Initialize all data stores and variables
  - Ensure application does not use functionality that breaks compatibility with any operating system security vulnerability protection features (e.g. ASLR & DEP])[9]
  - Use of Data Flow Diagrams to fully understand all entry and exit points
  - Complier switches that flag unsafe practices should always be used (e.g., /GS)
  - Developers should run static code analysis tools before checking in code

[9] Microsoft® Security Research and Defense, On the effectiveness of DEP and ASLR (Microsoft, http://blogs.technet.com/b/srd/archive/2010/12/08/on-the-effectiveness-of-dep-and-aslr.aspx, 2010).

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

- Authentication and Access Control
  - Fail-safe and/or fail-secure, as appropriate, application authentication and access controls
  - Use trusted processes/objects (do not trust client-side controls) for access control decisions
  - Validate all requests made by authenticated users, not just the initial request
  - Ensure only authenticated and authorized users can access application resources
  - Do authentication and access controls checks **only** on the server
  - Centralize authentication and access control functionality using common approved libraries
  - Protect against brute force attacks by enforcing account lockout
  - Review design of password reset functionality and ensure it is secure
  - Ensure high entropy of authentication credentials and security questions. Enforce authentication credentials history and expiration policies
  - Use out-of-band communication and multi-factor authentication for critical applications
  - Do not store, transmit or log authentication credentials in the clear. Use strong cryptographically, one-way salted hashes to store authentication credentials. Ensure restricted access to credential store
  - Avoid information disclosure by ensuring failed authentication attempts do not divulge implementation details
  - Encrypt and securely store authentication credentials used by the application to access other services, applications, and databases

- Entitlements
  - Do entitlement checks **only** by the server
  - Avoid proliferation of roles and ensure secure design by abstracting privileges into appropriate roles
  - Centralize all entitlement checks and strive to externalize entitlement logic
  - Keep the role hierarchy simple. Complex hierarchical roles and groupings lead to misconfigurations resulting in loss of least privilege

- Session Management
  - Only implement custom session management as a last resort. Strive to use session management functionality provided by underlying frameworks, Web/application servers
  - Do not mix unauthenticated and authenticated session identifiers
  - Ensure high entropy for session identifiers
  - Protect session identifiers from accidental disclosure
  - Enforce session timeouts, deactivation and force-outs

- Input Validation
  - Validate all input on the server
  - Centralize input validation functionality
  - Do input validation only on properly canonicalized data
  - Ensure all client data is validated prior to processing

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

  - Scan any uploaded files for malware

- Encoding/Sanitization of Output
  For systems where data and application controls are co-mingled (e.g. interpreters, SQL, etc.)
  - Encode (e.g., interpreters) or sanitize (e.g., SQL, XML) all output
  - Centralize and do encoding/sanitization on the server. Factor in requests to not only external systems but also internal systems

- Error Handling, Logging and Auditing
  - Avoid sensitive information disclosure in error messages, alerts, logs, and other application messages
  - Implement standard generic error messages to avoid unauthorized information disclosure
  - Centralize all error handling, logging and auditing functionality on the server
  - Ensure secure design of error reporting, logging, and auditing functionality. All sensitive operations should be logged. Type of information reported and frequency of logs should also be considered
  - Attempt to use industry standard routines
  - Restrict access to errors, logging and auditing information to authorized individuals only

- Data and Database Protection
  - Enforce encryption of sensitive data in transit, at rest and in memory
  - Ensure all entities that deal with data at rest or in transit are secure and protected against data loss (e.g., caching servers, external services/applications)
  - Limit duration of time that data exists on external systems
  - Ensure that only authorized individuals/systems can access data
  - Use parameterized queries, stored procedures and principle of least-privilege on the database

- Operational
  - Secure updating
    - Use crypto signatures for code updates
    - Secure transmission channels of code updates
  - Ensure all default accounts, passwords, services, methods, ports and processes on all systems supporting the application are reviewed, modified as appropriate and enabled only if necessary
  - Ensure only code that is required for the application to function resides on the production servers. Remove all test code, backup code, unneeded extensions, etc.
  - Ensure all authentication credentials used to access the database are encrypted and encryption keys are protected
  - Ensure all supporting systems (servers, databases, etc.) are using latest approved version and are patched. Where appropriate ensure that systems are hardened

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

- Memory Management
  - Ensure secure design of memory management and allocation. Avoid buffer overflow issues by validating requested memory and destination buffer sizes prior to use
  - Unallocate unused memory, close resources and implement garbage collection
  - Avoid use of vulnerable functions

A mature secure coding practice has a common approved library of security functions that developers can programmatically invoke. This approach has a very high return on investment (ROI) since it reduces developer training, coding, testing, documentation and increases software development velocity. In addition, it ensures consistency of implementation, higher degree of security and provides an ideal insertion point for dealing with new threats and attacks. The security libraries can be modified internally to deal with the new types of threats and attacks and if the APIs remain unchanged, the impact to developers is minimal.

A common failure is for firms to develop libraries only for a certain technology or language (e.g., Java or .NET). Firms should do an inventory of their enterprise and strive to ensure there are security libraries for all of their supported platforms.

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Chapter 5: Security Testing

Introduction

The ability to effectively validate that secure design principles, decisions, and requirements have been properly developed into a software solution is critical to a secure SDLC process. Without effective testing practices implemented into the development lifecycle, well-conceived sets of declared security requirements, security architectural designs, and/or threat models may not be adequately implemented or mitigated, resulting in a system design more prone to compromise. The Testing Practices section of this Framework describes a set of principles financial services institutions should consider when integrating security into their overall development and testing lifecycles.

Security Testing – Program Goals

It is important to consider the intended goals or purpose that an effective security testing program intends to achieve. At a high-level, the primary goal of a security testing program should be to assure that the security requirements of a software development effort have been properly implemented. Regardless if the system is being developed by internal resources or by a third-party supplier, financial services institutions should consider the following key goals for a successful testing program:

Comprehensive: A Security Testing Program must include validation of security requirements across the entire application infrastructure - not just the application itself - to include all system design elements and components, including:

- *Databases and Database Servers*, such as Oracle, MS SQL, and DB2, which store application or sensitive client data.
- *Server/Mainframe Operating Systems*, such as MS Windows, Linux, and z/OS, which host the application tier.
- *Application Servers*, such as IBM Websphere and J2EE which host the application platform.
- *Web Servers*, such as Microsoft IIS, Apache, and other that serve content with which the intended end user interacts.
- *Enterprise Architecture components*, such as Extract, Transform, and Load (ETL) environments, or Service-Oriented Architectures (SOA).

Other components, such as network routers and firewalls, may also be part of the testing lifecycle depending on the nature of the development effort, but are not specifically within the scope of this document.

Creative: The practitioners responsible for performing security testing should be creative. Threats and exposed security vulnerabilities, by their very nature, involve some element of the unknown, where security testing teams are in fact attempting to test what *should not* happen versus, say, a traditional functional or non-functional requirement with defined test

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

criteria. For example, an Internet-facing application designed to allow private wealth clients the ability to view the contents of their investment portfolio may allow the client access to portfolio statements where the full path to the statement is somehow addressable via the URL. Without adequate authorization controls in place, an attacker or malicious user could modify or craft the URL to access statements for other clients. A successful security testing program should promote innovation during the testing process through adequate security training, effective threat modeling, and good fuzz testing practices (see page 23). Each of these practices, if they involve the testing team, can encourage the testing practitioners to essentially think more like an attacker, thereby making them more successful security testers and further adding value to the security testing process.

Flexible: Business and functional requirements inevitably change during the SDLC process. A successful testing program should be able to adapt to such modifications in project scope and adjust accordingly. For example, threat models should be assessed or re-assessed for validity, and as these are updated, testing requirements against those threat models should also be updated so that they are thoroughly vetted in the testing cycle.

Integrated: Security testing should not be performed independent of the overall testing process, but rather, should be effectively *integrated* into the financial services institution's testing lifecycle. Like any successful SDLC, financial services institutions should involve the testing organization earlier in the SDLC to develop appropriate acceptance criteria and measures for success. For example, a financial services institution may consider involving testers in threat modeling exercises to help the testing team to think more like attackers and carry that mindset into the actual testing lifecycle. As noted earlier, security testing should be integrated to include all components of an application platform instead of just the application itself, and should be enabled to include specific threats identified during the threat modeling phase, all exercised by the dynamic and manual (static) testing process. Finally, as an additional measure, financial services firms should ensure, to the degree applicable, that application vulnerability scans incorporate the latest vulnerability research available and are executed against the built code base prior to the system being introduced into production, and on an on-going basis as an operational function.

Measurable: Any successful security testing program must provide mechanisms that convey the effectiveness of the security testing. Financial services institutions should consider developing metrics that meaningfully describe the testing results of previously identified security requirements and threat models. This can be done both on a system-by-system basis and on the health or success of the enterprise security testing program as a whole. These metrics can offer a balanced risk view that accurately conveys the impact, or potential impact, of any defects found. Valuable measurements on the success of the testing effort will not only provide firms accurate information related to the results of the security testing, but will also provide demonstrable, repeatable artifacts that can be reproduced to other parties, such as internal/external auditors and regulators.

Security Testing – Program Components

Creating and maintaining a security testing program that is comprehensive, creative, flexible, integrated, and measurable for any financial services institution – especially as the industry continues

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

to witness ever-increasing market changes and regulatory pressures – is essential for any software security framework. The following are key components we recommend firms evaluate for introduction into their own SDLC process to provide better assurance around security testing. Each of these components is organized by the SDLC phase where they would ordinarily occur during an iterative software testing lifecycle.

Security Testing Planning

Before any developed software code is handed to the testing team, firms should take steps to assure that the testing effort is adequately scoped based on the nature of the application and the inherent risks identified by the project team and/or the information risk management organization. Financial services firms should evaluate the following with respect to planning and program management:

- **Develop a Risk-Based Framework to Security Testing**: It is important to clearly define standards for security testing, based on the agreed-upon risk profile of the software development effort. For example, a firm may choose to allow an internal-only application that does not handle Non-Public Personal Information (NPPI) to have one or more "High risk" or "Severity Level 1" defects move into production, but that same firm may not allow a client-facing Web application to have even a single high risk defect in the released product.
    - Software applications under development should undergo an information risk assessment to determine the levels of risk, and by extension minimum security testing acceptance criteria.
    - Deviations in minimum acceptance criteria across different applications with different levels of risk should be documented via bug bars or other documented artifacts.
    - Alignment should be obtained with the development teams to triage and remediate identified security defects. Security defects should be addressed and remediated during the development cycle's quality toll gates, and, as discovered subsequently, during the application's "warranty" period or during overall lifecycle of the application post-implementation.
- **Involve Testers in the Design Phase**: Involving testers during a project's design phase – particularly during threat modeling exercises - gives testers valuable insight into how a system can conceptually be compromised. This added perspective can prove valuable to the testing team during the various testing phases.
- **Security Defects are "Defects," not just "Security Defects"**: As deviations from existing security requirements are identified or as security vulnerabilities are discovered during the testing process, these defects should be classified and grouped along with defects found on other system functional and system non-functional requirements. Severity levels previously defined for defects should be included in defect logs. Test summary reports should be escalated to management along with other defects to ensure they receive the appropriate level of visibility across key stakeholders. For example, a

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

defect within a client-facing, mortgage lending application that allows for elevation of privilege (which will likely be assigned a Severity 1), should be reported as a high risk to management along with defects that are found in the application's inability to properly calculate a potential borrower's loan-to-value (LTV) for a subject property.

- **Utilize Privatized or Sanitized Test Data**: Financial services firms should always avoid using live production data, particularly data uniquely associated with actual customers, for any testing purposes. Data used in all phases of the test cycle should either be completely fabricated, or appropriately obfuscated. Using live production data increases the exposure of a confidentiality breach, and could also introduce regulatory impacts to applicable laws, such as the Gramm-Leach-Bliley Act (GLBA), the standards such as the Payment Card Industry Data Security Standards (PCI-DSS), and the disclosure guidance of the Securities and Exchange Commission (SEC).

Decisions regarding masking of sensitive data that is moved from a production environment to a non-production environment (test, quality assurance, user acceptance test, development, etc.) for the explicit purposes of testing the functionality of the application are often determined based on either the classification and/or the risk score. Most organizations ensure their production environment controls include more rigor than non-production environments so that the movement of data outside of a production environment requires a de-identification (or de-personalization) process. Data de-identification can include:

- Data masking – identifying sensitive data like a Social Security Number and changing the values
- Data tokenization – changing the characters using a method that enables changing them back to the original characters using a key structure
- Obfuscation – changing the format and number of characters randomly

Data de-identification is often used in the testing phase of development but it can also be incorporated into the application itself to prevent sensitive information from being shared when it is not necessary. A common example of this technique applies to customer statements that only include the last 4 digits of an account or credit card.

- **Evaluate the need for Penetration Testing**: Certain high-risk financial systems, such as mobile banking or mobile payments systems, and even automated teller machines (ATMs), may benefit from a targeted penetration test. Consider however, that any penetration testing effort is only as comprehensive as the amount of time or money devoted to it and the competency of the tester. Consequently, firms should consider the expected value or benefit from conducting such testing, perhaps limiting it to only its highest-risk systems.

Security Testing Execution

Once testing requirements have been identified, the appropriate testing resources allotted and the application correctly deployed in a Quality Assurance (QA) or other non-production environment, firms can begin validating that security requirements have been effectively coded into the developed

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

software. What follows is an overview of a variety of test execution methods for financial firms to consider, based on both the application's architecture and its risk profile.

As mentioned previously, firms should ensure that the testing process is tightly integrated with the existing enterprise software development and testing framework, and where possible, should leverage existing tools to track results and defects to provide consistent reporting to all stakeholders.

- **Automated Testing**: Similar to traditional functional, integration, and/or client acceptance testing of non-security related requirements, testing results for security requirements are usually performed most consistently when automated tools are used. For example, a routine requirement such as input validation can be evaluated using a variety of automated tools, such as Hewlett Packard's Quick'Test Professional (QTP) or Microsoft's AppVerifier, with a greater degree of assurance than manually testing input validation on every field and in every form that requests user-supplied input. Web application vulnerability scanners can also be useful in this regard (see Web Application Vulnerability Scanners, as discussed later in this section).

- **Static Code Analysis**: Static code analysis involves evaluating pre-compiled source code to evaluate conformance to identified security requirements. Because the code is not yet compiled or built, static code analysis is usually performed by the development staff, before the compiled code is released for testing.

  Examples of where static code analysis could be helpful can include identifying instances where:
  - Insecure or unauthorized APIs or language functions are referenced
  - Actual SQL statements being directly called in stored procedures
  - Code could be exploited to create memory buffer overflows

- **Dynamic Code Analysis**: As opposed to static code analysis, dynamic testing should be performed on post-compiled source code that is actually running. For this reason, dynamic testing is only capable of identifying defects on code while it is actually executed, as opposed to the entire code base available to static testers. Financial services firms should rely on their testing organizations to perform the dynamic code analysis. Care should also be taken to ensure that dynamic testing efforts achieve appropriate coverage across all the application's components (i.e., Web servers, databases, etc.). Dynamic code analysis should be performed, as appropriate per a firm's pre-defined risk assessment, on completed and/or compiled code for both client/server, desktop or mobile applications, and web-based applications.

  - **Client/Server & Compiled Code**: There are a variety of commercial and open-source dynamic testing tools available to firms, including *Fortify, HP DevInspect*, and *Veracode*. Microsoft also makes available several tools which can be used to dynamically test Win32/Win64 code, such as *Driver Verifier* and *Device Path Exerciser*.

  - **Web Application Vulnerability Testing**: Web application vulnerability scanner tools provide another form of dynamic code analysis for web-based applications, and

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

the reports they generate can provide a financial services firm a quick and relatively low-cost, high-level summary of security vulnerabilities detected by the tools. Commercially-available and freeware tools and offerings from IBM, HP, Qualys, WhiteHat Security, Burp, and many, many others are available, which financial services firms can both evaluate and deploy to identify security vulnerabilities within systems under development as well as production systems. These tools work by "scanning" the application's infrastructure, and by submitting arbitrary input in an automated fashion to attempt to identify any software or system security vulnerabilities. These tools then provide the findings as a report to be viewed and assessed by system administrators and developers for further action.

Financial services firms, however, should be cautious in relying on these tools as the sole basis for evaluating an application's security for the following reasons:

- Vulnerability scanners detect vulnerabilities using an almost signature-based approach, whereby the scanner evaluates an application for vulnerabilities by inputting the same, almost predictable data. This "false negative" rate makes it possible for a skilled attacker to identify or exploit basic Web application vulnerabilities not identified by the tool.
- Conversely, vulnerability scanners often also report false positives, whereby the scanner mistakenly reports a vulnerability that does not actually exist.
- Vulnerability scanners do not take into account any threat models identified by the project team, nor do they consider emerging threats (i.e., mobile banking, remote deposit image capture, or mobile payments threats).
- Vulnerabilities identified during a vulnerability scan often require code changes to remediate, followed by another vulnerability scan to validate. Performing other security testing activities, such as static dynamic testing, may have identified and remediated these vulnerabilities at a lower cost point.

Vulnerability scanning, where performed, should be performed during the integration testing phase, ideally before client acceptance testing (CAT) or user acceptance testing (UAT) is performed.

- **Fuzz Testing**: Fuzz testing involves the practice of providing unexpected input to an application during the testing phase, and evaluating how the application reacts as a result. For example, a Web application used between mortgage companies to evaluate and underwrite flood insurance applications may provide a means by which the lender can securely upload the relevant borrower loan documents in either MS Word .docx or Adobe .pdf format. A valid fuzz test of that functionality may involve re-naming a very large, multi-gigabyte file with a .docx or .pdf extension and attempting to upload that file as a document to see how the Web application responds. The application might reject the upload, but it may also accept the upload. In doing so, does the application become unresponsive to other requests, does the application crash due to limited disk space, and if so, does it provide any revealing errors to the end user which could be useful as part of another attack?

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Firms should strongly consider integrating fuzz testing into their software development lifecycle, particularly for publicly-available, Internet-facing applications. Fuzz testing can be an extremely valuable tool in validating identified threat models or design assumptions, and can be particularly useful in validating application code developed by third-party software providers or business partners.

There are many automated fuzz testing tools and frameworks available, many of which are built to focus on application development languages or platforms, such as Python or Java. Many fuzz testers are also available as open-source software and free of charge.

Third-Party Application Testing

Applications developed or hosted by third-party software providers present challenges to testing teams, primarily because the testing team usually does not have access to the source code. The following table lists the different testing methods previously described, and how these can be performed (where applicable) with third-party applications:

Testing Type	Comments
Automated Testing	**Available**. Requires firm to have automated testing tools in place.
Static Testing	**Emerging Availability**. Generally cannot be performed without the application's source code. Reports can be requested from the software vendor or software provider. (A limited number of vendors now offer products that can perform a binary scan without access to the source code.)
Dynamic Testing	**Available**. Requires firm to have possession of the compiled binaries and libraries. Web-based applications require a vulnerability scanner, and the consent of the third-party (if hosted externally).
Fuzz Testing	**Available**. Results are better when the testers are creative, have appropriate tools, understand the business process, and any identified threat models.

Financial services firms may come across resistance from third-party service providers regarding receiving authorization to perform a vulnerability scan, due to confidentiality, availability, or other concerns posed by the provider. Firms may consider accepting the reported results of a recent vulnerability scan performed by the third-party, or the reported results conducted by an independent party. Firms should also impose contractual controls as part of their overall supplier risk management and due diligence process to ensure the provider is appropriately obligated to build and maintain appropriate security controls. Firms should use this Framework document as a basis for the types of processes and practices for building secure software that they should require of their providers.

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Other challenges exist with third-party developed systems when it comes to assessing specific security requirements as imposed by financial services firms, such as encryption in transit. Without a network analyzer installed between system components and a cryptanalyst to perform a packet analysis, it can be difficult to determine if network communications are encrypted with an authorized encryption algorithm and key length.

Firms may also have standard security requirements imposed on third-party applications related to other information security domains, such as credential management (i.e., User ID/password lengths), or logging requirements. Firms should consider developing standard acceptance criteria for these requirements so that a testing team can more easily build customized test cases to validate compliance with these requirements. For example:

Standard Security Requirement	Acceptance Criteria
[PASSWORD LENGTH] All passwords must be at least eight characters in length.	While logged into the system, attempt to modify the user's password to a value containing fewer than 8 characters and confirm a system error returns and that the password change is disallowed.

- **Validate Test Coverage vs. Code Complete (Regression Testing)**: Changes often occur in the software's scope, features, or functionality during the development and testing process. As these changes are vetted and approved, it is important for security testing teams to carefully assess the nature of such changes against the security tests already executed. Do the changes impact any validated threat models, and should they be re-evaluated? Can the changes invalidate other security testing performed previously? Financial services firms should re-assess completed security activities, and perform regression tests as appropriate to re-validate existing findings.

  For example, if an investment bank is building a new internal system to manage trust accounts for its client base, and security testing for the application is nearly complete when the business requests that the application integrate with a data feed from another application that was previously out of scope, how should that new requirement impact security testing? Should a threat model be created around that new integration? Should fuzz testing tests be performed against the integration itself? Should specific new controls integrated as a result of the new requirements (e.g., encryption in transit, if required) be validated for this new integration?

Security Testing Reporting

Reporting security testing activities is critically important in measuring the success of the security testing effort. Reporting can provide valuable insight on shortcomings not only within the specific, targeted applications, but also across entire technology portfolios or even the entire enterprise. Moreover, because of highly-regulated nature of the financial services industry, useful reporting and metrics can become instrumental in validating the effectiveness of a security testing program to other parties including auditors and regulators.

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Below are certain components of security testing reporting that financial services firms should focus on as they further build or mature their security testing efforts.

- **Validate Test Coverage vs. Requirements/Development Standard**: Software security teams at financial services firms must be able to effectively discern gaps between identified security requirements and development standards to what will actually be tested (see Development Standards section). One method of achieving this can be through a documented Testing Plan, where all stakeholders approve the testing methodology for the specific project or product prior to the code being delivered to the testing environments. The software security team should be a stakeholder or approver of the document, which along with other requirements could serve as a prerequisite for testing, and thereby help to assure that the appropriate security requirements will be evaluated.

- **Tracking Bug/Defect Remediation**: Once security testing execution is complete, the testing team must be able to provide information regarding any bugs or defects identified during the testing, along with a mechanism for tracking that defect until it has been remediated or approved, based on the severity level of the defect.

  For example, assume testing reveals a brokerage application used to track dividends paid to investors provides detailed server, IP address, and database information to the end user when a fault occurs, in violation of security standards. This defect would be assigned a Severity Level and sent back to Development team for remediation. The software security team, or at a minimum the testing team, should have visibility into the status of this effort until the defect has been corrected. Commercial testing platforms such as *HP Quality Center* provide tools to allow security stakeholders and testers insight into such activities.

- **Reporting Defects**: When the testing cycle ends, a major goal is that defects that can be resolved in the application's upcoming release are in fact resolved. There may, however, remain one or more defects that cannot be remediated. Often, these are defects whose remediation requires more significant updates to the application code, which may impact delivery timelines. Once all security testing has been completed, final Defect Reports and Test Summary Reports should be prepared and distributed to all stakeholders, including the software security team, for analysis and approval, and used as an artifact to determine whether the release can move into the production environment. The primary consideration firms should have at this stage is an understanding as to whether there are any high-risk security defects remaining in the software code. Where such defects exist, firms should incorporate a risk-based approach to determine if the release will be allowed to continue into production. Firms should also consider whether a remediation plan or point upgrade can be deployed shortly after implementation.

- **Identifying Trends**: Effective security testing reporting can provide software security teams and managers valuable insight into the overall software security development lifecycle. Well thought out reporting and metrics in this area can be used to provide answers to many questions, including the following:
  - Are certain developers or product teams in need of additional security training?

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

- Is security training having a positive effect on the number of testing defects over time?
- Are certain types of defects more prevalent than others?
- How long does it take to remediate security defects by type?
- Are minimum requirements for regulatory compliance being met by product?
- How long does it take to perform security testing?

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Chapter 6: Pre-Implementation Practices

Purpose

This section of the Framework provides a comprehensive list of requirements for software security assurance that are needed for the final production launch of applications.

Usage and Outcome

This chapter of the Framework applies during the "Release Phase" of a firm's Secure Software Development Lifecycle. Pre-Implementation Review (PIR) is a comprehensive examination of all security activities performed on software prior to its release. The PIR includes, but is not limited to, the review of threat models, bug or defect reports and reports from vulnerability assessment tools.

The PIR should result in one of the following three outcomes: Passed PIR, Passed PIR with exceptions and PIR with escalation.

- Passed PIR – Indicates that the review was conducted successfully with zero, or perhaps very minor, deviations from expected results as defined by the project team in collaboration with the security organization.
- Passed PIR with Exceptions – Indicates a conditional acceptance of the security results, and authorization to proceed into the implementation phase, under the condition that certain deviations or defects be mitigated or resolved, usually within a defined and agreed upon timeframe. For example, an internal .NET web-based application that does not store or process sensitive company or client data, whose database connection strings and passwords are stored in clear text in the web server's web.config file, may be allowed to proceed into production, so long as the connection string are encrypted in the file within two weeks of going into production.
- PIR with Escalation – The review identified significant deviations or security defects, which require escalation within the line of business to make a risk-based decision on whether or not to allow the system to proceed into production.

Any decision and relevant artifacts such as a checklist, provided in a PIR should be appropriately documented and maintained if required for independent review post-implementation.

The following checklist contains examples of considerations for use during the "Release Phase" of the Secure Software Development Lifecycle.

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

PIR Requirements Examples

#	Requirement
Security Requirements	
S1	All action items from the architecture and design review have been completed.
S2	All security defects reported from manual code review at the level of severity required have been fixed.
S3	All security defects reported from automated code review at the level of severity required have been fixed.
S4	All security defects reported from dynamic analysis at the level of severity required have been fixed.
S5	All security defects reported from penetration testing at the level of severity required have been fixed.
S6	Review threat models and ensure no new threats and vulnerabilities have arisen and all existing ones have b fully identified and mitigated.
S7	Does each unfixed security defect have an approved exception from management?
S8	Have all security settings turned on to the highest recommended level by default?
S9	Has all development data been purged from the system of record?
S10	Have all development and default service accounts been reissued and reassigned?
Privacy Requirements	
P1	All action items from the privacy review have been completed.
P2	Are all privacy related documentation/disclosures ready to launch along with the application?
Incident Response	
I1	Is a security incident response plan ready, tested and approved?
I2	Is a privacy incident response plan ready, tested and approved?
Launch Readiness	
L1	Necessary Change and Release Management formalities completed and approvals obtained?
L2	Network hardening completed in the production environment (as per approved network hardening standar
L3	Host hardening completed in the production environment (as per approved host hardening standard(s))?
L4	Is security monitoring implemented and tested in the production environment?
L5	Is a roll back plan ready, tested and approved?
L6	Is emergency patching process ready, tested and approved?
L7	Is the Disaster Recovery (DR) plan ready, tested and approved?

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Chapter 7: Software Assurance Documentation Archive Best Practices

Documentation corroborates the process used to develop software securely, the outcomes and results of each phase in the lifecycle and the actions taken to correct identified defects. This documentation will be required by various constituencies including:

- Internal and external risk review individuals such as internal auditors, external auditors and regulators
- For third-party developed software, clients for whom the software was developed.

This section of the Framework describes the types of documentation for retention, as well as suggests processes for gathering and retaining the documentation.

Inventory

There must be an application inventory that includes technology and business risk associated with the application. This inventory should have the ability to assess multiple dimensional factors and determine the inherent risk of applications.

Ideally, the inventory tool should be able to support intrinsic information and metadata about the application whether internally developed, contractor developed, or developed by offshore resources. The tool should include information such as the following:

- Application architecture
- Transaction processing amounts (ranges)
- Application interdependencies
- Regulatory requirements/oversight
- Application components such as:
  - Code base
  - Code framework
  - Development methodology utilized
  - Source code control system
  - Control points for sign-off of the code/workflows for code delivery
  - Business process supporting documentation
  - Entitlements
  - Authentication models/tools utilized

If a single source tool does not meet these needs, then a federated model of systems of record should be used to obtain the information. Without the proper identification of the risk of the application, priority decisions on the software assurance lifecycle will not be aligned with business priorities and objectives.

For vendor purchased or hosted applications, the firm must still know the information about the application and the inherent risk of it. During the analysis phase of selecting software, the same items for an internal application must be obtained.

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Lastly, the inventory must be maintained. A strong governance structure must be put in place to ensure the quality and accuracy of the data, including the key business stakeholders. Regular attestation cycles must be managed and governed to ensure data quality. Firms should leverage the information risk management of other Governance, Risk and Compliance (GRC) tools at their disposal to effectively assess and manage applications' risk in their enterprise. The implementation and use of these tools are outside the scope of this paper.

Documentation for Stages of Software Development

Throughout all of the stages of software development, artifacts should be maintained and available to the personnel who require access to the information. Hence, the process of documenting must be fully embedded within the software development lifecycle with checkpoints to ensure that the documentation is in place prior to proceeding to the next phase in the lifecycle.

As discussed below, there are key elements that should be maintained per application, preferably in the inventory or in a documentation management system. Security documentation must be included with all other documentation – it should not be maintained separately from the rest of the application. Institutions should, however, consider placing higher restrictions on access to security-related documentation. Documentation can be placed into traditional word processing or spreadsheet applications. However, when requirements are very complex, specialized requirements management tools may be warranted.

There are key document requirements that should be maintained to ensure proper quality and transparency. The process of documenting, including security documentation should be fully integrated into all phases of the development lifecycle and the documents should be side-by-side with all other application documentation.

Institutions should consider a requirement wherein they verify the documentation requirements from the previous stage have been met and verified in the application inventory before allowing movement to the next stage of the software development life cycle (e.g., gating at the appropriate stage).

Business Requirements

Business Requirements define the reasons that the application exists – they are the foundation for what will be implemented. Business analysts familiar with business needs should create the requirements and collaborate with the development teams to ensure they can be met. Without proper requirements documentation, software changes become more difficult—and therefore more error prone (decreased software quality) and time-consuming (expensive).

If the software is a first release that is later built upon, requirements documentation is very helpful when managing subsequent changes of the software and verifying that nothing has been broken in the software when it is modified.

If vendor-purchased code is sought, the business requirements should be part of a Request for Proposal.

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

BITS Software Assurance Framework
Software Assurance Documentation Archive Practices

Application Purpose and Expected Outcomes

The reason for the application's existence must be properly documented so that functionality requirements of the business are noted. It is important to clearly understand these requirements so that during testing phases the requirements are tested.

Security Property and Attribute Requirements

The expected security requirements of the application must be documented and integrated into the business requirements. Security documentation cannot be a stand-alone effort, but instead, must be integrated with the business requirements.

Entitlements

Expected functionality, including entitlements should be part of the business requirements. Periodic access control reviews typically rely on the accuracy of this information.

Functional Design Specification

This phase of the secure software development lifecycle utilizes the business requirements to develop a conceptual model of the application. Here, the business analysis and design teams work to design the functional specification for the application. This documentation should contain details regarding the workflow, architecture and overall topology as it relates to the underlying infrastructure.

Detailed Design/Architecture Specification

These documents do not describe how to program a specific routine, but indicate why the routine exists. They describe all inputs, outputs and possible data formats. Key elements that should be included are:

- Entitlement Models and Solutions Utilized (e.g., home grown or standard central corporate solution)
- Expected interfaces with other applications/utility applications
- Data Models/Relational database schema
    - Entity Sets and their attributes
    - Relationships and their attributes
    - Tables, attributes, and their properties
    - Views
    - Constraints such as primary keys and foreign keys

Threat Modeling

The finalized threat model must be maintained in the document archive facility. The threat model should document key elements of the threat analysis such as account the type of code, development framework, algorithms, interfaces, APIs and underlying infrastructure. The

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

application artifacts/documentation archive should be taken into account when developing the threat model.

Test Plans

The functionality and security test plans should be derived from the design specifications and threat model. Details of the test plans should be stored in a centralized repository accompanied with results and sign-off by the testers for all of the use cases.

Output of the test cases, which should include formal outcomes linked to defects in a defect tracking system tied to risk treatment, should also be part of the documentation.

Defect Tracking

Defect tracking is a key component of the documentation. Security defects are a subset of a functionality defect. Care should be taken to limit detailed defect knowledge to those who need to know, combined with a corporate policy that prohibits the distribution of this information, unless explicitly provided by an approved level of management.

In addition, defects can also be a powerful tool in the measurement of quality code from developers. Accurate information about the code defect is critical when this information is used in performance management activities for the developers.

A key element of defect tracking should also include the "cost to fix." If this is not measured, the ability to illustrate the cost savings of addressing vulnerabilities early in the development life cycle cannot be tied to actual data of the firm.

When dealing with suppliers, there should be formal documentation that attests to the quality of the software delivered. Any third party code defects should also be tracked in the same manner so that these can be utilized for overall supplier management, particularly during maintenance renegotiations and contract renewals.

Risk Mitigation and Acceptance

The documentation library should contain a repository to track and acknowledge the risks and mitigations or accepted risk levels. Any risk acceptance should be aligned with the acceptable risk tolerance of the firm. Personnel at the business or in centralized risk management functions who may sign off on the appropriateness of the level of residual risk should be pre-identified. Automated workflows should be used to assure approval by these key personnel. However, if the risk crosses multiple business lines and can have an enterprise impact, it must be agreed upon by a corporate governing body due to the potential impact to the firm as a whole.

Certificates of Testing

If independent firms are used for activities such as ethical hacking, they should provide written documents of their results – often in the form of certificates. There should be a central point of contact for certificates from the testing. In addition, a documented request

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

and release process should be maintained to limit distribution to those who need to know, including the appropriate level of detail to provide.

Contract Language

Contracts with third party suppliers of software should allow for the serviced organization to conduct reviews of the practices of the supplier. This Framework can provide the basis for conducting such reviews. Serviced organizations should assess the secure development processes of their suppliers against the recommended practices in each area of the framework.

Standard expectations for quality from third party suppliers of code must be maintained within a centralized group. Once created, employees must be educated on who to contact for the standard language and the legal areas to work with. If there are any areas where the third party firm is not willing to agree to terms, this should follow a standard risk treatment, aligned with the risk that this could pose to the firm.

Metrics

Meaningful metrics regarding the application secure software development lifecycle must be created and reported to various levels of management. Examples of metrics include:

- Top issues identified
- Issues by Development Manager
- Issues dimensioned to the business criticality of the application
- Cost to remediate, tied to the stage of the development life cycle
- Developer strengths/weaknesses determined by the software defects and training programs

Disposal

The desired retention period for all documentation should be established at the beginning of the application and adhered to. In addition, the disposal methodology for the documentation at application retirement must also be considered and noted in the user manual for the application.

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

Chapter 8: Post Implementation Phase Controls

An application, whether developed internally, via contract with a third party or acquired via purchase, eventually makes its way into an organization's internal or third party hosted production environment.

Once implemented, applications then enter the Post Implementation Phase of the Software Development Lifecycle (SDLC). There are significant post implementation activities required to address software security. Some of these are already in practice, but there are several new practices that are emerging as mainstream practice.

This section on Post Implementation addresses both mature (established) and emerging (new) practices that are not in widespread use, but represent a potential opportunity to enhance the software security ecosystem.

Established Practices

Defense in depth approaches to software security require multiple layers of controls within the SDLC. Recent technology innovation has enabled controls that are applicable to the early phases of the SDLC to improve effectiveness in risk management, increase efficiencies, and reduce operating costs. Multiple layers of controls also provide opportunities to "test" controls for effectiveness. For example, the use of dynamic scanning technology in Q/A following the use of static (source code) analysis in the development phase helps to determine the effectiveness of the static analysis control and the effectiveness of threat modeling in the design phase. Penetration testing beyond these other layers offers an additional opportunity to determine if the controls applied earlier in the SDLC are effective (both preventative and detective). Using a layered approach to detective controls in the development process achieves defense in depth and enables application developers to think of security vulnerabilities identified simply as *software defects* that require work to resolve. Encouraging those responsible for development to treat all security vulnerabilities found as software defects that need to be fixed according to priority (risk) is an indicator of maturity in software security. The fundamental difference between applying detective controls *prior* to production implementation and applying detective controls *within* production is in how the results should be treated or handled. Security vulnerabilities identified **during** the development and Q/A processes should be addressed simply as software defects. Software development teams, whether working at a vendor or within a company, already know how to deal with software defects. Developers may require some help prioritizing defects (based on risk), but they already know how to fix defects.

Security vulnerabilities identified in applications in production, whether within a firm or at a third party, should ***not*** be treated as software defects but as one part of the organization's security incident response process. By contrast then:

- Vulnerabilities discovered in development and Q/A are defects.
- Vulnerabilities detected in production should be treated as security incidents that require immediate attention for corrective action (remediation) and an opportunity to determine

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

if adjustments to the secure software development lifecycle are necessary to prevent future repetition of issues.

Applying this notion (defects in development, incidents in production) may represent a level of maturity that some organizations are not prepared to implement. If the organization is not ready for this approach then a target date for implementation should be established to work toward this level of maturity.

Emerging Practices

Technology advances and software security program maturity present an opportunity to significantly improve application security by treating the organization's Web infrastructure and IT infrastructure as an ecosystem filled with information that can be mined to determine specific threat trends that are unique to the ecosystem. Some organizations consider this practice area as *Software Security Intelligence*, one part of the traditional security intelligence function that exists to focus on the specific threats to specific Web applications within the organization's Web complex.

The technology advancements include software and devices designed to monitor, and in some cases prevent, security threats within the production environment. In addition, tools to detect the presence of malware on Web applications or spread through banner ads and pop-ups have emerged as useful production monitoring capabilities. Another category of tools support the detection of security vulnerabilities in Web applications running in production. The software includes commercial or custom software components designed to closely monitor Web application behavior within production and identify potential security threats and exploits. The hardware and software appears in the form of application firewalls designed to operate in a passive or protective mode, running rules that interpret application behavior in real time and either report on or block certain application behavior deemed to be malicious based on the application firewall rules.

Both of these very different technology components share one common characteristic – they offer real time monitoring of threats within a Web complex to observe potential exploits and learn how threat attack vectors evolve. The threat trend information from these sources is highly valuable and should influence the following:

1. Threat models used in application design
2. Rules used for static analysis tools
3. Types of dynamic scanning used
4. Techniques used in penetration testing

All of these controls today are based on either OWASP Top 10 or SANS Top 25 Application Programming Errors. Both sources are valuable, but both represent an earlier generation of software security intelligence. They represent commonly exploited vulnerabilities across the Web landscape for all organizations and they have had a profound effect on improving software security programs over the past 5-6 years.

The point is, when you want to know whether to bring your umbrella to work or not, do you look at a weather satellite image of North America from last year or do you look at the local weather forecast for your location? The latter helps you answer the question, the former is simply

© BITS/The Financial Services Roundtable 2011. All Rights Reserved.

REVERSE TRADE MISSION SURVEY

The Business Council for International Understanding is committed to the goals and objectives of the U.S. Trade and Development Agency. It is therefore important to us to ensure the quality of our work and of the programs that we offer on behalf of USTDA.

The following survey is to assess the usefulness of the program to date in terms of the added value it has provided, as well as to identify improvements for the subsequent phases of the program. We appreciate you taking the time to complete the survey and provide feedback.

Additionally, if you have specific concerns or comments that you would like to discuss in greater detail, please contact Nina Kundra at n-kundra@bciu.org or Tel: 212-490-0460.

AGENDA, SPEAKERS & PARTICIPATION

How would you rate the overall quality of the itinerary, in terms of cities and companies selected for meetings, U.S. Government agencies, and briefings? Please Explain.

<EXCELLENT> <VERY GOOD> <AVERAGE> <NEGATIVE>

What were your goals and objectives for the RTM, and how were they met? Please explain

<EXCELLENT> <VERY GOOD> <AVERAGE> <NEGATIVE>

Do you feel that you have gained possible business opportunities from your trips to Washington, D.C.; New York and California which you can follow up upon your return home? Which companies/ organizations do you intend to follow up with upon your return home, if any? Please Explain.

<EXCELLENT> <VERY GOOD> <AVERAGE> <NEGATIVE>

How would you rate the quality of the meetings and presentations provided during meetings in *Washington, DC*? On average, did you find that they were experts in their fields and had a great deal of knowledge to impart? Please Explain.

<EXCELLENT> <VERY GOOD> <AVERAGE> <NEGATIVE>

How would you rate the quality of the meetings and presentations provided during meetings in *New York*? On average, did you find that they were experts in their fields and had a great deal of knowledge to impart? Please Explain.

<EXCELLENT> <VERY GOOD> <AVERAGE> <NEGATIVE>

How would you rate the quality of the meetings and presentations provided during meetings in California? On average, did you find that they were experts in their fields and had a great deal of knowledge to impart? Please Explain.

<EXCELLENT> <VERY GOOD> <AVERAGE> <NEGATIVE>

What specific products or services are you most likely to consider acquiring in the next 12 months?

How would you rate the potential for future business opportunities from the meetings during the Reverse Trade Mission?

Meeting	Excellent	Very Good	Average	Poor
U.S. Department of the Treasury, Office of Technical Assistance	☐	☐	☐	☐
IBM/Initiate	☐	☐	☐	☐
NACHA, the Electronic Payments Association	☐	☐	☐	☐
Experian	☐	☐	☐	☐
MicroStrategy, Inc	☐	☐	☐	☐
Unisys Corporation	☐	☐	☐	☐
Export-Import Bank of the United States	☐	☐	☐	☐
Banking Industry Technology Secretariat (BITS)	☐	☐	☐	☐
Mandiant Corporation	☐	☐	☐	☐
Federal Deposit Insurance Corporation (FDIC)	☐	☐	☐	☐
SQN Banking Systems	☐	☐	☐	☐
Oracle	☐	☐	☐	☐
New York Stock Exchange (NYSE)	☐	☐	☐	☐
CA Technologies	☐	☐	☐	☐
Society for Worldwide Interbank Financial Telecommunication (SWIFT)	☐	☐	☐	☐
Fiserv, Inc.	☐	☐	☐	☐
MorphoTrust USA, Inc./ L-1 Identity Solutions Inc	☐	☐	☐	☐
Visa/Paul Hastings LLP.	☐	☐	☐	☐
Symantec Corporation	☐	☐	☐	☐
EMC Corporation	☐	☐	☐	☐
Informatica Corporation	☐	☐	☐	☐
Juniper Networks	☐	☐	☐	☐
Other:	☐	☐	☐	☐
Other:	☐	☐	☐	☐

How would you rate the quality of the briefing materials (this Handbook)? Were they clear and supportive of your needs? Please Explain.

<EXCELLENT> <VERY GOOD> <AVERAGE> <NEGATIVE>

FACILITIES & LOGISTICS

Has BCIU staff been helpful, available and responsive to your needs and requests? Please explain.

<EXCELLENT> <VERY GOOD> <AVERAGE> <NEGATIVE>

How would you rate the quality of the:

Travel itinerary (flight schedule)

<EXCELLENT> <VERY GOOD> <AVERAGE> <NEGATIVE>

Hotel accommodations

<EXCELLENT> <VERY GOOD> <AVERAGE> <NEGATIVE>

Local transportation

<EXCELLENT> <VERY GOOD> <AVERAGE> <NEGATIVE>

Restaurants selected for you by BCIU

<EXCELLENT> <VERY GOOD> <AVERAGE> <NEGATIVE>

Are there any specific suggestions you would like to make for improvements?

SUPPLEMENTAL MEAL OPTIONS

PRE-PAID BY BCIU AND AT NO ADDITIONAL COST TO DELEGATES

In Washington, DC, BCIU has arranged for breakfast to be provided at the Edgar Restaurant February 3-6, 2013. BCIU will provide you with breakfast vouchers redeemable at Edgar Restaurant located on the ground level of the hotel.

In New York, BCIU has arranged for breakfast to be provided at Olive's located at the W Hotel from February 7-11, 2013. Please charge your breakfast to your room.

In San Francisco, BCIU has arranged for breakfast to be provided at Sol Breakfast Cafe in the Sheraton Fisherman's Wharf from February 12-13, 2013. The restaurant is located just beyond the lobby of the hotel. Please charge your breakfast to your room.

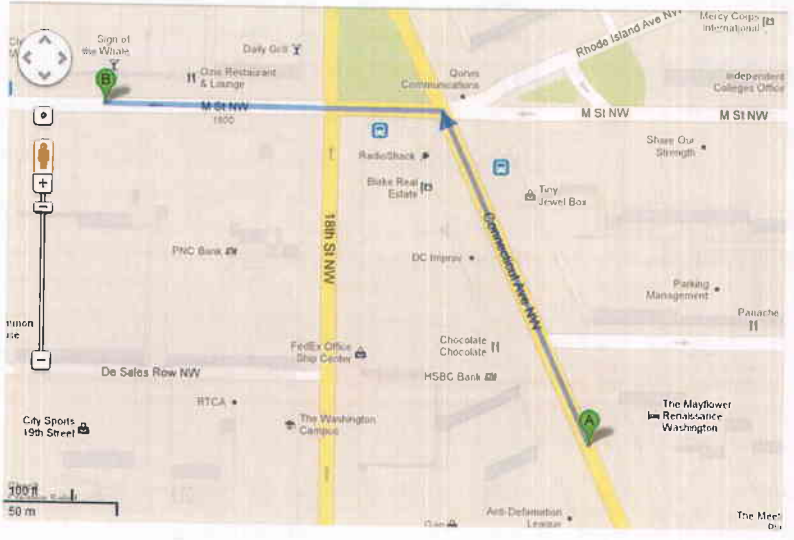
For lunches and dinners not specified on the itinerary, BCIU has arranged for several Halal and Halal-friendly restaurants, to supply dinners and lunches. Please submit the appropriate voucher, which will be provided to you by BCIU staff, to the restaurant for one appetizer, one entree and soft drink of your choice. Restaurant menus and walking directions can be found in the accompanying pages. For restaurants in California, please reference the included menus and inform us of your restaurant preferences.

Any vouchers unused need to be returned to BCIU staff upon check out of the hotel in each city. If the weather does not permit walking to one of the suggested restaurants, BCIU will reimburse for cab rides to/from the restaurants or provide alternative transportation.

Should there be other restaurants that you would visit, please feel free to convey this request to either Nina Kundra or Tosha Wilkes.

Washington, DC

MALAYSIA KOPITIAM (HALAL)



1. Head northwest on Connecticut Ave NW from The Mayflower Renaissance toward Desales St NW – 0.1 mi.
2. Turn left onto M St NW – 479 ft; destination will be on the right: Malaysia Kopitiam, 1827 M St NW.

Route Time: 4 minutes.

Malaysia Kopitiam
1827 M St NW
Washington, DC 20036-2503
Btwn 18th & 19th St NW

202 833-6232
Fax: 202 833-6233

YOUR AD HERE
MenuPages ***PRIME*** Advertising
for more info: www.menupages.com

Delivery & Takeout

Appetizers

118. Ampang Yong Tofu (A22) *mixed vegetables stuffed with minced shrimp and chicken in chicken or curry broth*..... 12.15
120. Char Tao Kuih (A25) *pan-fried rice cake with chives, bean sprouts, egg, turnip and chili sauce. hot and spicy*..... 8.85
100. Deluxe Sampler (A1) *4 skewers of chicken, 2 pieces of otak-otak, 2 pieces of curry puffs, 1 piece lo bak, 1 piece of po pia and crispy and spicy vermicelli*..... 15.45
115. Otak-Otak (A19) *salmon, minced chicken and shrimp with egg and various spices grilled in a banana leaf*..... 3.35
107. Po Pia (A8) *2 pieces of fresh soft roll with jicama, lettuce, eggs, dried shrimp and crispy shallot wrap in thin soft crepe with hot chili and hoisin sauce*..... 6.65
108. Roti Canay (A9) *flat layer of indian bread, served with bowl of curry chicken*..... 5.55
102. Satay Chicken (A3) *4 skewers of grilled marinated chicken with spices on a bamboo skewer, served with satay peanut sauce, cucumber and fresh onion*..... 5.85
123. Achar (A10) *pickles, pineapple, jicama, carrot, cucumber and cabbage in a spicy sweet and sour sauce, topped with peanuts and sesame seeds*..... 5.55
125. Vegetarian Roti Canay (A14)..... 5.55
122. Baby Oyster Omelette *pan-fried bay oyster omelette*..... 8.85
111. Curry Puff (A15) *2 pieces of crispy pastry with minced chicken and potatoes in a curry flavor.* 3.95
106. Lo Bak (A7) *2 pieces of crispy roll with pork, onion and jicama*..... 4.45
119. Plain Roti Bread (A23) *indian flat bread*..... 3.35
114. Rembah Udang (A18) *sticky rice stuffed with spicy minced chicken and shrimp grilled in banana leaf*..... 5.05
104. Satay Beef (A5) *4 skewers of grilled marinated beef with spices on a bamboo skewer, served with satay peanut sauce, cucumber and fresh onion*..... 5.85
101. Stuffed Rice Crepe (A2) *rice crepe stuffed with jicama and shrimp topped with crispy shallots and sesame seed in sweet soy sauce*..... 7.75
124. Mango & Tofu Salad (A11) *shredded green apples, green mango, fresh shallots and mint leaves tossed in sweet and spicy vinaigrette topped with fried tofu and crispy shallot*..... 8.85
126. Fried Tofu *fried tofu marinated in tamarind and honey served with cucumber and fresh onion*..... 5.05

Soups $12.15

208. Assam Laska Noodle Soup (S3) *noodle soup with tuna in a spicy sweet and sour broth topped with cucumber, fresh onions and mint leaves*..... *add salty fish*..... 3.50
206. Curry Laksa Chicken Noodle Soup (S1) *noodle soup with curry chicken and curry broth*.....
209. Ipoh Chicken Noodle Soup (S4) *noodles with shredded chicken and fish cake in chicken broth*.....
210. Penang Prawn Mee Soup (S5) *noodles with shrimp, egg and watercress in spicy shrimp broth*.....
211. Vegetarian Curry Laksa Soup (A6) *noodles with tofu and vegetables in curry broth*.....
214. Curry Laksa Beef Noodle Soup (S9) *noodles with beef in curry broth*.....
212. Fish Ball Noodle Soup (S7) *noodles with fish ball in chicken or curry broth*.....
207. Noodle Soup With Vegetables (S2) *noodle soup with mixed vegetables stuffed with minced chicken and shrimp. your choice of chicken or curry broth and type of noodles. choice of noodles: egg noodle, long thin rice noodle, flat rice noodle*.....
216. Seafood Noodle Soup (S11) *special noodles with shrimp, fish cake, and fish ball in chicken broth.*
213. Braised Duck Leg Noodle Soup (S8) *noodle soup with braised duck leg and bean sprouts*..

Salads

200. Achar Salad (A10) *malaysian pickled salad with pineapple, jicama, carrot, cucumber and cabbage in a spicy sweet and sour sauce, topped with peanuts and sesame seeds*..... 5.55
205. Indian Rojak Salad (E7) *shrimp fritter with fresh jicama, cucumber, bean sprouts and egg in spicy, sweet and sour sauce. topped with potatoes, peanuts and sesame seeds*..... 9.95
203. Veggie Salad *crispy noodles, apple, red bell peppers, lettuce, cucumbers, red onions, chinese parsley and tomato with sesame seeds in spicy lemongrass dressing*..... 11.05
201. Mango & Tofu Salad (A11) *shredded green apples, green mango, fresh shallots and mint leaves tossed in sweet and spicy vinaigrette topped with fried tofu and crispy shallot*..... 8.85
204. Satay Salad *choice of main ingredient: beef, chicken*..... 14.35

Noodles & Fried Rice

431. Beef Hor Fun (FN3) *stir-fried flat rice noodle with beef, bean sprouts and u-choy*..... 12.15
426. Curry Chicken Gravy Noodle (G1) *noodle topped with curry chicken and curry gravy, u-choy and bean sprouts*..... 12.15
427. Braised Duck Leg Noodle (FN7) *noodles topped with braised duck leg, u-choy and bean sprouts*..... 12.15
437. Hokkien Mee (FN9) *braised thick egg noodle with shrimp, fish cake, cabbage and u-choy in a thick soy sauce*..... 12.15
458. Malaysian Style Fried Rice (R5) *shrimp and chicken fried rice, malaysian style; with u-choy, tomatoes, carrots, green and red peppers, topped with pan-fried egg and crispy shallots and fresh lettuce*..... 11.05
436. Mamak Mee Goreng (FN8) *stir-fried spicy egg noodle with shrimp, tofu, bean sprouts, egg, tomatoes and potatoes topped with lettuce and crispy shallot*..... 12.15
434. Vegetarian Pickle Mustard Lo Mein (FN8) *stir-fried lo main with pickle mustard, tofu, broccoli, cabbage, green onions and carrots*..... 12.15
430. Singapore Noodle (FN2) *stir-fried long thin rice noodle with shrimp, egg, onion, green and red bell pepper in curry flavor*..... 12.15
429. Vermicelli (FN1) *stir-fried soft vermicelli with shrimp, egg, bean sprouts, green and red bell pepper - topped with crispy shallots*..... 12.15
487. Tuck Kee Noodle (FN14) *stir-fried mix of long thin rice noodle and egg noodle with shrimp, fish cake and u-choy*..... 12.15
428. Curry Beef Noodle (G3) *noodle topped with curry beef and curry gravy, u-choy and bean sprouts*..... 12.15
438. Char Kuih Teow (FN10) *stir-fried flat noodle with shrimp, egg, chives and bean sprouts*..... 12.15
435. Fish Cake Hor Fun (FN7) *stir-fried flat rice noodle, with fish cake, bean sprout and u-choy*..... 12.15
440. Kopitam Noodle (FN12) *stir-fried long thin egg noodle with shrimp, fish cake, u-choy and bean sprouts*..... 12.15
480. Mee Siam (FN13) *long thin rice noodle with shrimp, egg, chicken, tofu, cabbage, onion, carrots and red bell pepper topped with fresh lettuce and crispy shallots*..... 12.15
433. Pearl Noodle (FN5) *stir-fried thick rice noodle with shrimp, fish cake, egg, bean sprouts, carrots, straw mushrooms, green and red bell peppers, topped with crispy shallots*..... 12.15
443. Salty Fish & Chicken Fried Rice (R3) *fried rice with salty fish, chicken and lettuce*..... 11.05
439. Vegetarian Stir-Fried Mix Noodle (FN11) *stir-fried long thin rice noodle and egg noodle with cabbage, chinese mushroom, u-choy*..... 12.15

MP

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

YOUR AD HERE
MenuPages ***PRIME*** Advertising
for more info: www.menupages.com

432. Watt Tan Hor Fun (FN4) *stir-fried flat rice noodle with shrimp, fish cake, pork and u-choy in a heavy egg sauce* 12.15

Chicken Entrées

All Are Served With Rice.

423. Black Pepper Chicken (NE10) *chicken sauteed with onions, bell pepper and scallion in black pepper sauce. served with steamed rice* 15.45

422. Ginger Chicken (NE9) *steamed boneless chicken topped with fresh minced ginger. served with steamed rice* 13.25

455. Koptiam Whole Chicken (E12) *fried chicken with special chef sauce* 22.05

442. Nasi Lemak (R2) *rice cooked in coconut milk wth side of curry chicken, curry anchovies, peanuts, egg and cucumber* 12.15

411. Raja Chicken (E13) *crispy boneless chicken on a bed of our fresh made special spicy sauce side with crispy vermicelli, carrot, scallion, and parsley. topped with sesame seeds in spicy lemon grass dressing and garnished with steamed shrimp. served with rice* 16.55

404. Chicken Rendang (E5) *chicken curry simmered in thick curry gravy with coconut milk and spices. served with steamed rice* 15.45

441. Hainanese Chicken Rice (R1) *steamed white chicken breast with sweet soy sauce and special rice cooked in chicken broth* 11.05

401. Malaysian Curry Chicken (E2) *malaysian curry chicken in coconut milk and spices. served with steamed rice* 15.45

410. Nyonya Chicken (E12) *golden boneless chicken topped with fresh made nyonya dressing garnished with fresh cucumber. served with steamed rice* 15.45

Beef, Lamb & Pork Entrées

402. Beef Rendang (E3) *curry beef simmered in thick curry gravy in coconut milk and various spices. served with steamed rice* 17.65

405. Curry Lamb (E6) *chunks of lamb simmered in thick, curry gravy with coconut milk and spices. served with steamed rice* 18.75

424. Black Pepper Lamb (NE11) *lamb sauteed with onion, bell peppers and scallion in black pepper sauce. served with steamed rice* 18.75

409. Spicy Tamarind Beef (E11) *curry beef with tomatoes and eggplant, simmered in spicy tamarind sauce and topped with fresh onions. served with steamed rice* 17.65

Vegetarian Entrées

453. Vegetarian Duck (V9) *mock duck stir-fried with onion, scallion, green bell pepper and hot chili pepper* 11.05

454. Belachan Okra (V10) *dried spice shrimp paste with okra* 12.15

445. Kai Lan (V1) *chinese broccoli in oyster sauce or stir-fried in fresh garlic* 11.05

452. Vegetable Delight (V8) *stir-fried daily fresh mixed vegetables* 11.05

481. Vegetarian Goose (V5) *layers and layers of tofu sheets in marinated tofu sauce* 14.35

454. Belachan Eggplant (V4) *dried spicy shrimp paste with eggplant* 12.15

451. Curry Mixed Vegetable Pot (V7) *cabbage, eggplant, okra, green bell pepper, onion, tomatoes and tofu in a pot of malaysian curry broth* 11.05

446. U-Choy (V2) *chinese spinach in oyster sauce or stir-fried in fresh garlic* 11.05

447. Watercress In Foo Yee (V3) *in fermented tofu sauce* 11.05

Seafood Entrées

471. Curry Fish Fillet (E14) *fish fillet with okra, eggplant, tomatoes and pineapple in spicy and sour curry broth. served with steamed rice* 18.75

472. Assam Sambal Squid (E4) *squid stir-fried with pineapple, okra, onion, red pepper, carrot and tomatoes in spicy sambal sauce. served with steamed rice* 16.55

407. Malaysian Chili Scallop (E9) *scallops in chili sauce with garlic and egg white. served with steamed rice* 17.65

473. Mango Shrimp (NE14) *stir-fried shrimp with mango, red and green peppers, onions and carrots in a sweet spicy mango sauce. served with steamed rice* 17.65

419. Steamed Fish Fillet In Sweet Soy Sauce (NE6) *served with steamed rice* 15.45

476. Twin Whole Small Mackerel (E16) *whole mackerel in spicy garlic chef sauce. served with steamed rice* 11.05

499. Crispy Squid In Spicy Salt (E17) *served with steamed rice* 15.45

497. Steamed Tofu With Fish Purée (NE3) *steamed tofu stuffed with fish purée in a special soy sauce. served with steamed rice* 15.45

495. Pickle Mustard Shrimp (NE13) *shrimp stir-fried with pickled shrimp. served with steamed rice* 16.55

400. Assam Sambal Shrimp (E21) *shrimp stir-fried with red onion and red bell pepper in spicy and sour sambal sauce. served with steamed rice* 17.65

408. Malaysian Assam Fish Of The Day (E10) *fish fillet with pineapple and bell pepper in spicy and sour sauce. served with steamed rice* 17.65

406. Malaysian Chili Shrimp (E8) *shrimp in chili sauce, with garlic and egg white. served with steamed rice* 17.65

421. Seafood Tofu Clay Pot (NE8) *scallop, shrimp, fish cake, tofu, straw mushrooms, chinese broccoli, carrot and scallions in chicken broth served with clay pot. served with steamed rice* 15.45

418. Steamed Fish Fillet With Ginger Sauce (NE5) *served with steamed rice* 15.45

414. Golden Shrimp (NE1) *crispy shrimp stir-fried with salty egg yolk on a bed of lettuce. served with steamed rice* 19.85

498. Seafood Omelet (NE2) *shrimp and scallop omelet. served with steamed rice* 17.65

496. Salt Fish & Chicken With Tofu Pot (NE4) *salty fish, chicken and tofu simmered in thick chicken broth. served with steamed rice* 11.05

Combinations

444. Combo Satay Rice (R4) *choice of any 8 skewers of satay served with coconut rice and achar* 15.45

420. Kai Lan Beef (NE7) *chinese broccoli stir-fried with beef. served with steamed rice* 15.45

417. Salt Fish & Chicken With Tofu Pot (NE4) *salty fish, chicken and tofu simmered in a thick chicken broth. served with steamed rice* 11.05

425. Stuffed Lotus Root (NE12) *pan-fried lotus root stuffed with minced chicken and shrimp with scallion and fresh parsley. served with steamed rice* 15.45

Sides

702. Chicken Flavored Rice Side Order 2.30

704. Steamed Rice Side Order 2.25

703. Coconut Flavored Rice Side Order 2.30

Desserts $6.65

604. Mango Rice With Peanuts & Sesame Seed *mango and sweet sticky rice in coconut milk with peanuts and sesame seed*

613. Mango Rice With Malaysian Sweet Crispy Crepe *mango and sweet sticky rice in coconut milk and malaysian sweet crispy crepe*

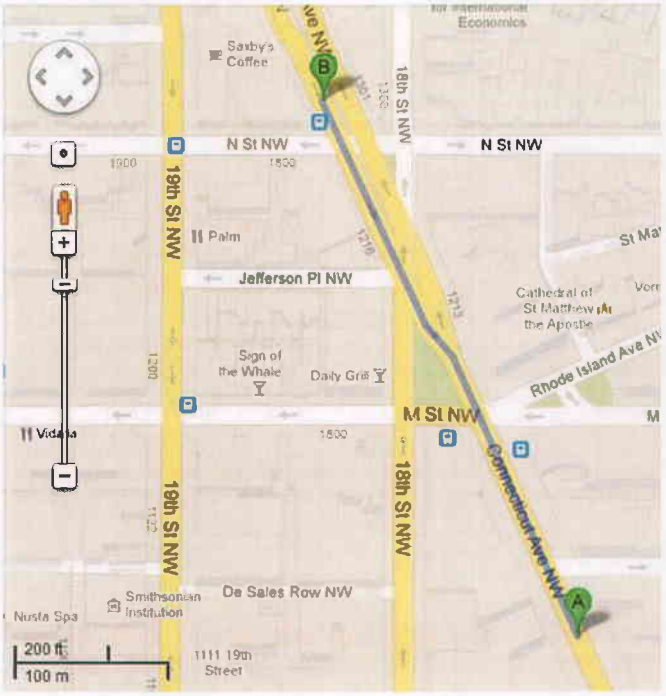
Beverages And Place Settings

Soda *soda choice: pepsi, mountain dew, diet pepsi, sierra mist* 2.25
(6pack) 6.99
Aquafina Water 2.25
Lipton Iced Tea 2.25
Place Setting ea 0.35
6 Pack Of Aquafina Water 12.50
Lipton Lemonade 2.25
Serving Utensils ea 0.75

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

MOBY DICK (HALAL)



1. Head northwest on Connecticut Ave NW from The Mayflower Renaissance toward Desales St NW – 0.2 mi; destination will be on the left, Moby Dick House of Kabob, 1300 Connecticut Ave NW.

Route Time: 5 minutes.

Moby Dick

1300 Connecticut Ave NW
Washington, DC 20036
At N St NW

202 833-9788

YOUR AD HERE
MenuPages **PRIME** Advertising
for more info: www.menupages.com

Appetizers $3.99

Kashk-O Bademjan *a mixture of sautéed eggplant, grilled onion, garlic and boiled yogurt.*
Mast-O Mooseer *yogurt mixed with shallots.*
Hummus *a mixture of mashed chick peas, tahini sauce, lemon juice and fresh garlic.*
Dolmeh *stuffed grape leaves (vegetarian).*

Salads

Garden Salad *lettuce, tomato, onion, cucumber, mushroom served with choice of dressing. (house, italian or ranch).* sm 3.79 lg 4.99
Moby's Salad *lettuce, tomato, cucumber, onion, feta cheese, kalamata olives and pepperoncini served with choice of dressing. (house, italian or ranch).* sm 4.49 lg 6.49
Shirazi Salad *chopped cucumber, tomato, fresh herbs and onion served with house dressing.* lg 2.49
Spinach Salad *fresh baby spinach, sliced hard boiled egg, sliced mushroom and feta cheese with choice of dressing. (house, italian or ranch).* sm 4.49 lg 6.49
Kubideh Salad *grilled ground beef, grated onion with our house seasoning, lettuce, tomato, onion, cucumber, mushroom served with house dressing.* 8.49
Chenjeh Salad *grilled chunks of filet marinated with our house seasoning, lettuce, tomato, onion, cucumber, mushroom served with house dressing.* 10.49
Lamb Salad(Halal) *grilled chunks of lamb marinated with our house seasoning, lettuce, tomato, onion, cucumber, mushroom served with house dressing.* 11.49
Joojeh Salad *grilled chunks of boneless skinless chicken breast marinated with our house seasoning, lettuce, tomato, onion, cucumber, mushroom served with house dressing.* 8.99
Moby's Combo I Salad *combination of one ground beef and one filet.* 11.99
Moby's Combo II Salad *combination of one ground beef and one chicken breast.* 11.49
Moby's Combo III Salad *combination of one ground beef and one lamb.* 12.49
Moby's Super Combo Salad *combination of one chicken breast, and one filet lamb.* 14.49 15.49
Fish Salad *grilled chunks of marinated sword fish, lettuce, tomato, onion, cucumber, mushroom served with house dressing.* 12.49

Sandwiches

Sandwich / Platter***

Moby's Kubideh *ground beef, grated onion with our special house seasoning.* 6.29 7.79
Moby's Chenjeh *chunks of filet marinated in our special house seasoning.* 6.99 8.49
Moby's Barreh (Halal) *chunks of lamb marinated in our special house seasoning.* 7.29 8.79
Moby's Joojeh *chunks of boneless skinless chicken breast marinated in our special house seasoning.* 6.79 8.29
Moby's Gyro *sliced seasoned beef.* 6.29 7.79
Moby's Spicy Ground Chicken Kabob *ground chicken, grated onion with special house seasoning.* 6.29 7.79
Moby's Bone-In Chicken Kabob (Halal) *bone-in chicken marinated in our special house seasoning platter.* 8.99

** All Sandwiches Are Served On Our House Pita Bread With Lettuce, Tomato, Onion, And Feta Cheese With Yogurt Cucumber Sauce On The Side. ** Platters Served With Rice, Small Moby's Salad And Yogurt Sauce On The Side.*

Entrees

Spicy Ground Chicken Kabob *ground chicken, grated onion with special house seasoning.* 7.49 8.49 8.99
Kabob-E Kubideh *ground beef, grated onion with our house seasoning.* 7.49 8.49 8.99
Kabob-E Chenjeh *chunks of filt marinated in our special house seasoning.* 9.49 10.49 10.99
Kabob-E Barreh(Halal) *chunks of lamb marinated in our special house seasoning.* 10.49 10.49 11.99
Kabob-E Joojeh *chunks of boneless skinless chicken breast marinated in our special house seasoning.* 7.79 8.99 9.49
Moby's Combo I *combination of one ground beef and one filet.* 10.99 11.99 12.49
Moby's Combo II *combination of one ground beef and one chicken breast.* 10.49 11.49 11.99
Moby's Combo III *combination of one ground beef and one lamb.* 11.49 12.49 12.99
Moby's Super Combo *combination of one chicken breast, one filet.* 13.49 14.49 14.99
Moby's Super Combo Lamb 14.49 15.49 15.99
Fish Kabob *chunks of boneless sword fish marinated in our special house seasoning.* 11.49 12.49 12.99

Veggies

Moby's Veggie (Platter) *sautéed fresh mushrooms, onion, tomato, and spinach served on a bed of basmati rice.* 8.49
Platter Cold Veggie Delight (Sandwich) *fresh avocado, provolone cheese, mushrooms, tomato, spinach, and mayo served on fresh pita bread.* 8.49
Hot Moby's Melt (Sandwich) *combination of melted provolone and american cheese on top of fresh mushrooms, onion, tomato, and spinach served on fresh pita bread.* 6.29
Falafel *vegetable patties made with chick peas, fava beans, parsley, onions, cilantro, garlic, sesame seed, sea salt fried in vegetable oil, served with tahini sauce.*
sandwich 6.29
platter 7.79

Vegetarian Platters Served With 1/2 A Pita Bread and A Side Of Yogurt.

Side Orders

Sm /Lg

Mast-O Kheyar *yogurt mixed with chopped cucumber and fresh herbs* 1.19 2.19
Seer Torshi *marinated garlic in vinegar and spices* 2.49 3.49
Torshi *mixture of diced vegetables marinated in vinegar and spices* 2.49 3.49
Fresh Whole Pita Bread lg 1.75
Plain Rice 2.49 3.99
Char-Grilled Tomatoes 1.19 2.49
Char-Grilled Onions 1.19 2.49
Kalamata Olive 1.19 2.49
Pepperoncini 1.19 2.19
Feta Cheese 1.49 2.49
Fresh Onion 1.19 2.19
Kubideh Kabob lg 2.99
Chenjeh Kabob lg 6.99
Lamb Kabob(Halal) lg 7.79
Joojeh Kabob lg 5.49
Spicy Ground Chicken Kabob lg 2.99
Bone-In Chicken Kabob(Halal) lg 5.99
Fish Kabob lg 8.

Lunch Specials

Lubya Polo (Monday) *steamed basmati rice mixed with green beans, a medley of beef, onion, and tomato base sauce, and exotic spice including cinnamon.* 7.99
Baghaala Polo (Tuesday) (Halal) *steamed basmati rice, fava beans and fresh dill weed, served with baked chicken.* 7.99
with lamb shank. 8.99
Khoresht Gheymeh Bademjan (Wednesday) *sautéed slices of eggplant, yellow peas, chunks of beef, onion and tomato sauce with exotic spices braised to perfection and served with steamed basmati rice.* 7.99
Zereshk Polo (Thursday)(Halal) *sautéed barberry (currents), shredded tangerine peel, sugar and saffron served on steamed basmati rice and beaded with baked chicken.* 7.90
Ghormeh Sabzi (Friday) *sautéed chunks of beef, fresh cilantro, parsley, leeks and exotic spices braised to perfection and served with steamed basmati rice.* 7.99

Desserts

Baklava Homemade

Baklava 3.79
Bamiyah 3.79
Rolette 1.99

Beverages

Bottled Doogh

Homemade Doogh 1.99
Bottled Doogh 2.49
Sodas 1.79
Juices 1.89
Spring Water 1.59
Persian Brewed Hot Tea 1.29

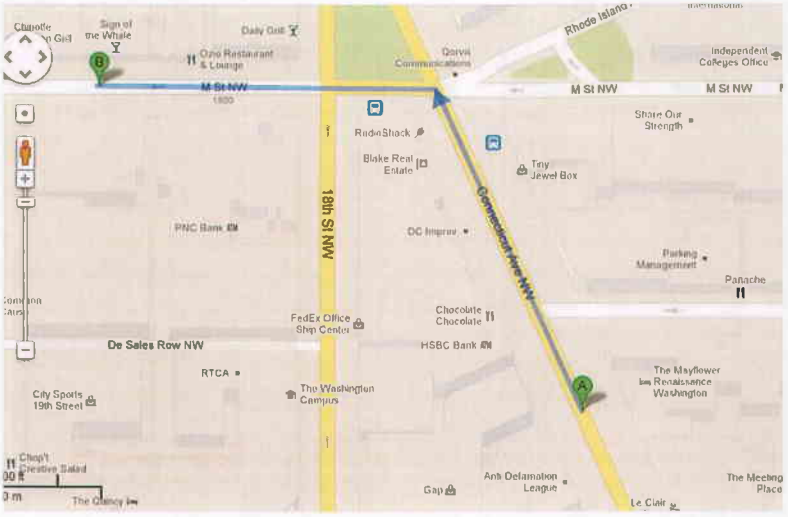
Family Platters

Platter # 1 *3 skewers ground beef, 1 skewer chicken breast, 1 skewer beef filet or lamb with choice of two appetizers or desserts* (serves 3 to 4) 32.99
Platter # 2 *4 skewers ground beef, 2 skewers chicken breast, 2 skewers beef filet or lamb with choice of three appetizers or desserts* (serves 5 to 7) 54.

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

HOUSE OF KABOB (HALAL)



1. Head northwest on Connecticut Ave NW from The Mayflower Renaissance toward Desales St NW – 0.1 mi.
2. Turn left onto M St NW – 495 ft; destination will be on the right, House of Kabob, 1829 M St NW #100.

Route Time: 4 minutes.

HOUSE OF KABOB

Appetizers

All Served With Pita Bread, Unless Otherwise Noted

Hummus $4.95

pureed chick pea with tahini, lemon juice and olive oil

Baba-ghanouj **$4.95**

zesty eggplant dip with tahini, garlic, lemon juice and olive oil.

Lebnee **$4.95**

lebanese cream yogurt, sprinkled with olive oil and mint.

Persian Egg Plant **$4.95**

oven roasted eggplant, blended with tomatoes, garlic and eggs.

Fool Mudammas **$4.95**

fava beans marinated with garlic, lemon juice herbs topped with olive oil.

Falafel **$4.95**

fried patties of chick peas mixed with coriander and other spices, served with tahini sauce

Dolmas/grape Leaves **$4.95**

tender grape leaves, rice, scallion, tomato parsley and, spices.

Ara-yes **$4.95**

a ground lean mixture of beef and lamb, onion, parsley, tomatoes, blanketed between pita bread and grilled to crisp.

Lebanese Kibbeh **$6.95**

freshly ground sirloin mixed with cracked wheat and special spices stuffed with onion and beef tips.

Beef Sambosek **$4.95**

tender beef mixed with onion simmered in palmegrant sauce wrapped in crispy roll

Cheese Sambosek **$4.95**

chunks of feta cheese mixed with onion, and, bell pepper blended with mint and olive oil wrapped in a crispy roll.

Spanakopita **$5.95**

traditional greek spinach with feta cheese pie

$6.95

Lebanese Chicken Wings

toseed in lebanese garlic sauce or original hot sauce

Soups

$4.95

Lamb Tongue

lamb tongue, simmered in saffron served with pita bread.

$2.95

Lintel Soup

lintel, onion, cilantro, and cumin.

$3.95

Chicken Farmers Soup

chicken, simmered with onion, tomato, potatoes, and rice topped with cilantro.

Salads

$3.95

Persian Salad

diced tomatoes, cucumbers, onions, with lemon juice and olive oil.

$5.95

Topped With Chicken Or Gyros **$4.00**

Greek Salad

feta cheese, dolmas, tomatoes, lettuce, onion, kalamata olives, bellpepper, peperchini pepper, cucumber, sprinkled with mint and oliveoil.

$4.95

Topped With Chicken**$4.00**

Fettoush Salad

an original lebanese delicacy, fresh tomatoes, cucumbers, onions, bell pepper, and fresh parsley in a dressing of lemon juice and olive oil, tossed with seasoned pita bread croutons.

$4.95

Topped With Chicken**$6.00**

Tabbouleh Salad

finely minced fresh parsley, cracked wheat, onion, diced tomatoes, blended with mint, lemon juice, and olive oil.

Sauces & Side Orders

Full **$3.50**

Small **$0.50**

Yogurt With Cucumber

Full **$3.50**

Small **$0.50**

Creamy Garlic Sauce

Tazeyke Dip — Full **$3.50** / Small **$0.50**

French Fries — **$2.50**

Basmati Rice — **$2.50**

Pita Bread — **$1.00**

Entrees - Beef

All Served With Basmati Rice, And Salad Unless Otherwise Noted

Kobeideh — **$11.95**

two skewers of ground lean mixture of beef lamb, onion, and fresh tomato.

Special Soltani — **$18.95**

a skewer of filet mignon and one skewer of kobeideh

Special Barg Supreme — **$15.95**

a skewer of filet mignon.

Beef Shish Kabob — **$11.95**

two skewers of tender marinated beef, tomato, bell peppers, and onions.

Lebanese Beef Shish Kabob — **$13.95** / Add Rice **$2.50**

two skewers of tender marinated beef served with hummus, and tabouleh.

Ghorme Sabzi — **$11.95**

pieces of beef cooked in chopped green onions, leeks, parsley, spinach, dried lime, kidney beans and our own spices.

Ghaime Bamia (stew) — **$11.95**

pieces of beef cooked in split peas and dried lime, okra mixed with our own blend of spices.

Mousaka — **$11.95**

a casserole layered with eggplant, potatoes, cheese and creamy parmesan custard sauce. topped with light tomato sauce.

Beef Shawarma — **$11.95**

tasty strips of beef marinated olive oil and lebanese spices, cut into thin slices served with creamy garlic sauce

Entrees - Lamb

$14.95

Lamb Shish Kabob

two skewers of marinated leg of lamb, tomatoes, bell peppers, and onions.

$16.95

Add Rice **$2.50**

Lebanese Lamb Shish Kabob

two skewers of marinated leg of lamb served with hummus, and tabbouleh.

$16.95

Lamb Chops

traditional grilled tender pieces of spring lamb chops.

$14.95

Lamb Shanks

whole lamb shank cooked in garlic sauce served over saffron rice b) whole lamb shank cooked in ghorme sabzie sauce.

$11.95

Abgosht (stew)

a savory mix of oven baked lamb with tomatoes, potatoes, navy beans, chick peas.

$11.95

Gyros

slices of gyros (spicy greek mixture of beef and lamb) served with greek salad.

Entrees - Lamb

All Served With Basmati Rice, And Salad Unless Otherwise Noted

$15.95

Lamb Curry

lamb, tomatoes, bell peppers, and onions sauteed in curry sauce.

Chicken

$12.95

Chicken Shawarma

tasty strips of chicken marinated olive oil garlic and lebanese spices, cut into thin slices served with creamy garlic sauce.

$12.95

Shish-taok

seasoned chicken breast sautéed with onion, bell pepper and tomatoes.

$11.95

Chicken Shish Kabob

two skewers of charcoal broiled chicken, tomato, bell peppers and onions.

$13.95

Add Rice **$2.50**

Lebanese Chicken Shish Kabob

two skewers of charcoal broiled chicken served with hummus and tabouleh.

Fesenjan (stew) **$11.95**

pieces of chicken cooked with walnuts and pomegranate sauce.

Roasted Chicken **$12.95**

½ chicken oven roasted to perfection atop mount of french fries or basmati rice served with a side of our creamy garlic sauce

Chicken Curry **$13.95**

chicken, tomatoes, bell peppers and onions sauteed in curry sauce

Combination

Sultan Combo **$14.95**

Lamb Add **$2.00**

four pieces of beef, chicken, falafel, hummus, baba ghanouj, tabbouleh, stuffed grape leaves.

Any (2) Shish Kabob **$12.95**

Lamb Skewer **$2.00**

beef or chicken

Any (2) Lebanese Kabob **$14.95**

Add Lamb Skewer **$2.00**

beef or chicken

Any (3) Shish Kabob **$16.95**

Add Lamb Skewer **$2.00**

beef or chicken

Any (3) Lebanese Kabob **$18.95**

Add Lamb Skewer **$2.00**

Add Rice **$2.50**

beef or chicken

Sea Food

Shrimp Scampi **$14.95**

sautéed shrimp in fresh tomatoes, and onions in a buttery garlic cream sauce.

Fillet Of Fish **$16.95**

fish fillet prepared lebanese-style, with fresh tomatoes, bell peppers, and onions in a spicy tahini sauce.

Vegetarian

Char Broiled Veggies — $9.95

two skewers of char broiled tomato, bell pepper, and onions

Vegetarian Combo Plate — **$11.95**

falafel, hummus, eggplant, tabbouleh, stuffed grape leaves

Lebanese Delight — **$10.95**

a delightful combination of falafel, hummus, and fettoush

Sandwiches

Add French Fries To Any Sandwich $ 1

Hummus — **$3.95**

Baba Ghanouj — **$3.95**

Shawarma Chicken, Or Beef — **$4.95**

Falafel With Hummus — **$4.95**

Kobeideh Kabob — **$4.95**

Chicken Kabob — **$4.95**

Gyros — **$4.95**

Lamb Kabob — **$6.95**

Beef Kabob — **$4.95**

Desserts

Baklava, Kenafa, Or Katifa — **$2.50**

Kenafa — **$2.50**

Katifa — **$2.50**

KABABJI GRILL (HALAL)

1. Head northwest on Connecticut Ave NW from The Mayflower Renaissance toward Desales St NW – 0.3 mi; destination will be on the right: Kababji Grill, 1351 Connecticut Ave NW.

Route Time: 7 minutes.

Kababji Grill
1351 Connecticut Ave NW
Washington, DC 20036
Btwn Dupont Cir & N St NW

202 822-8999
Fax: 202 822-9888

YOUR AD HERE
MenuPages ***PRIME*** Advertising
for more info: www.menupages.com

Delivery & Take Out - Lunch

Available Monday-Friday Until 2:30pm & Saturday & Sunday Until 4pm.

Mezza

Appetizers.

Shorbit Al Addas (V) *lentil soup. orange lentils, sautéed onions, rice, simmered in vegetable broth with spices, served with pita chips.....* 6.50

Baba Ghannouj *fresh roasted eggplant lightly mashed with tahini, lemon juice and a dash of garlic. topped with extra-virgin olive oil..*(half order) 3.50
.....(full order) 6.50

Kebbeh Mikleyeh *fried beef kebbeh. beef and cracked wheat, fresh mint and basil, blended and stuffed with sautéed ground beef, onion and pine nuts.....* 7.00

Labneh (V) *yogurt cream. house-made strained yogurt cream spread, topped with extra-virgin olive oil.....*(half order) 3.50
.....(full order) 6.50

Hummus *a spread prepared with chickpeas, tahini, lemon juice and a hint of garlic topped with extra virgin olive oil.....*(half order) 3.50
.....(full order) 6.50

Warak Enab (V) *stuffed grape leaves. hand-rolled and stuffed grape leaves flavored with pomegranate sauce, herbs and spices.....* 7.00

Rkakat Jibneh *fried cheese balls. cheese rolls prepared with white cheddar and mozzarella cheeses in parsley, mint and onions, rolled in a phyllo pastry.....* 7.00

Khyar Bi Laban (V) *cucumber yogurt. yogurt and diced cucumber mixed with dried mint....*(half order) 3.50
.....(full order) 6.50

Salad

Half Order $3.50 / Full Order $6.50.

Tabouleh Salad (V) *fresh cut parsley, tomatoes, tossed with cracked wheat, diced onions, lemon juice, extra virgin olive oil, & sumac.....*

Salata Libaneyeh (V) *lebanese salad. romaine lettuce, tomato, cucumbers, parsley, onion, lemon juice, extra virgin olive oil.....*

Fattouch Salad *garden greens and pita chips. medley of mixed greens, fresh mint, arugula, tomato and cucumber dressed with lemon juice, garlic, sumac and pomegranate. topped with roasted pita chips.....*

Salatet Kababji (V) *kababji signature salad. diced tomatoes & cucumber, dry mint, lemon juice, & a hint of balsamic vinegar.....*

Lebanese Pita Sandwich Platters

Choose Your Sandwich With Fries Or With Lentil Soup And Lebanese Salad.

Laham Mishwe Sandwich *juicy tenderloin wrapped with hummus, grilled onions & pickles.....* 10.95

Halabi Kabab Sandwich *seasoned ground lamb wrapped with parsley, hummus and pickles.* 9.95

Feter Kabab Sandwich (V) *grilled marinated portobello mushrooms wrapped with lettuce, tomato, garlic paste and pickles.....* 9.95

Labneh Sandwich *yogurt cream wrapped with cucumber, black olives, tomato and fresh mint.....* 7.95

Shish Taouk Sandwich *halal. marinated chicken breast wrapped with pickles and garlic.....* 9.95

Kafta Kabab Sandwich *seasoned ground beef wrapped with parsley, hummus and pickles.* 9.95

Hummus Sandwich (V) *hummus wrapped with tomato and pickles.....* 7.95

Kabab Platters

All Entrées Served With Grilled Vegetables, Rice, & Seasoned Lebanese Br

Mixed Grill *serves one. halabi lamb, laham mishwe (filet) and chicken shish taouk, served with signature house garlic spread.....* 20.00

Kafta Kabab *beef kabab. perfect balance of ground beef, kneaded with a house-blend of spices and chopped parsley.....* 13.50

Kabab Khodra (V) *vegetable kabab. garden vegetables brushed with extra virgin olive oil & served with garlic pita.....* 12.00

Halabi Kabab *lamb kabab. prefect balance of ground lean lamb, kneaded with a house-blend of spices & chopped parsley.....* 14.00

Shish Taouk *halal. chicken cubes. grilled skinless chicken breast cubes marinated in garlic, tomato, lemon and a blend of spices.....* 14.00

Laham Mishwe Kabab *beef tenderloin kabab. cubes of marinated beef tenderloin paired with vidalia onions.....* 16.00

Desserts $7

Namoura *a traditional lebanese cake made from semolina, rose-water syrup and topped with an almond.....*

Finger Baklava *3 pieces. layers of phyllo dough rolled with ground nuts and sweetened with honey.....*

Baklava *layers of phyllo dough filled with ground nuts and sweetened with honey.....*

Mixed Sweets *3 pieces. trio of namoura, baklava and finger baklava.....*

Beverages

Soda..... 1.75
Bottled Water..... 1.75
Mint Lemonade..... 1.75
6-Pack Soda..... 8.00
6-Pack Of Bottled Water..... 8.00

Delivery & Take Out - Dinner

Available Monday-Friday At 5pm-Close & Saturday & Sunday At 4pm-Close.

Cold Mezza

Appetizers.

Kebbeh Nayeh *raw item. lebanese steak tartar-lebanon `s national dish. a blend of refined lean beef and cracked wheat served in two different styles. northern kebbeh with mint, onion and basil and southern kebbeh (spicy) with mint, onion, parsley, hot pepper, spicy house blend sauce.....*
kebbeh nayeh choice: northern kebbeh..... 14.00
kebbeh nayeh choice : southern kebbeh - spicy..... 15.00

Baba Ghannouj *fresh roasted eggplant lightly mashed with tahini, lemon juice and a dash of garlic. topped with extra-virgin olive oil..*(half order) 3.50
.....(full order) 6.50

Warak Enab (V) *stuffed grape leaves. hand-rolled and stuffed grape leaves flavored with pomegranate sauce, herbs and spices.....* 7.00

Salatit Batinjan *vegetarian eggplant salad. fresh roasted eggplant, peeled and chilled, topped with extra virgin olive oil, sea salt, oregano and diced roma tomato.....* 6.50

Khyar Bi Laban (V) *cucumber yogurt. yogurt and diced cucumber mixed with dried mint....*(half order) 3.50
.....(full order) 7.50

Hummus *a spread prepared with chickpeas, tahini, lemon juice and a hint of garlic topped with extra virgin olive oil.....*(half order) 3.50
.....(full order) 6.50

Salatit Al Raheb (V) *monk salad. roasted eggplant with roma tomato, bell pepper, onions and garlic, tossed with lemon juice, parsley and extra-virgin olive oil.....*(half order) 3.50
.....(full order) 6.50

Labneh (V) *yogurt cream. house-made strained yogurt cream spread, topped with extra-virgin olive oil.....*(half order) 3.50
.....(full order) 6.00

Sahan Khodra (V) *assorted vegetable plate. fresh radishes, tomato slices and mint leaves, pickled cucumber and chili peppers with imported lebanese olives.....* 5.00

MP

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

YOUR AD HERE
MenuPages ***PRIME*** Advertising
for more info: www.menupages.com

Hot Mezza

Appetizers.

Kebbeh Mikleyeh *fried beef kebbeh. beef and cracked wheat, fresh mint and basil, blended and stuffed with sautéed ground beef, onion and pine nuts.* 7.00

Rkakat Jibneh *fried cheese balls. cheese rolls prepared with white cheddar and mozzarella cheeses in parsley, mint and onions, rolled in a phyllo pastry.* 7.00

Fattet Hummus *chickpeas with yogurt. whole chick peas mixed with yogurt and garlic and topped with pine nuts.* (half order) 3.50 (full order) 6.50

Kebbeh Laktin (V) *pumpkin kebbeh. baked pumpkin and cracked wheat stuffed with swiss chard, chick peas, sumac and onion.* 7.00

Foul Moudammas (V) *fava bean salad. fava beans simmered with fresh garlic, tomato, onion, parsley and lemon juice.* (half order) 3.50 (full order) 6.50

Balila (V) *spiced chickpeas. whole chickpeas slowly boiled and seasoned with a hint of cumin and garlic. topped with imported extra-virgin olive oil.* (half order) 3.50 (full order) 6.50

Soup

Shorbit Al Addas (V) *lentil soup. orange lentils, sautéed onions, rice, simmered in vegetable broth with spices, served with pita chips.* 6.50

Salads

Salatet Kababji *vegetarian. kababji signature salad. diced tomatoes & cucumber, dry mint, lemon juice, & a hint of balsamic vinegar.* (half mezze portion) 3.50 (mezze portion) 6.50 (large portion) 11.00

Tabouleh Salad *vegetarian. fresh cut parsley, tomatoes, tossed with cracked wheat, diced onions, lemon juice, extra virgin olive oil, & sumac.* (half order) 3.50 (full order) 6.50

Salatet Shish Kabab *steak and potato salad. grilled seasoned tenderloin cubes served over baked potatoes and onions tossed with extra-virgin olive oil.* 13.50

Salata Libaneyeh *vegetarian. lebanese salad. romaine lettuce, tomato, cucumbers, parsley, onion, lemon juice, extra virgin olive oil.* (half mezze portion) 3.50 (mezze portion) 6.50 (large portion) 11.00

Fattouch Salad *garden greens and pita chips. medley of mixed greens, fresh mint, arugula, tomato and cucumber dressed with lemon juice, garlic, sumac and pomegranate. topped with roasted pita chips.* (half mezze portion) 3.50 (mezze portion) 6.50 (large portion) 11.00

Salatet Shish Taouk *halal. grilled chicken salad. chicken breast cubes, grilled over charcoal with kababji seasoning on a bed mixed greens, tomato and cucumber tossed with extra-virgin olive oil.* 13.00

Lebanese Pita Sandwich Platters

Choose Your Sandwich With Fries Or With Lentil Soup And Lebanese Salad.

Laham Mishwe Sandwich *juicy tenderloin wrapped with hummus, grilled onions & pickles.* 10.95

Halabi Kabab Sandwich *seasoned ground lamb wrapped with parsley, hummus and pickles.* 9.95

Intabli Kabab Sandwich *spicy. ground beef seasoned with spices, peppers, parsley and mild pepper paste, wrapped with hummus and pickles.* 9.95

Kebbeh Meshwiyeh Sandwich *seasoned mixture of ground beef, roasted pine nuts, pistachios and cracked wheat wrapped with hummus, tomato, sumac and pickles.* 9.95

Hummus Sandwich (V) *hummus wrapped with tomato and pickles.* 7.95

Shish Taouk Sandwich *halal. marinated chicken breast wrapped with pickles and garlic.* 9.95

Kafta Kabab Sandwich *seasoned ground beef wrapped with parsley, hummus and pickles.* 9.95

Dejaj Kabab Sandwich *halal. spiced ground chicken breast wrapped with garlic spread and pickles.* 9.95

Feter Kabab Sandwich (V) *grilled marinated portobello mushrooms wrapped with lettuce, tomato, garlic paste and pickles.* 9.95

Labneh Sandwich *yogurt cream wrapped with cucumber, black olives, tomato and fresh mint.* 7.95

Main Courses - Signature Kabab

Halabi Kabab *lamb kabab. prefect balance of ground lean lamb, kneaded with a house-blend of spices & chopped parsley.* 16.00

Dejaj Kabab *halal. chicken kabab. ground chicken breast mixed with a light blend of spices & grilled.* 16.00

Laham Mishwe Kabab *beef tenderloin kabab. cubes of marinated beef tenderloin paired with vidalia onions.* 22.00

Frangali Kabab *beef & mushroom kabab. seasoned refined beef combined with tomato wedges and portobello mushrooms.* 16.00

Kabab Festok *pistachio kabab. seasoned refined beef mixed with imported pistachios.* 18.00

Orfali Kabab *beef and vegetable kabab. refined lean beef paired with fresh tomato, eggplant cubes, onions, & green chili pepper.* 17.00

Kafta Kabab *beef kabab. perfect balance of ground beef, kneaded with a house-blend of spices and chopped parsley.* 15.00

Shish Taouk *halal. chicken cubes. grilled skinless chicken breast cubes marinated in garlic, tomato, lemon and a blend of spices.* 16.00

Kabab Khodra (V) *vegetable kabab. garden vegetables brushed with extra virgin olive oil & served with garlic pita.* 12.00

Intabli Kabab *spicy kabab. beef seasoned with house-blend spices, fresh peppers, chopped parsley and mild pepper paste.* 16.00

Kebbeh Meshwiyeh *grilled kebbeh. seasoned ground beef chuck with roasted pine nuts, pistachios, & cracked wheat, grilled & served with cucumber yogurt salad.* 18.00

Main Course - From The Grill

Arayes *meat stuffed pita. pita pocket grilled on charcoal and stuffed with ground beef, parsley, fresh tomato sauce, hot pepper paste, pine nuts, and kababji seasoning.* 8.00

Kababji Signature Grill *serves 2. laham, mishwe, shish taouk, frangali kabab, dejaj kabab, halabi kabab and kafta kabab served with pita bread and parsley onion mix. includes orfali kabab.* 42.00

Mixed Grill *serves 1. halabi, laham mishwe and shish taouk with vegetables and garlic spread.* 20.00

Desserts $7

Namoura *a traditional lebanese cake made from semolina, rose-water syrup and topped with an almond.*

Finger Baklava *3 pieces. layers of phyllo dough rolled with ground nuts and sweetened with honey.*

Baklava *layers of phyllo dough filled with ground nuts and sweetened with honey.*

Mixed Sweets *3 pieces. trio of namoura, baklava and finger baklava.*

Beverages

Soda *soda choice: coke, diet coke, sprite* 1.75

Bottled Water 1.75

Mint Lemonade 1.75

6-Pack Soda *soda choice: coke, diet coke, sprite* 8.00

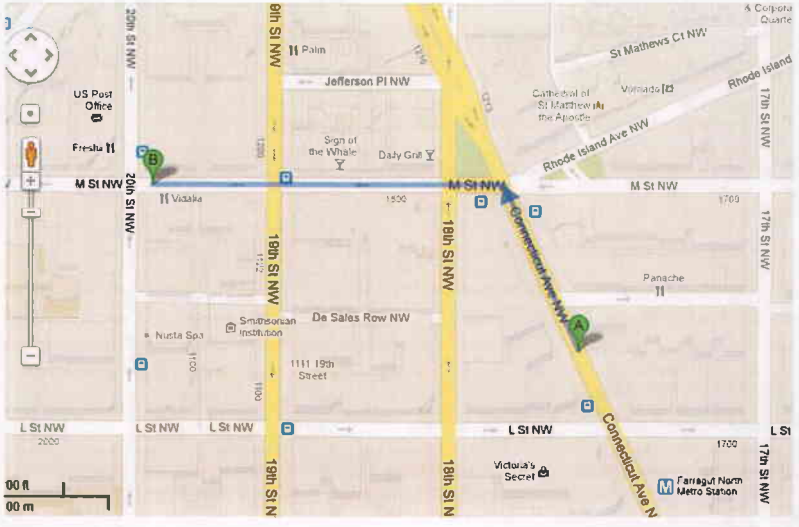
6-Pack Of Bottled Water 8.00

(V) Vegetarian.

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

COUSCOUS CAFÉ (HALAL)



1. Head northwest on Connecticut Ave NW from The Mayflower Renaissance toward Desales St NW – 0.1 mi.
2. Turn left onto M St NW – 0.2 mi; destination will be on the left: Couscous Café, 1990 M St NW.

Route Time: 4 minutes.

Couscous Cafe
1195 20th St NW
Washington, DC 20036-3404
At M St NW

202 689-1233

YOUR AD HERE
MenuPages **PRIME** Advertising
for more info: www.menupages.com

Sunshine Breakfast

Bagel Cream Cheese 2.99
Plain Omelet On Toasted Bagel 3.99
Cheese & Bacon Omelet *served on croissant or house bread* 3.99
Lamb Sausage Omelet *tucked in pita bread* 4.99
Crepes (2) A La Francaise *with orange marmalade or chocolate sauce* 4.99
1 Crepe *with chocolate or chocolate & banana or strawberry preserves* 2.99
with chocolate 2.49

Bakery

Plain Croissant Or Lowfat Muffins 1.69
Low Fat Muffins 1.69
Danish Or Pain Raisin 1.59
Biscotti 1.29
Homemade Cookies 1.00
Brownies 1.69
Kalb Elloouz 1.99

Lunch

Soups

Cup / Bowl

Lentil Soup *with beef & carrots* 3.99 4.99
Tomato Soup Andalusia *lamb cubes, crushed wheat, chick peas, celery, cilantro and mint* 3.99 4.99
Soup Of The Day 2.99 3.99

Entrée Salads

Seasonal Fresh Fruit Salad 2.99
Caesar Salad 4.99
Chicken Caesar Salad *chicken breast cubes romaine lettuce, parmesan* 6.99
Mixed Green Salad *tomatoes, carrots, shallots, dijon vinaigrette* 4.99

Sandwiches

With Soda

Chicken Caesar Salad Wrap 5.99
Tuna Salad *celery, carrots, dill cream cheese, dill, capers, shallots on wheat bread* 5.99
Hummus Sandwich *tucked in pita bread served with tomato, cucumber, lettuce* 4.99

Sandwich Platters $6.99

Served With Salad

Paillard Sandwich *grilled thin steak, lettuce, mustard on baguette*
Merguez Sandwich *spicy lamb sausage with harissa sauce on baguette*

Side Dishes

Hummus *with pita bread* 3.19
Tabouleh 3.19
Baba Ghannouj 3.19
Ratatouille 3.19
Cucumber And Tomato Salad 3.19
Beets Salad 3.19
Lentil Salad 2.99
Gourmet Carrots Salad 3.19
Vegetarian Grape Leaves 2.99
Couscous Salad 3.99
Tzatziki 3.19

Vegetarian Entrees

Vegetarian Couscous *stew of zucchini, chick peas, carrots, butternut squash and turnips* 6.99
Kemya Platter *ratatouille, hummus, baba ghannouj, grape leaves, tabouleh* 7.99
Falafel Patter *falafel cakes wrapped in pita with parsley, turnips, served with salad* 5.99

Entrees

Couscous A La Royal *with merguez, chicken and lamb & vegetables* 10.99
Couscous With Lamb *stew of zucchini, chick peas, carrots, butternut squash and turnips* 8.99
Couscous With Chicken (Dark Meat) *stew of zucchini, chick peas, carrots, butternut squash and turnips* 7.99
Couscous With Chicken (White Meat) *stew of zucchini, chick peas, carrots, butternut squash and turnips* 8.99
Chicken Kabob *served with basmati rice* 6.99
Broiled Salmon Glazed With Pesto *served ratatouille with basmati rice or couscous* 8.99
Brochette Of Lamb *broiled lamb cubes with green peppers and tomatoes on rice* 8.99
Golden Saffron Chicken Tajine *with green olives served on basmati rice* 6.9
Chicken B'Stilla Pie *roasted chicken, spices, sweet almonds paste, rolled in phyllo* 8.99

Desserts

Apple Strudel 2.99
Crème Brulee 3.99
Baklawa 1.59
Makroud 1.59

Drinks

Soft Drinks Or Lemonade 1.29
Snapple 1.89
Can Sodas 1.10
Freshly Squeezed O.J. Standard Size 2.00
Perrier Or Evian Water 1.89
Orangina 1.89
An Assortment Of Teas Available 1.10
Authentic North African Green Tea *with fresh mint* 1.89

Coffees And Chocolate

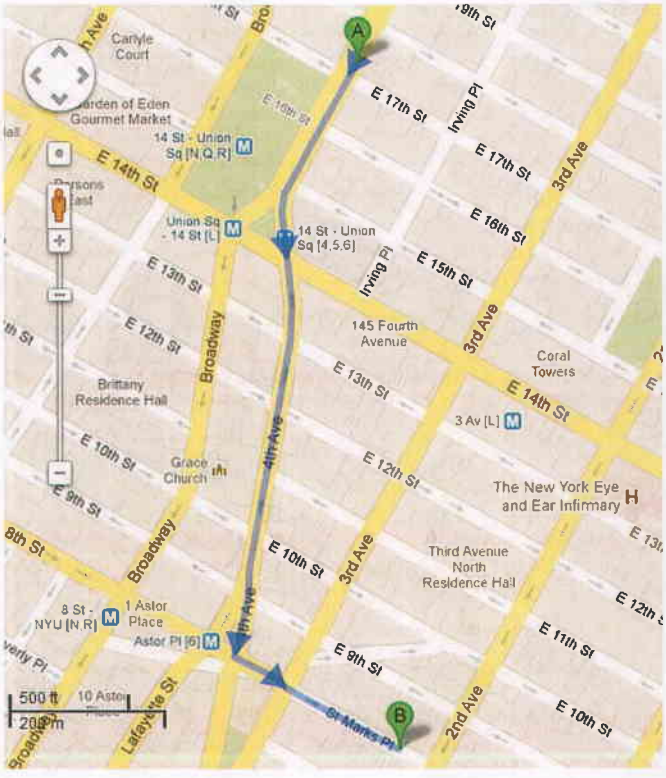
Coffee *french toast, arabica beans* 1.59
Turkish Coffee 2.99
Expresso sgl 1.95 dbl 2.39
Cappuccino sgl 2.39 dbl 2.99
House Latte sgl 2.39 dbl 2.99
Café Mocha sgl 2.39 dbl 3.19
Our Signature Hot Chocolate *melted belgium chocolate ganache, topped with whipped cream* sgl 2.39 dbl 3.19
Café Viennois sgl 2.39 dbl 3.

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

New York

KHYBER PASS (HALAL)



1. Head southwest on Park Ave S from W Union Square toward E 17th St – 62 ft.
2. Continue onto Union Square E – 0.2 mi.
3. Continue onto 4th Ave – 0.3 mi.
4. Turn left onto Astor Pl – 253 ft.
5. Continue onto St Marks Pl – 0.1 mi; destination will be on the right: Khyber Pass, 34 St Marks Pl

Route Time: 13 minutes

Khyber Pass
34 St Mark's Pl
New York, NY 10003-8035
Btwn 2nd & 3rd Ave

212 473-0989
Fax: 212 473-2451

YOUR AD HERE
MenuPages ***PRIME*** Advertising
for more info: www.menupages.com

Appetizers

Ashak *steamed scallion dumpling with yogurt-mint sauce; with or without meat (ground beef)* 5.50
Badenjan Bouranee *sautéed eggplant slices topped with yogurt-mint sauce; with or without meat (ground beef)* 5.50
Boulanee Kadu *turnover filled with pumpkin; with yogurt dip* 4.95
Sambosa *crispy deep-fried dumpling stuffed with beef, split peas and spices; with yogurt dip* 4.95
Fesenjan *sweet and sour tender pieces of boneless chicken flavored with walnuts and pomegranate juice* 5.50
Mantoo *steamed dumpling filled with beef, onion and spices; topped with yogurt, and meat sauce* 5.50
Boulanee *turnover filled with scallion; with yogurt dip* 4.95
Boulanee Kachaloo *turnover filled with potatoes, herbs and spices, with yogurt dip* 4.95
Combo Turnover *sambosa, boulanee kadu, and boulanee kachaloo* 12.50
Humus *chick peas spread topped with olive oil and spices* 5.00

Soups

Ashe Soup *traditional vegetable soup with homemade noodles, yogurt; with or without meat (ground beef)* 3.50

Salads

Herb Salad *chopped fresh lettuce, tomatoes, and cucumbers; topped with fresh herbs* 5.95
Panir Sabzee Salad *fresh mint, watercress, basil leaves, scallions, radishes, feta cheese* 4.95
Masto Khiar Salad *homemade yogurt with chopped cucumbers and mint* 5.00
Greek Salad *chopped fresh lettuce, tomatoes, and cucumbers, green pepper, olives, and feta cheese; with oil-vinegar* 6.95
Salad Shirazee Salad *sliced cucumbers, tomatoes, scallion and mint leaves, with lemon juice and olives oil dressing* 4.95

Kabobs

Charcoal Grilled On Skewers And Served With Choice Of Rice

Barg *tender pieces of fillet mignon, marinated with saffron and other spices, served with choice of rice and grilled tomatoes* 13.95
Kabab-E-Sultani *one skewer of barg and one skewer of koobideh; served with white basmati rice and grilled tomatoes* 16.95
Joojeh *marinated cornish game hen; served with choice of rice and grilled tomatoes* 12.95
Choopan (Shepherd's Kabab) *lamb chops marinated with fresh herbs; served with rice and grilled tomatoes* 14.95
Chicken Adana *grounded chicken marinated with garlic onion herbs and spices served with rice and grill tomato* 13.95
Koobideh *mildly spiced patties of minced lean beef; served with choice of rice and grilled tomatoes* 11.95
Morgh *tender pieces of boneless chicken, marinated in garlic, onions and spices; served with choice of rice and grilled tomatoes* 12.95
Shish Kabab (Bara) *chunks of boneless lamb, marinated in onions, garlic and spices; served with rice, grilled tomatoes and onions* 12.95
Combination Kabab *1/2 skewer of barg, koobideh and morgh; served with rice and house salad (lettuce, tomatoes and cucumber)* 20.00

Vegetarian Dishes

Kabuli Palow *browned basmati rice topped with raisins, slivered carrots and almonds. served with a choice of spinach, eggplant, pumpkin or red kidney beans* 11.50
Quorma Badenjan *eggplant sautéed with onion, tomatoes and green pepper; served with browned basmati rice* 10.50
Sabze Chalow *spicy sautéed chopped spinach, and scallions, served with white rice* 10.50
Quorma Kadu *pumpkin sautéed with onions, tomatoes and spices; served with white basmati rice* 10.50
Kachaloo Chalow *potatoes sautéed with onion, tomatoes and spices; served with white rice* 10.50
Shireen Palow *exotic rice dish cooked with orange peels, saffron, almonds and pistachios; served with a choice of spinach, eggplant, pumpkin or red kidney beans* 11.50
Bouranee Badenjan *eggplant sliced layered over mint yogurt, garnished with fresh coriander. steamed fresh vegetables, served over white basmati rice* 10.50
Lubia Palow *sautéed red kidney beans with onions, garlic and tomatoes, served with brown rice* 9.95
Bamia Chalow *okra sautéed with onions, tomatoes and spices; served with white basmati rice* 11.50

Authentic Afghani Pasta Dishes

Asheh Keshida *homemade noodles in tangy yogurt sauce, drizzled with sautéed garlic and butter* 9.95
Asheh Gooshti *homemade noodles with yogurt topped with mildly spiced meat sauce* 9.95
Ashak Pasta *homemade noodles. steamed scallion dumpling with yogurt sauce; with or without meat (ground beef)* 10.95
Asheh Keshida Lubiah *homemade noodles in tangy yogurt sauce, topped with red kidney beans and butter* 9.95
Mantoo Pasta *homemade noodles. steamed dumpling filled with minced beef, onions, herbs and spices; topped with yogurt and meat sauce* 10.95

Entrees

Quorma Sabzee With Lamb *spicy sautéed of chopped spinach, coriander and scallions, with morsels of tender lamb; served with white basmati rice* 11.95
Kabuli Palow With Lamb *brown basmati rice topped with raisins, slivered carrots and almonds; served with tender chunks of lamb* 12.50
Quorma Chalow *lamb, sautéed with onions and tomatoes; served with white basmati rice* 12.50
Lowand Chalow *tender morsels of boneless chicken sautéed in a savory yogurt sauce seasoned with spices; served with white rice* 12.50
Chicken Curry *chicken sautéed with onions, green peppers, tomatoes and curry; served with basmati rice* 12.50
Kofta Chalow *meatballs in tomatoes sauce and spices; served with white rice* 12.95
Quorma Badenjan With Lamb *eggplant sautéed with onions, green peppers, tomatoes and topped with slices of lamb; served with brown basmati rice* 11.
Shireen Palow Entrée *exotic rice dish cooked with orange peels, saffron, almonds a pistachios, served with grilled cornish game hen* 12.95
Fesenjan Entrée *sweet and sour pieces of boneless chicken flavored with walnuts and pomegranate juice; served with white rice* 12.95
Badenjan Bouranee *eggplant slices layered over mint yogurt, topped with savory meat sauce and garnished with parsley* 11.50
Lamb Curry *pieces of lamb sautéed with onions, green peppers, tomatoes and curry; served with basmati rice* 12.95

Sides

Side Order Of Vegetables *choice of spinach, eggplant, beans, pumpkin, or okra* 4.50
Toorshi *mixed pickled vegetables* 2.50
Dish Of Rice *white rice or brown rice* 5.00
Extra Bread *afghani bread* 1.00

Desserts $3.50

Baklava *rich layered dessert made with nuts and honey*
Firnee *traditional afghan milk, pudding with pistachios and rose water*

Beverages

Juice 1.95
Dough-Natural Yogurt Drink 1.75
Sodas *coke, sprite, ginger ale, diet coke, seltzer, orange* 1.75

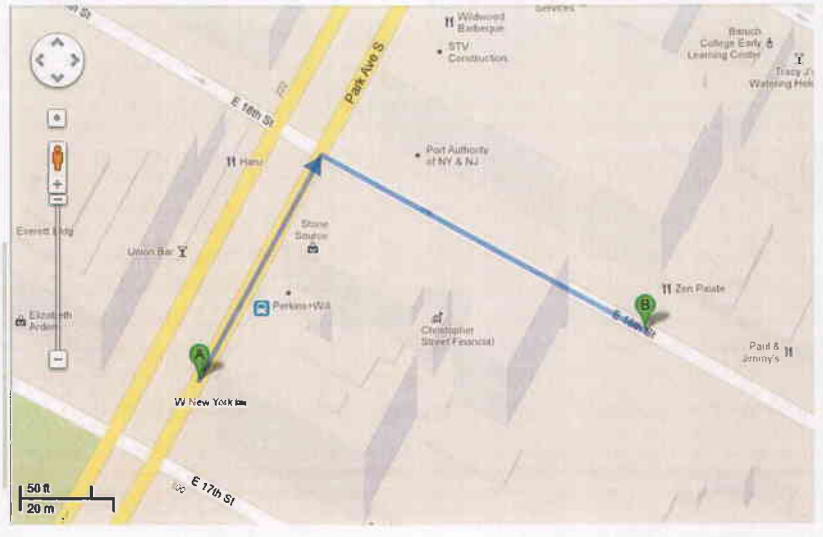
Tea

Earl Gray Tea 1.75
Peppermint Tea 1.75
Cardamom Tea 1.95
Pot Of Green Tea 4.50
Pot Of Persian Tea 4.50
Darjeeling Tea 1.75
Chamomile Tea 1.75
Shir Chay Tea *traditional afghani tea brewed with milk, sugar, cardamom and rose water* 5.
Pot Of Mint Tea 4.

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

ZEN PALATE (VEGETARIAN)



1. Head northeast on Park Ave S from W Union Square toward E 18th St – 180 ft.
2. Turn right onto E 18th St – 256 ft; destination will be on the left: Zen Palate, 115 E 18th St.

Route Time: 2 minutes.

Zen Palate

663 9th Ave
New York, NY 10036-1906
At 46th St

212 582-1669
Fax: 212 582-1708

YOUR AD HERE
MenuPages **PRIME** Advertising
for more info: www.menupages.com

Starters

Basil Peanut Moo Shu Rolls (2) 3.50
Edamame 3.95
Stuffed Mushroom Bean Loaves 6.75
Sampler *autumn rolls, tri-color zenmaki, moo shu rolls, stuffed mushroom, bean loaves, marinated soy pate, sweet yam fries* (for 2) 17.50
Taro Spring Rolls (4) 4.25
Vegetable Dumplings *steamed or pan-fried* (6) 6.25
Autumn Rolls (6) 6.95
Tri-Color Zenmaki 6.95
Scallion Pancakes 6.25
Grilled Marinated Seitan 8.25
Zen-Tastic Tofu 7.25
Sweet Yam Fries 5.50

Soups

Wonton Soup 4.25
Hot & Sour Soup 4.25
Miso Soup 3.95

Salads

Spinach Linguine Salad *carrots, bean sprouts and veggie burger meat in sesame peanut dressing* 6.95
Thai Chopped Salad *julienne of tossed asian vegetables in a refined peanut dressing, topped with peanut sprinkles* 6.95
Nature's Oasis Salad *baby greens, enoki mushrooms, cherry tomatoes, red onions, grilled marinated tofu soy cheese and cashews in a balsamic ginger soy dressing* 7.25
Grilled Sesame Tofu Salad *grilled marinated tofu with napa cabbage, watercress, crispy rice noodles and cherry tomatoes with sesame vinaigrette dressing* 7.50
Kale & Seaweed Salad *with silken tofu, with ginger vinaigrette dressing* 7.50

Noodle & Rice

Cantonese Pan-Fried Noodles *lightly pan-fried wheat noodles topped with broccoli, cauliflower, carrots, shitake mushrooms, snow peas & bokchoy in a kung-pao sauce* 11.50
Bangkok Fried Rice With Fresh Pineapple *fresh pineapple, wheat protein, bean sprouts, peas, onions, raisins, wolfeberry seeds, broccoli & cashew nuts stir-fried with brown / red rices* 12.95
Hong Kong-Style Stir-Fried Rice Fettuccini *with veggies* 8.95
Stir-Fried Whole-Wheat Noodles *with veggies* 9.50
Singaproe-Style Curried Rice Noodles *with veggies* 8.95
Tong Mein Noodle Soup *with deluxe soy nuggets & veggies* 8.95
Veggie Noodle Soup *choice: soba noodles, rice noodles, or spaghetti* 7.95
Curry Veggie Noodle Soup *choice: soba noodles, rice noodles, or spaghetti* 7.95
Steamed Sticky Rice 3.50
Steamed Brown / Red Rice 1.95
Moo Shu Crepe 0.95

Main Course

Celestial Tofu *delicately-battered soft bean curd with sundried tomato, tender seitan and broccolirabe with jalapeno in a light tomato-sage sauce* 16.95
Moo Shu Fantasia *wok-sauteed shredded green cabbage, carrots, glass noodles, mushrooms and savory soy ham, served with 4 wheat crepes* 16.95
Sizzling Medallions *crispy wheat gluten filet a l'orange, with fresh asparagus, mushrooms, string beans, and red onions on a sizzling platter* 19.25
Temple Of Zen *a thalthful melange of string beans, squash, carrot, broccoli, snow peas, mushrooms, red cabbage and jalapeno peppers, topped with grilled tofu, and crunchy kale* 16.50
Mushroom Forest *finely chopped mushrooms, snow peas, soy ham, sweet bell pepper & pineapple, served in lettuce cups* 18.95
Mala Portobello *fresh portobello mushroom caps and tender soy nuggets on a bed of romaine lettuce in a pungent black peppercorn-ginger sauce* 18.95
Red Mist *layers of bean crepe wrapped in seaweed in a sweet & spicy satay sauce topped julienne red pepper, snow peas, shiitake mushroom, enoki mushroom, and red onion served with thin rice, noodle and broccoli* 18.25
Tapestry Embarace *grilled marinated seitan fillet and fresh shiitake mushroom in a sweet teriyaki sauce, with fresh zucchini, yellow squash and a banana-leaf cone of asian sticky rice* 20.95
Wheel Of Dharma *tempura-battered shiitake mushrooms, mashed sweet potato and snow peas in a delicate onion-sage sauce* 20.95
West Lake *fresh shiitake mushroom caps and savory soy pate, in a light soy sauce with / cilantro, scallion, and steamed greens* 20.25
Crepe De Fleur *soy portein, pine nuts, waterchestnuts and vermicelli noodles with shiitake mushrooms, new potatoes, fresh basil and red onion in light curry sauce garinshed with a crispy yuba beggar's purse and tender asparagus spears* 21.95
E.T. *eggplant, tofu with tender wheat gluten, asparagus spears and ginko nuts in a delicate black bean and basil sauce, served on a sizzling platter* 17.50
Taste Of Curry *squash, cauliflower, okra, waterchestnuts, new potato and delicate tofu puffs in a spicy malaysian curry sauce on a wheat basket* 16.50
Garden Delight *a medley of grilled portobello mushroom, bell pepper, eggplant, asparagus, red onion and soy pate marinated in a vietnamese style lemongrass sauce* 16.95
Dream Land *fresh shiitake mushrooms, bean sprouts & crispy spinach linguine with pickled ginger on the top in sweet sour brown sauce with sesame seeds* 20.95

Prix Fixe

With Spring Rolls And Brown Rice

Shredded Heaven *chives, bean sprouts, bell peppers, jalapenos, shredded soy / wheat gluten* 11.25
Sweet And Sour Sensation *battered soy protein in sweet and sour sauce on a bed of blanched broccoli* 10.50
Mango Halo *fresh mangoes, cherry tomatoes, gingko nuts, snow peas & soy nuggets in a sweet kung pao sauce* 11.95
South By Southeast *beans and hearty soy croquettes served with a light and spicy vietnamese-style lemngreass sauce. with basil moo shu roll & blanched veggies.* 11.95
Shepherd Pie Croquette *potato pies stuff with a hardy comb of soy protein and veggies in teriyaki sauce. with basil rolls, pickled cabbage & salad* 10.95
Shredded Melody *shredded soy protein, celery, zucchini & pine nuts in a light garic sauce* 10.95
Felicity Mushroom With Basil Moo Shu Roll *fresh shiitake & button mushrooms sauteed with basil, bamboo shoots & carrots* 11.75
Curry Supreme *tender soy protein with potatoes & carrots in a mild curry sauce* 9.95
Rose Petals *home-made soy crepes with wolfberry seeds & garden vegetables in a sweet rice ginger sauce* 10.75
Mediterranean Medley *artichokes, wheat protein, basil & tomatoes stir-fried in basil-ginger white sauce* 10.50
Eggplant Zentastic *eggplant & bok choy in garlic sauce* 10.75
Tofu Delight *soft tofu, zucchini & tomatoes in a black bean sauce.* 9.95
Tex-Mex Moo Shu *kidney beans, barley & soy protein with spinach crepes served with guacamole & carrot peanut cole slaw* 10.95
Sesame Medallions *wheat gluten in an asian barbecue sauce on a bed of blanched broccoli* 11.25

Sandwiches

Zen Burger And Yam Fries 9.50
Portobello Burger And Yam Fries 8.50
Peking-Style Duck Wrap *with salad* 8.50
Zen Ham & Avocado Sandwich *with salad* 8.50

Cold Beverages

Fresh-Squeezed Orange Juice 5.75
Fresh-Squeezed Carrot Juice 5.75
Mixed Orange / Carrot Juice 5.75
Cranberry Iced Tea 3.95
Apple Iced Tea 3.95
Pneapple Iced Tea 3.95
Green Iced Tea 3.95
Regular Iced Tea 3.95
All Natural Root Beer 3.50
All Natural Ginger Beer 3.50
Fresh Ginger Ale 4.00
Soy Milk 2.95
Soda can 1.95
Fiji Water 6.25
San Pellegrino sm 3.75 lg 6.25

Hot Beverages

Fresh-Brewed Coffee 2.75
Organic Tea *earlgrey / green* 2.25
Decaf Tea *mint / chamomile* 2.25
Green Oolong 2.95

Desserts $5.50

Tofu Cheesecake
Banana Bliss
Key Lime Pie
Molton Hot Chocolate Cake

Delivery & Take Out

Starters

Taro Spring Rolls (2) *with shredded chinese cabbage, mushrooms, taro root and soy protein, fried until crisp and served with seasoned soy sauce* 3.50
extras: hot sauce, garlic sauce, extra red sauce 1.00
Sweet Yam Fries *crisp, sweet, delicious and nutritious!* 4.95
extras: hot sauce, garlic sauce, extra red sauce 1.00
Scallion Pancakes *pan-fried until crisp and served with hoisin sauce and fresh vegetable garnish. contains dairy protein* 5.50
extras: hot sauce, garlic sauce, extra red sauce 1.00
Autumn Rolls (6) *wood ear and enoki mushrooms with savory soy ham, bamboo shoots and crisp julienne snow peas wrapped in delicate soy bean sheets and fried until crisp. served with a sweet & tangy dipping sauce. contains dairy protein* 6.95
Sampler (Dinner) *autumn rolls, tri-color zenmaki, basil moo shu rolls, soy duck, soy chicken, and yam fries. contains dairy protein.* 16.50
Basil Peanut Moo-Shu Rolls (2) *dried jicama, carrots, mushrooms and soy with fresh basil, ginger and crushed peanuts rolled in rice paper.* 3.50
extras: hot sauce, garlic sauce, extra red sauce 1.00
Vegetable Dumplings (6) *fresh chopped vegetables, mushrooms and soy protein seasoned with ginger and cilantro wrapped in a tender wheat dumpling dough. lightly steamed or pan-fried.* 5.75
dumpling choice: steamed, pan-fried.
Edamame *tender, young soybeans steamed until tender in the pod and seasoned with salt.* 4.95
extras: hot sauce, garlic sauce, extra red sauce 1.00
Tri-Color Zenmaki (Dinner) *contains dairy protein* 6.95

Soups $3.95

Wonton Soup *house-made vegetable wontons in a delicate soup stock with tender spinach leaves and scallions*
Miso Soup *japanese white miso broth with a wakame seaweed, soft tofu and scallions*
Hot & Sour Soup *our vegetarian version of a chinese classic! with fresh coriander, black pepper and chinese red vinegar.*

Salads $5.95

Dressing Is Served On The Side.

House Salad *fresh mesclun leaves, cherry tomatoes, red onions and fresh enoki mushrooms, served with our soy vinaigrette*
Grilled Sesame Tofu Salad *grilled tofu, cherry tomatoes and crispy rice noodles over fresh watercress, chinese cabbage and mesclun leaves in a savory sesame vinaigrette*
Spinach Linguine Salad *fresh spinach noodles, carrot julienne and bean sprouts dressed with soy vinaigrette and peanut dressing*
Thai Chopped Salad *crispy julienne strips of fresh jicama, snow peas, cucumbers and carrot with sweet bell peppers and mesclun leaves in a thai peanut dressing.*
Kale & Seaweed Salad *chopped wakame, blanched kale and soft tofu in a tangy soy dressing*

Sandwiches $9.50

Zen Burger & Yam Fries *our original vegetable burger served on a whole-wheat bun with lettuce, tomato, alfalfa sprouts and a garbanzo bean spread. served with our delicious yam fries.*
Peking-Style Zenduck Wrap W/ Small Salad *tender soy duck and crispy yuba with whole leaf lettuce, crisp vegetables and hoisin sauce wrapped in a spinach tortilla. contains dairy protein*
substitute salad w/ yam fries. 1.00
Portobello Burger & Yam Fries *grilled marinated portobello mushroom cap topped with shredded carrots, alfalfa sprouts and tomato in a wheat bun. served with our classic yam fries.*

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

YOUR AD HERE
MenuPages ***PRIME*** Advertising
for more info: www.menupages.com

Zenham & Avocado Sandwich W/ Small Salad *on whole-grain bread with lettuce, tomatoes, carrots and alfalfa sprouts. contains dairy protein* ... 1.00
substitute salad w/ yam fries ... 1.00

Prix-Fixe Menu

Shredded Heaven *chives, bean sprouts, three kinds of shredded soy, and wheat gluten. served with taro spring roll and brown and red rice. contains dairy protein* ... 11.95
add brown rice ... 1.00
substitute w. moo shoo basil roll ... 1.00
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Mango Halo *with taro spring rolls and brown & red rice. fresh mangos, cherry tomatoes, ginko nuts, snow peas and soy nuggets in a sweet kung pau sauce. contains eggs* ... 11.95
substitute spring roll w/ peanut basil moo shu roll ... 1.00

Shredded Melody *shredded soy gluten sautéed with celery, carrots, zucchini and pine nuts in spicy sweet sauce. served with taro spring rolls, brown and red rice* ... 10.95
substitute w. moo shoo basil roll ... 1.00
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Curry Supreme *tender soy protein with potatoes and carrots in mild curry sauce. served with taro spring rolls, brown and red rice* ... 9.95
substitute w. moo shoo basil roll ... 1.00
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Rose Petals *home-made soy crepes with wolfberry seeds and garden vegetables in sweet rice ginger sauce. served with taro spring rolls, brown and red rice* ... 11.75
substitute w. moo shoo basil roll ... 1.00
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Eggplant Zentastic *eggplant and shanghai bok choy in spicy garlic sauce. served with taro spring rolls, brown and red rice* ... 10.75
substitute w. moo shoo basil roll ... 1.00
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Tex-Mex Moo Shu *kidney beans, soy gluten served in spinach crepes with guacamole sauce, carrot peanut cole slaw. served with salad and taro spring rolls* ... 11.95
substitute w. moo shoo basil roll ... 1.00
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Shepherd Pie Croquette *3 mini potato pies stuffed with a hardy combination of soy proteins and veggies. served with teriyaki sauce, 2 pieces of basil roll, and pickled cabbage and salad* ... 11.95

Sweet & Sour Sensation *battered soy protein in sweet and sour sauce on a bed of steamed broccoli. served with taro spring roll and brown and red rice* ... 10.50
add brown rice ... 1.00
substitute w. moo shoo basil roll ... 1.00
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

South By South East *a healthy mix of southeast asian and southern american flavors, kidney beans and hearty crouquettes, served with a light and spicy vietnamese style lemongrass sauce. served with basil moo shu rolls and blanched vegetables* ... 11.95
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Felicity Mushroom *fresh shiitake and button mushrooms sautéed with basil, bamboo shoots and carrots. served with basil peanut rolls, brown and red rice* ... 12.50
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Moo Shu Fantasia *wok-sauteed shredded green cabbage, carrots, glass noodles, mushrooms, and savory soy ham. served with 2 wheat crepes* ... 11.50
substitute w. moo shoo basil roll ... 1.00
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Mediterranean Medley *artichokes, basil and tomatoes stir-fried to perfection in a zesty garlic sauce with seitan. served with taro spring rolls and brown & red rice* ... 11.95
extras: hot sauce, garlic sauce, extra red sauce ... 1.00
substitute w. moo shoo basil roll ... 1.00

Tofu Delight *zucchini, tomatoes, soft tofu in black bean sauce. served with taro spring rolls, brown and red rice* ... 9.95
add brown rice ... 1.00
substitute w. moo shoo basil roll ... 1.00
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Sesame Medallions *thinly sliced wheat gluten in asian barbeque sauce garnished with steamed broccoli. served with taro spring rolls, brown and red rice* ... 11.25
add brown rice ... 1.00
substitute w. moo shoo basil roll ... 1.00
extras: hot sauce, garlic sauce, extra red sauce ... 1.00
extra duck sauce ... 0.50

Mini Veggie Loaf *served with spaghetti, broccoli and 2 taro spring rolls. made of jicama, cilantro, chestnut, and tofu. veggie sauce is made of onions, tomatoes, apples, and soy* ... 11.95

Entrées

Celestial Tofu (Dinner) *delicately-battered sof bean curd with sun-dried tomato, tender seitan and broccoli-rabe and jalapeno in a light tomato-sage sauce* ... 16.95
substitute spring roll: substitute w. moo shoo basil roll ... 1.00
extras: hot sauce
extras: garlic sauce, extra red sauce ... 1.00

a healthful melange of string beans, squash, carrot, broccoli, snow peas, mushrooms, red cabbage and jalapeno peppers, topped with grilled tofu, and crunchy kale and sesame seeds. contains eggs ... 16.50

Temple Of Zen (Dinner) *substitute spring roll: substitute w. moo shoo basil roll* ... 1.00
extras: hot sauce
extras: garlic sauce, extra red sauce

Wheel Of Dharma (Dinner) *tempura-battered shiitake mushrooms, mashed sweet potato and snow peas in a delicate onion-sage sauce. contains eggs* ... 19.95
substitute spring roll: substitute w. moo shoo basil roll ... 1.00
extras: hot sauce
extras: garlic sauce, extra red sauce ... 1.00

E.T. (Dinner) *eggplant and tofu! with tender wheat gluten, asparagus spears and gingko nuts in a delicate black bean and basil sauce, served on a sizzling platter* ... 18.50
substitute spring roll: substitute w. moo shoo basil roll ... 1.00
extras: hot sauce
extras: garlic sauce, extra red sauce ... 1.00

Red Mist *layers of soy bean crepe wrapped in seaweed in a coconut spicy sauce topped with snow pea, shitake and enoki mushrooms, jalapeno peppers and red onion served with rice noodle and broccoli* ... 17.50
substitute spring roll: substitute w. moo shoo basil roll ... 1.00
extras: hot sauce
extras: garlic sauce, extra red sauce ... 1.00

Sizzling Medallions (Dinner) *crispy wheat gluten filet a l`orange, with fresh asparagus, mushrroms, string beans, and red onions on a sizzling platter* ... 19.25
substitute spring roll: substitute w. moo shoo basil roll ... 1.00
extras: hot sauce
extras: garlic sauce, extra red sauce ... 1.00

Tapestry Embrace (Dinner) *grilled marinated seitan filet and fresh shiitake mushroom in a sweet teriyaki sauce, with fresh zucchini and yellow squash with a banana-leaf cone of asian sticky rice. contains eggs* ... 19.95

Crepe De Fleur (Dinner) *soy protein, pine nuts, waterchestnuts and vermicelli noodles with oyster mushrooms, new potatoes, fresh basil, and red onion in light curry sauce. garnished with a crispy yuba beggar`s purse and tender asparagus spears. contains eggs* ... 21.50
substitute spring roll: substitute w. moo shoo basil roll ... 1.00
extras: hot sauce
extras: garlic sauce, extra red sauce ... 1.00

Taste Of Curry (Dinner) *squash, cauliflower, okra, waterchestnuts, new potato, and delicate tofu puffs in a spicy malaysian curry sauce on wheat basket*
substitute spring roll: substitute w. moo shoo basil roll
extras: hot sauce
extras: garlic sauce, extra red sauce

Rice & Noodles

Stir Fried Soba Noodles *with soy and vegetables. contains dairy protein* ... 8.95
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Curry Rice Noodle Soup *tender chunks of soy protein, potatoes and carrots in a yellow curry soup with wide rice noodles* ... 8.95
extra protein ... 1.00

Tong-Mein Noodle Soup With Deluxe Vegetables *slices of our house-made soy chicken and mock duck, crisp garden vegetables and tender wheat noodles in a delightful vegetable broth. light, satisfying and delicious* ... 9.25
tong mein extras: extra soy chicken, extra mock duck ... 1.00
tong mein extras: extra mock ham ... 2.00
with mock ham instead of mock duck ... 1.00
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Stir-Fried Spinach Linguine *fresh spinach noodles wok-sautéed with sliced mushrooms, cabbage, carrots and snow peas in a light soy sauce* ... 8.95
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Stir-Fried Brown Rice With Soy *with soy. contains dairy protein* ... 7.95

Cantonese Pan-Fried Noodles W/ Vegetables (Dinner) *contains dairy protein* ... 12.50
extra: hot sauce
extras: garlic sauce, extra red sauce ... 1.00

Steamed Sticky Rice (Dinner) *contains dairy protein* ... 3.50

Bangkok Fried Rice *contains dairy protein* ... 12.50
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Curry Noodle Soup *tender chunks of soy protein, potatoes and carrots in a yellow curry soup with thin wheat noodles* ... 8.95
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Dumpling Soup With Vegetables *house-made veggie dumplings with crisp garden vegetables, chinese mustard greens and scallions in a delightful vegetable broth* ... 8.95
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Hong Kong-Style Stir-Fried Rice Fettuccini *with soy. contains dairy protein* ... 8.95
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Singapore-Style Curried Rice Noodles *contains dairy protein* ... 8.95
extras: hot sauce, garlic sauce, extra red sauce ... 1.00

Steamed Brown & Red Rice *wholegrain brown and red rice steamed until tender* ... 1.95

Moo Shu Crepe *contains dairy protein* ... (two per order) 1.90

Desserts $4.50

Tofu Cheesecake *served with blueberry sauce*
Key Lime High
Banana Bliss
Molten Hot Chocolate Cake

Beverages

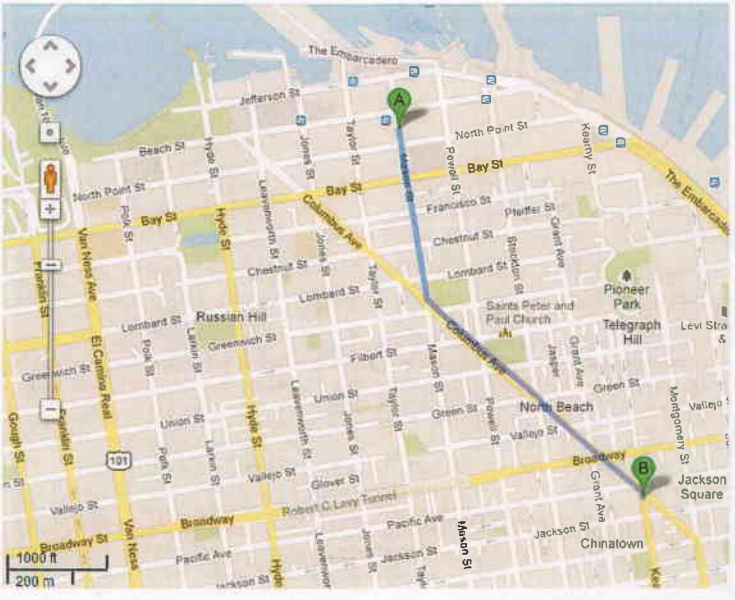
Canned Soda *soda choice: coke , diet coke, sprite, diet sprite, ginger ale* ... 1.95
Fresh Ginger Ale ... 4.00
San Pellegrino Water ... sm 3.75 lg 5.95
Fresh-Squeezed Carrot Juice ... 5.95
Cranberry Iced Tea *ice option: ice , no ice* ... 2.95
Pineapple Iced Tea *ice option: ice , no ice* ... 2.95
Regular Iced Tea *ice option: ice , no ice* ... 2.95
Fresh Brewed Coffee ... 2.75
Decaf Relaxing Tea ... 2.25
Jasmine Tea ... 2.25
All Natural Root Beer ... 2.50
Fiji Water ... *mineral water size: small $3.75, large $5.95* ... sm 3.75 lg 5.95
Fresh-Squeezed Orange Juice 5.95
Mixed Carrot & Orange Juice 5.95
Apple Ice Tea *ice option: ice , no ice* ... 2.95
Green Iced Tea *ice option: ice , no ice* ... 2.95
Soy Milk ... 3.50
Decaf Tea *decaf choice: mint, chamomile* ... 1.95
Organic Green Tea ... 2.25

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

San Francisco

TANDOORI MAHAL (HALAL)



1. Head south on Mason St from Sheraton Fisherman's Wharf toward North Point St – 0.3 mi.
2. Slight left onto Columbus Ave – 0.6 mi.
3. Slight right onto Kearny St – 69 ft; destination will be on the right, Tandoori Mahal, 941 Kearny St.

Route Time: 19 minutes.

Tandoori Mahal

941 Kearny St
San Francisco, CA 94133
At Columbus Ave

415 951-0505
Fax: 415 951-0506

YOUR AD HERE
MenuPages **PRIME** Advertising
for more info: www.menupages.com

Appetizers

Served with Homemade Mint and Sweet & Sour Tamarind Chutney

1. Papadum *crispy spiced lentil wafers* 2.00
2. Vegetable Samosa *homemade crisp patties, stuffed with fresh potatoes & peas* 4.50
3. Onion Bhaji *delicately spiced deep-fried onion fritters* 3.95
4. Palak Pakora *spinach coated in garbanzo batter, then deep fried* 4.95
5. Vegetable Pakora *mixed vegetable fritters delicately spiced* 3.95
6. Aloo Tikki *mashed potato patties served with chutney* 4.50
7. Cheese Pakora *homemade cheese pieces dipped in a batter & deep fried* 4.95
8. Fish Pakora *juicy & delicately spiced deep fried chicken fritters* 5.50
9. Chicken Pakora *juicy & delicately spiced deep fried chicken fritters* 4.95
10. Assorted Vegetable Platter 6.95
11. Assorted Clay Oven 8.95
12. Chicken Wing Tandoori 6.95

Soups, Salads & Sides

14. Dal Soup *delicately spiced lentil soup garnished with vegetables* 2.95
15. Chicken Soup *chicken soup, flavored with indian herbs* 3.95
16. Mulligatawny Soup *a delicately spiced chicken and lemon soup* 4.95
17. Mixed Green Salad 3.95
18. Cucumber Salad *indian style cucumber, tomato and onion salad* 3.95
19. Raita *homemade yogurt with cucumber and spices* 1.50
20. Mango Chutney 2.00
21. Mixed Pickles 1.50

Mint Chutney 0.75
Tamarind Sauce 0.75

Breads

Freshly Clay Oven Baked Breads

22. Nan *leavened bread baked in tandoor* 2.00
23. Cheese Nan *nan stuffed with homemade cheese* 2.95
24. Onion Kulcha *nan stuffed with onion* 2.95
25. Garlic Man *leavened bread stuffed with fresh garlic* 2.95
26. Kashmiri Nan *nan stuffed with raisins, nuts, coconut and cherries* 2.95
27. Chicken Nan *nan stuffed with spiced bits of chicken* 3.95
28. Keema Nan *leavened bread stuffed with minced lamb* 3.95
29. Chapatti *famous whole wheat bread* 2.00
30. Paratha *buttered and multi-layered whole wheat bread* 2.95
31. Aloo Paratha *whole wheat bread stuffed with spiced potatoes & peas* 2.95
32. Chili Nan *nan stuffed with fresh chili* 3.95
33. Poori *deep fried whole wheat punjabi balloon bread* 1.50
34. Bhatura *white flour deep fried bread* 2.00
35. Spinach Nan *nan stuffed with fresh spinach* 3.95
36. Assorted Basket *one each of kashmiri nan, garlic nan and chapatti* 7.95

Pudina Nan *nan stuffed with fresh mint* 3.95

Lamb Dishes

Served Mild, Medium of Spicy Hot Upon Request

37. Lamb Coconut A La Carte *lamb simmered in coconut milk* 12.95
38. Hyderabadi Lamb A La Carte *cubes of lamb cooked hyderabadi style with apricot &potato straws* 13.95
39. Classic Lamb Curry A La Carte *rogan josh- traditional authentic lamb curry cooked in a blend of tomato & spices* 11.95
40. Lamb Do Piaza A La Carte *lamb cubes cooked with stir-fried onion, ginger, garlic tomato and spices* 11.95
41. Punjabi Lamb Curry *a north indian preparation of hot lamb curry* 10.95
42. Lamb Saag A La Carte *lamb cooked with delicious spiced creamed spinach* 12.95
43. Lamb Vindaloo A La Carte *lamb in a hot spicy sauce with potatoes* 12.95
44. Karabi Ghost A La Carte *cubes of lamb cooked in fresh garlic* 12.95
45. Lamb Kofta A La Carte *minced lamb balls cooked in mildly spiced creamy sauce* 12.95
46. Lamb Korma A La Carte *lamb cooked in mildly spiced cream sauce with saffron and nuts* 13.95
47. Lamb Tikka Masala A La Carte *clay oven roasted lamb cubes in spicy sauce* 13.95
48. Lamb Jal Frazie A La Carte *tender lamb pieces pan fried with a potpourri of chopped assorted vegetables* 12.95
49. Kashmiri Lamb A La Carte *clay oven roasted lamb with spinach* 13.95

Tandoori Lamb Chops *tender lamb marinated in our special sauce and spices, then roasted to perfection in our tandoori oven* 19.95

Chicken Dishes

Served Mild, Medium of Spicy Hot Upon Request

50. Chicken Coconut Curry *chicken cooked in coconut sauce and spices with lentils* 11.95
51. Chicken Curry *chicken cooked in a blend of tomatoes and spices* 10.95
52. Chicken Da Piaza *chicken cooked with stir-fried onion, ginger, garlic, tomato and spices* 10.95
53. Chicken Vindaloo *chicken cooked in hot spicy sauce with potatoes* 10.95
54. Chicken Tikka Masala *clay oven roasted chicken in spicy sauce* 12.95
55. Chicken Makhni *tandoori chicken cooked in a mildly spicy sauce* 11.95
56. Chicken Korma *chicken in a moderately spiced cream sauce with nuts* 11.95
57. Garlic Chicken *chicken cooked in fresh garlic, green onion and spices* 10.95
58. Chicken Mushroom *tender chicken cooked with spices and mushrooms* 10.95
59. Chicken Saag *tender chicken cooked with spices and mushrooms* 11.95
60. Chicken Jal Frazie *tender chicken cooked with a potpourri of chopped assorted vegetables* 11.95
61. Punjabi Chicken Curry *a north indian preparation of hot chicken curry* 11.95
62. Hyderabadi Chicken Curry *chicken cooked hyderabadi style with spices, apricots and potato straws* 11.95
63. Velvet Butter Chicken *an old favorite, diced chicken cooked with aromatic spices* 12.95
64. Kashmiri Chicken *clay oven roasted strips of chicken in spinach* 12.95

India Clay Oven Specialties

All dishes are cooked on charcoal fire in clay pot and served on sizzling platter.

65. Tandoori Chicken *chicken marinated in yogurt, ginger and garlic, then roasted in our clay oven* 10.95
66. Chicken Tekka Kabab *boneless chicken cubes marinated in spices and cooked in the clay oven a charcoal fire* 12.95
67. Kashmiri Kabab *boneless chicken cubes marinated kashmiri style and roasted* 11.95
68. Boti Kabab *succulent cubed leg of lamb, marinated and roasted in the clay oven* 14.95
69. Prawn Tandoori *jumbo prawns marinated in yogurt & spices then roasted in the clay oven* 15.95
70. Fish Tandoori *fish marinated in special spices and herbs cooked on skewers* 15.95
71. Seekh Kabab *minced leg of lamb mixed with herbs and spices, then dry cooked on skewers* 14.95
72. Tandoori Minced Grill *assorted clay oven specialties* 16.95

Rice Dishes

Tempting Rice Dishes

73. Pilaf Rice *saffron flavored basmati rice garnished with green peas* 2.95
74. Vegetable Biryani *saffron flavored basmati rice with vegetables and nuts* 9.95
75. Chicken Biryani *saffron flavored basmati rice with spiced chicken and nuts* 11.95
76. Lamb Biryani *saffron flavored basmati rice with spiced lamb and nuts* 12.95
77. Prawn Biryani *saffron flavored basmati rice with prawns and nuts* 14.95
78. Punjabi Fried Rice *basmati rice fried with potatoes, egg & green peas* 6.95

Seafood Entrees

79. Punjabi Prawn Curry *prawn cooked in a blend of tomato and spices* 13.95
80. Prawn Do Piaza *prawns cooked with stir fried onions & ginger* 13.95
81. Prawn Vindaloo *shrimp cooked hot and spicy sauce with potatoes* 13.95
82. Prawn Saag *prawns cooked in deliciously spiced cream spinach* 13.95
83. Prawn Tikka Masala *clay oven roasted prawns in a mild cream sauce* 14.95
84. Prawn Mushroom *prawns cooked with spices and mushrooms* 13.95
85. Prawn Jalfrezi *prawns cooked with a potpourri of assorted vegetables* 13.95
86. Prawns Korma *prawns cooked in a moderately spiced cream sauce* 14.95
87. Prawns Goa Curry *king prawns cooked traditional goanese style with coconut milk & spices* 14.95
88. Fish Vindaloo *select fish cooked with stir fired onion, tomato & potatoes* 13.95
89. Fish Tikka Masala *clay oven roasted fish cooked in an exotic blend of spices* 14.95
90. Punjabi Fish Curry *a northern indian preparation of hot fish curry* 14.95
91. Kashmiri Fish *clay oven roasted fresh fish in cream spinach* 14.95

Vegetarian Entrees

92. Mixed Vegetable Masala *fresh cut assorted vegetables in stir fried onion, ginger, garlic & mild sauce* 9.95
93. Aloo Gobi *fresh cut assorted vegetables in stir fried onion, ginger, garlic & mild sauce* 9.95
94. Baingan Bhartha *fresh eggplant, baked and cooked with onions, tomatoes and spices* 9.95
95. Mushroom Masala *fresh mushrooms cooked with chopped onions, tomatoes & spices* 10.95
96. Mattar Paneer *green peas and homemade cheese cooked with spicy gravy* 9.95
97. Vegetable Korma *vegetables with farmers cheese and nuts in a mild creamy sauce* 10.95
98. Malai Kofta *cheese balls in a mildly spiced gravy* 9.95
99. Saag Paneer *fresh spinach cooked with herbs and spices with homemade cheese cubes* 9.95

Butter Vegetable *fresh cut vegetables cooked in a creamy tomato sauce* 10.95

100. Aloo Spinach *fresh spinach cooked with herbs, spices and potatoes* 9.95
101. Chana Masala *spicy garbanzo beans* 9.95
102. Dal Makhani *creamed lentils delicately spiced* 8.95
103. Bhindi Bhaji Masala *fresh cut okra cooked with chopped onions, tomatoes and spices* 10.95
104. Aloo Matter *green peas and potatoes cooked with chopped onions, tomatoes & spices* 9.95
105. Paneer Makhani *homemade cheese in creamy tomato sauce* 10.95
106. Vegetable Coconut Curry *fresh mixed vegetables in coconut milk* 10.95
107. Hyderabadi Vegetable *fresh mixed vegetables cooked hyderabadi style with spices, apricots and potato straws* 10.95
108. Palak Dal *fresh spinach cooked with lentils* 10.95

India Clay Oven Dinners

A Great Way To Experience A Taste Of India

Vegetable Thali Dinner For 2 Vegetarian *comes with dal makhni, saag paneer, vegetable samosa, papadam, rice, nan, kheer & rice* 34.95

110. Clay Oven Thali Dinner For 2 *comes with: tandoori chicken, boti kabab, saag paneer, papadam, rice, nan, raita, kheer, veggie samosa & chicken tikka masala* 39.95

Desserts

Kheer *dessert made from basmati rice cooked with sugar, milk and served cold with almonds & pistachio nuts* 2.95

Kulfi *authentic saffron flavored indian ice cream enriched with nuts* 3.50

Gulab Jamun *cottage cheese balls fried and soaked in flavored syrup* 3.50

Mango Ice Cream *fresh homemade ice cream with mango pulp* 3.50

Coconut Ice Cream *fresh homemade ice cream with delicious coconut* 3.50

Beverages

Lassi *a refreshing drink with homemade yogurt* 2.95

Mango Lassi *a refreshing drink with homemade yogurt & indian Alfonzo mango juice* 2.95

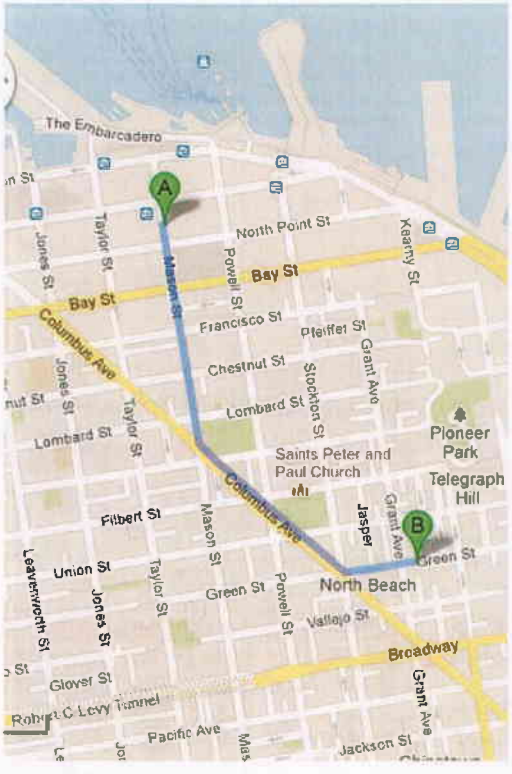
Chai Tea *special tea from east himalayan valleys* 2.00

Iced Tea 2.00
Sodas 2.00
Lemonade 2.00
Coffee 2

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

MAYKADEH PERSIAN CUISINE (HALAL)



1. Head south on Mason St from Sheraton Fisherman's Wharf toward North Point St – 0.3 mi.
2. Slight left onto Columbus Ave – 0.3 mi.
3. Turn left onto Green St – 0.1 mi; destination will be on the left, Maykadeh Persian Cuisine, 470 Green St.

Route Time: 16 minutes.

Maykadeh
470 Green St
San Francisco, CA 94133
At Grant Ave

415 362-8286
Fax: 415 362-8288

YOUR AD HERE
MenuPages **PRIME** Advertising
for more info: www.menupages.com

Mazeh Appetizers

Shirazi Salad *diced cucumber, tomato & onion with olive oil, lime juice* 6.00
Mast-O-Khier *homemade yogurt and cucumber* 6.00
Mast-O-Musir *yogurt with dried elephant garlic* 6.00
Feta Cheese Spread *oven roasted tomato, basil, olive oil and bulgarian feta cheese* 7.00
Feta Cheese And Olive *marinated calamata olives and bulgarian feta cheese* 7.00
Sabzee And Panir *traditional garnish & feta cheese* 7.00
Torshee *pickled vegetable* 6.00
Pickles *baby cucumber* 6.00
Fancy Salad *poached pear, baby spinach, hearts of palm, candied walnuts, pomegranate vinaigrette* 12.00
Greek Salad *heart of romaine, cucumber, tomato, feta cheese and olive* 9.00
Hearts Of Romaine *hearts of romaine with persian lime dressing* 8.00
Baba Ghanoush *smoked roasted eggplant, garlic, tahini* 9.00
Hummus *garbanzo, tahini and roasted garlic* 9.00
Kashke Bademjan *eggplant, mint garlic sauce* 9.00
Aash *barley and vegetable soup* 7.00
Polo *plate of basmati rice* 6.00
Koobideh *one side skewer of koobideh* 6.00
Lamb Tongue *lamb tongue with lime juice, sour cream and saffron* 15.00
Lamb Head *traditional, cinnamon and turmeric broth* 15.00
Brain *boiled brain, (100% cholesterol free) lime, saffron* 15.00
Pache *lamb feet, cinnamon, turmeric broth* 15.00
Rocky Mountain Oysters *when available* 16.00

Entrees

Chelo-Kebab Koobideh *skewered mixture of certified angus beef and leg of lamb, onion, ground daily, onion, persian spices, basmati rice* 14.75
Joojeh Kebab *boneless chicken thighs marinated in saffron, onion and lime juice, vegetables, basmati rice* 15.50
Breast Kebab *marinated boneless breast of chicken, in onion, basil, lime juice, vegetables, basmati rice* 16.50
Poussin *baby chicken with all the bones marinated in onion, saffron, lime juice, vegetables and basmati rice* 17.50
Shishlik *rack of lamb chops marinated with basil, garlic, onion, lime juice, vegetables, basmati rice* 25.00
Shish-Kebab *filet of lamb marinated in lime juice, saffron, onion, extra olive oil, vegetables and basmati rice* 25.00
Maykadeh Kabab (Barg) *skewered thin slices of filet mignon marinated in lime juice and onion* 25.00
Maykadeh Soltani *skewered thin slices of filet mignon marinated in lime juice and onion, plus one skewer of koobideh* 28.00
Ghorme Sabzee *lamb shank cooked in finely chopped onion, leek, scallions, chives & herbs, dried lime, basmati rice* 16.00
Khoresht Bademjan *lamb shank, baby eggplant braised with tomato, saffron, sun dried lime, basmati rice* 16.00
Khoresht Bademjan Vegetarian 16.00
Khoresht Fesenjoon *sweet and sour sauce, dry roasted walnuts, pomegranate juice, chicken thighs, basmati rice* 16.00
Khoresht Fesenjoon Vegetarian *sweet and sour sauce* 16.00
Khoresht Ghaymeh *pieces of lamb, yellow split peas, saffron, tomato, sundried lime, basmati rice* 16.00
Zereshk Polo *basmati rice, barberry, saffron, chicken thighs* 16.00
Baghali Polo *sunday only. fava beans, dill, rice, served with lamb shank in a glazed onion saffron sauce* 16.00

Steak

Filet Mignon *dry aged angus filet in stroganoff sauce or broiled served with persian fries and vegetables* 31.00
Rib Eye Steak *dry aged black angus rib eye broiled to perfection served with persian fries and vegetables* 28.00

Seafood

Giant Prawns *giant prawns in shell served with vegetable* 26.00
Wild Salmon Or Wild Sturgeon *when available*
Fish Of The Day

Desserts

Bastani *persian ice cream* 6.00
Pallodeh 6.00
Creme Caramel 6.00
Baklava 5.00
Poached Pears *in shiraz reduction sauce and a scoop of ice cream* 8.50

Beverage

Dough 3.50
Soft Drinks *no refill* 2.50
Persian Tea, Coffee, Milk 2.00

Halal Menu

Mazeh Appetizers

Shirazi Salad *diced cucumber, tomato & onion with olive oil, lime juice* 6.00
Mast-O-Khiar *homemade yogurt and cucumber* 6.00
Mast-O-Musir *yogurt with dried elephant garlic* 6.00
Feta Cheese Spread *oven roasted tomato, basil, olive oil and bulgarian feta cheese* 7.00
Feta Cheese And Olive *marinated calamata olives and bulgarian feta cheese* 7.00
Sabzee And Panir *traditional garnish & feta cheese* 7.00
Torshee *pickled vegetable* 6.00
Pickles *baby cucumber* 6.00
Fancy Salad *poached pear, spinach, hearts of palm, candied walnuts, pomegranate vinaigrette* 12.00
Greek Salad *heart of romaine, cucumber, tomato, feta cheese and olive* 9.00
Hearts Of Romaine *hearts of romaine with persian lime dressing* 8.00
Baba Ghanoush *smoked roasted eggplant, garlic, tahini* 9.00
Hummus *garbanzo, tahini and roasted garlic* 9.00
Kashke Bademjan *eggplant, mint garlic sauce* 9.00
Aash *barley and vegetable soup* 7.00
Poloo *plate of basmati rice* 6.00
Koobideh *one side skewer of koobideh* 6.00
Lamb Tongue *lamb tongue with lime juice, sour cream and saffron* 15.00
Lamb Head *traditional, cinnamon and turmeric broth* 15.00
Brain *boiled brain, (100% cholesterol free) lime, saffron* 15.00
Pache *lamb feet, cinnamon, turmeric broth* 15.00

Entrees

Chelo-Kebab Koobideh *skewered mixture of certified angus beef and leg of lamb, ground daily, onion, persian spices, basmati rice* 14.75
Joojeh Kebab *boneless chicken thighs marinated in saffron, onion and lime juice, vegetables, basmati rice* 15.50
Breast Kebab *marinated boneless breast of chicken, in onion, basil, lime juice, vegetables, basmati rice* 16.50
Poussin *baby chicken with all the bones marinated in onion, saffron, lime juice, vegetables and basmati rice* 17.50
Shishlik *rack of lamb chops marinated with basil, garlic, onion, lime juice, vegetables, basmati rice* 25.00
Shish-Kebab *filet of lamb marinated in lime juice, saffron, onion, extra virgin olive oil, vegetables and basmati rice* 25.00
Ghorme Sabzee *lamb shank cooked in finely chopped onion, leek, scallions, chives & herbs, dried lime, basmati rice* 16.00
Khoresht Bademjan *lamb shank, baby eggplant braised with tomato, saffron, sun dried lime, basmati rice* 16.00
Khoresht Bademjan Vegetarian 16.00
Khoresht Fesenjoon *sweet and sour sauce. dry roasted walnuts, pomegranate juice, chicken thighs, basmati rice* 16.
Khoresht Fesenjoon Vegetarian *sweet and sour sauce* 16.00
Khoresht Ghaymeh *pieces of lamb, yellow split peas, saffron, tomato, sun dried lime, basmati rice* 16.00
Zereshk Polo *basmati rice, barberry, saffron, chicken thighs* 16.00
Baghali Polo *sunday only. fava beans, dill, rice, served with lamb shank in a glazed onion saffron sauce* 16.00

Seafood

Giant Prawns *giant prawns in shell served with vegetable* 26.00
Wild Salmon Or Wild Sturgeon *when available*
Fish of The Day

Dessert

Bastani *persian ice cream* 6.00
Pallodeh 6.00
Creme Caramel 6.00
Baklava 5.00
Poached Pears *in shiraz reduction sauce and a scoop of ice cream* 8.50

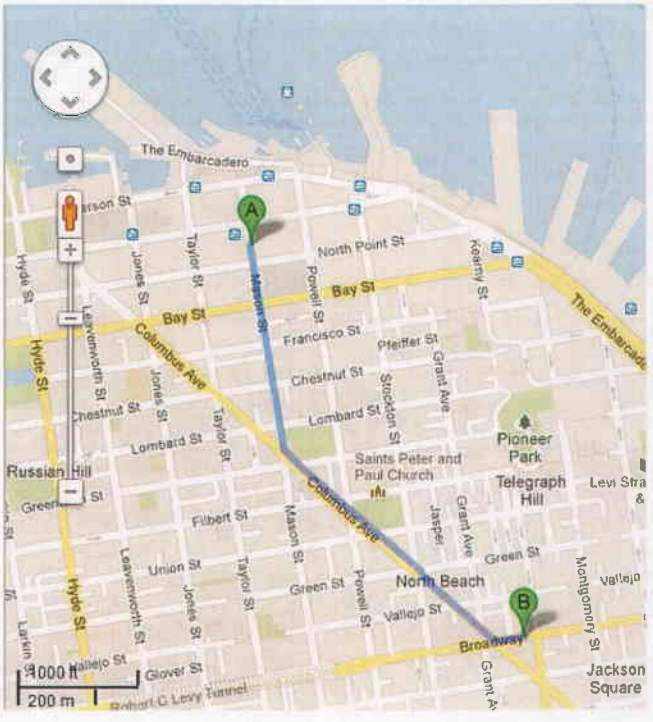
Beverage

Dough 3.50
Soft Drinks *no refill* 2.50
Persian Tea. Coffee, Milk 2.00

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

URBAN CURRY (HALAL)



1. Head south on Mason St from Sheraton Fisherman's Wharf toward North Point St – 0.3 mi.
2. Slight left onto Columbus Ave – 0.5 mi.
3. Turn left onto Broadway St – 240 ft; destination will be on the right, Urban Curry, 523 Broadway.

Route Time: 18 minutes.

Urban Curry
523 Broadway
San Francisco, CA 94133
Btwn Kearny St & Columbus Ave

415 677-9744

YOUR AD HERE
MenuPages ***PRIME*** Advertising
for more info: www.menupages.com

Appetizers

Aloo Tikki *mashed potatoes patties fried with herbs and spices* 3.99
Chicken Pakora *chicken slices coated in chickpeas batter with herbs and spices* 4.99
Fish Pakora *boneless fish slices coated in chickpeas batter with herbs and spices* 6.99
Paneer Pakora *cheese slices coated in chickpeas batter with herbs and spices* 4.99
Papadum *spiced crisp sun dried lentil wafers baked in clay oven* 1.99
Shrimp Pakora *tiger prawn coated in chickpeas batter with herbs and spices* 7.99
Vegetable Pakora *two crisp turn overstuffed with potatoes, peas, herbs and spices* 3.99
Vegetable Samosa *two crisp turn overstuffed with potatoes, peas, herbs and spices* 3.99

Soups & Salads

Chicken Salad *sliced chicken boti with mixed green salad* 5.99
Cucumber Salad *cucumbers with indian dressing* 3.99
Daal Soup *lentils simmered with cumin, cilantro, herbs and spices* 2.99
Mix Green Salad *mix green lettuce, tomatoes, cucumbers and green chillies* 3.99
Onion Chilli Salad *sliced onions with green chillies* 1.99
Prawn Salad *tiger prawn with mixed salad* 7.99

Tandoories

Chicken Boti *boneless chicken cubes marinated in yogurt, herbs and spices. baked in special clay oven* 8.99
Chicken Seekh Kabob *mildly spiced chicken minced and skewered with herbs and spices. baked in special clay oven* 5.99
Cream Pepper Chicken *boneless chicken (dark meat) marinated in cream, green chili, herbs and spices. baked in clay oven* 9.99
Fish Tandoori *boneless fish cubes marinated in herbs and spices. baked in special clay oven* 11.99
Lamb Boti *boneless lamb cubes marinated in yogurt, herbs and spices. baked in special clay oven* 11.99
Lamb Seekh Kabob *mildly spiced lamb minced and skewered with herbs and spices. baked in special clay oven* 6.99
Prawn Tandoori *tiger prawn marinated in herbs and spices. baked in special clay oven* 12.99
Tandoori Chicken *chicken marinated in yogurt, herbs and spices. baked in special clay oven* 8.99
breast 4.99
leg 3.99

Karahies

Chicken Karahi *mashed potatoes patties fried with herbs and spices* 9.99
Fish Karahi *chicken slices coated in chickpeas batter with herbs and spices* 10.99
Goat Karahi *boneless fish slices coated in chickpeas batter with herbs and spices* 12.99
Keema Karahi *cheese slices coated in chickpeas batter with herbs and spices* 9.99
Keema Mutter Karahi *spiced crisp sun dried lentil wafers baked in clay oven* 10.99
Lamb Karahi *tiger prawn coated in chickpeas batter with herbs and spices* 11.99
Prawn Karahi *two crisp turn overstuffed with potatoes, peas, herbs and spices* 13.99
Seekh Kabob Karahi *two crisp turn overstuffed with potatoes, peas, herbs and spices* 9.99

Vegetarian

Aloo Gobhi *cauliflower and potatoes cooked in onion based sauce with herbs and spices* 7.99
Aloo Palak *creamed spinach cooked with potatoes in onion based sauce with herbs and spices* 7.99
Bainghan Bartha *baked eggplant cooked with onions, peas, tomatoes, bell peppers, herbs and spices* 7.99
Bhindi Masala *okra cooked in onion based sauce with herbs and spices* 7.99
Daal Chana *yellow lentils cooked in onion based sauce with herbs and spices* 6.99
Lahori Cholay *garbanzo beans cooked in onion based sauce with herbs and spices* 6.99
Malai Kofta *homemade cheese cooked in creamy sauce, herbs and spices* 8.99
Mix Vegetable Curry *mixed vegetables cooked in onion based sauce with herbs and spices* 7.99
Mushroom Masala *mushrooms cooked in onion based sauce with herbs and spices* 7.99
Mutter Paneer *green peas, cheese cooked in onion based sauce with herbs and spices* 8.99
Navrattan Korma *mixed vegetables and cheese cooked in onion based sauce with dry fruits, herbs and spices* 8.99
Palak Paneer *creamed spinach cooked with homemade cheese, herbs and spices* 8.99
Paneer Tikka Masala *homemade cheese cooked in creamy sauce, herbs and spices* 8.99
Shahi Paneer *homemade cheese cooked in creamy sauce, bell peppers, herbs and spices* 8.99

Rice & Biryanies

Basmati Rice *boneless chicken cubes marinated in yogurt, herbs and spices. baked in special clay oven* 1.99
Chicken Biryani *mildly spiced chicken minced and skewered with herbs and spices. baked in special clay oven* 9.99
Goat Biryani *boneless chicken (dark meat) marinated in cream, green chili, herbs and spices. baked in clay oven* 12.99
Lamb Biryani *boneless fish cubes marinated in herbs and spices. baked in special clay oven* 10.99
Prawn Biryani *boneless lamb cubes marinated in yogurt, herbs and spices. baked in special clay oven* 13.99
Vegetable Biryani *mildly spiced lamb minced and skewered with herbs and spices. baked in special clay oven* 8.99

Chicken

Achari Chicken *boneless chicken cooked with pickles, herbs and spices* 8.99
Chicken Curry *boneless chicken cooked with ginger, garlic and special blend of spices* 7.99
Chicken Gobhi *boneless chicken cooked with cauliflower, herbs and spices* 7.99
Chicken Jalfrazi *chicken curry with bell peppers, onions, tomatoes, herbs and spices* 8.99
Chicken Palak *boneless chicken cooked with spinach, herbs and spices* 8.99
Chicken Tikka Masala *boneless chicken cooked in mild spiced cream and tomato sauce* 7.99
Chicken Vindaloo *boneless chicken cooked with potatoes, herbs and spices* 8.99
Daal Chicken *boneless chicken cooked with lentils, herbs and spices* 7.99

Lamb

Achari Ghosht *goat meat cooked with pickles, herbs and spices* 8.99
Gobhi Gosht *boneless lamb cooked with cauliflower, herbs and spices* 8.99
Lamb Curry *boneless lamb cooked with ginger, garlic and special blend of spices* 8.99
Lamb Daal *boneless lamb cooked with lentils, herbs and spices* 8.99
Lamb Jalfrazi *lamb curry with bell peppers, onions, tomatoes, herbs and spices* 8.99
Lamb Saagwala *boneless lamb cooked with spinach, herbs and spices* 9.99
Lamb Tikka Masala *boneless lamb cooked in mild spiced cream and tomato sauce* 8.99
Lamb Vindaloo *boneless lamb cooked with potatoes, herbs and spices* 8.99
Roghan Josh *boneless lamb cooked with special blend of spices* 9.99

Seafood

Fish Curry *boneless fish cooked with ginger, garlic and special blend of spices* 9.99
Fish Tikka Masala *boneless fish cooked in mild spiced cream and tomato sauce* 9.99
Lahori Fish *fish fried lahori style with our special homemade herbs and spices* 9.99
Mix Seafood Curry *boneless fish and prawns cooked with ginger, garlic and special blend of spices* 13.99
Prawn Jalfrazi *tiger prawns cooked with bell peppers, onions, tomatoes, herbs and spices* 12.99
Prawn Saagwala *tiger prawns cooked with spinach, herbs and spices* 12.99
Prawn Tikka Masala *tiger prawn cooked in mild spiced cream and tomato sauce* 12.99
Prawn Vindaloo *tiger prawns cooked with potatoes, herbs and spices* 12.99

Naan - Breads

Aloo Naan *white flour bread stuffed with potatoes and cilantro. baked in clay oven* 2.99
Garlic Naan *white flour bread with garlic baked in clay oven* 2.99
Keema Naan *white flour bread stuffed with chicken and cilantro. baked in clay oven* 3.99
Lacha Paratha *whole wheat flour bread baked in our special clay oven* 3.99
Onion Naan *white flour bread stuffed with onions and cilantro. baked in clay oven* 2.99
Paneer Naan *white flour bread stuffed with cheese and cilantro. baked in clay oven* 3.99
Plain Naan *white flour bread baked in clay oven* 1.99
Roti *whole wheat flour bread baked in clay oven* 1.99

Desserts $3.99

Almond Kheer *indian rice pudding with almond and cardamom*
Gulab Jamun *dry milk balls in syrup*

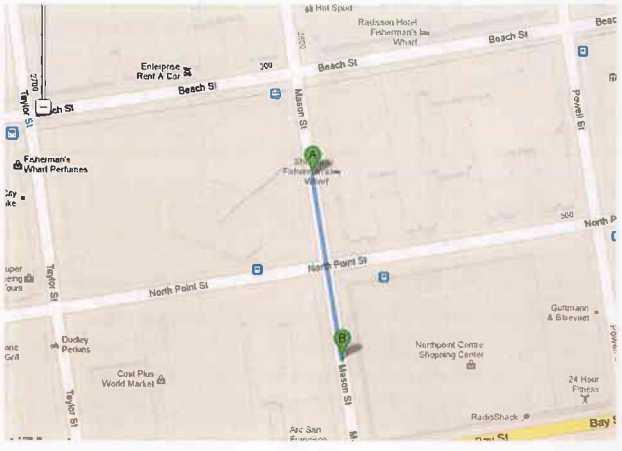
Beverages

Mango Lassi *mango and yogurt blended drink* 2.99
Soft Drinks *coke, diet coke, pepsi, sprite and mineral water* 1.00
Sweet & Salty Lassi *yogurt blended drink* 2.

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

Café Pescatore (Seafood)



1. Head south on Mason St toward North Point St – 350 ft; destination will be on the left, Cafe Pescatore, 2455 Mason St.

Route Time: 1 minute.

Cafe Pescatore

2455 Mason St
San Francisco, CA 94133
At N Point St

415 561-1111
Fax: 415 292-4549

YOUR AD HERE
MenuPages **PRIME** Advertising
for more info: www.menupages.com

Breakfast

Egg Specialties

Served With Home Fried Potatoes And Choice Of English Muffin, Sourdough, Rye Or Wheat Toast. Egg Beaters Available for Substitution

Sausage Omelete *spicy italian sausage, bell pepper, onion, mozzarella cheese* 12.00
Mushroom Omelete *mushroom, scallion, fontina cheese* 11.00
Ham Omelete *ham, scallion, cheddar cheese* 12.00
Vegetarian Frittata *mushroom, onion, bell pepper, spinach, fontina cheese* 10.00
Two Eggs Breakfast *two eggs any style, choice of bacon, italian sausage or ham* 11.00

House Favorites

Eggs Benedict *english muffin, sliced ham, two poached eggs, hollandaise sauce, home fries* 12.00
Hose made Cinnamon Raisin French Toast *fresh fruit, warm maple syrup* 11.00
The Continental *choice of croissant or muffin, fresh fruit, juice, coffee or tea* 12.00
The European *toast, sliced cheese, juice, coffee or tea* 11.00
House Made Granola *fresh fruit, yogurt* 9.00
Hot Oatmeal *currants, brown sugar* 7.00

Sides

Toast *sourdough, wheat, rye, english muffin* 3.00
Croissant Or Muffin 4.00
Fresh Fruit 5.00
Raisin Bran or Corn Flakes *with sliced banana* 5.00
Home Fries 3.00
Sliced Cheese 3.00
Applewood Smoked Bacon 5.00
Spicy Italian Link Sausage 5.00
Dakota Ham 5.00
Side Two Eggs 4.00

Eye Openers

Bloody Mary 8.00
Spicy Virgin Mary 4.00
Mimosa Or Bellini 8.00
Fresh Orange Or Grapefruit Juice 4.00
Apple, Cranberry, Pineapple Or Tomato Juice 3.00
Coffee *mountainos bros. shade grown organic, regular or decaf* 3.00
Espresso 3.00
Cappuccino, Latte Or Mocha 4.00
Mighty Leaf Hot Tea *organic breakfast, earl grey, green tea tropical, african nectar, chamomile citrus, mint mélange* 4.00

Lunch

Antipasti

Bruschetta *grilled country bread, fresh tomato, basil, garlic, olive oil, parmesan* 7.00
Insalata Mista Gorgonzola *mixed seasonal greens, balsamic vinaigrette, gorgonzola cheese, caramelized walnuts* 8.00
Insalata Di Cesare *hearts of romaine, anchovies, garlic croutons, shaved parmesan* 8.00
Radicchio Alla Griglia *warm radicchio salad, sweet corn, goat cheese, citrus vinaigrette* 7.00
Zuppa Vongole *creamy clam chowder* 7.00
Minestra Di Verdura *classic vegetable soup* 7.00
Calamari Fritti *lightly fried squid, lemon, chipotle garlic aioli* 10.00
Cozze Bollito *pei mussels, garlic, fresh herbs, white wine sauce* 7.00
Torte Di Granchio *dungeness crab cakes, cucumber, micro greens, lemon caper butter sauce* 12.00

Pizze

Verdi *baby spinach, red onion, pesto sauce, mozzarella cheese* 12.00
Margherita *fresh tomato, basil, marinara sauce, mozzarella cheese* 11.00
Rustica *spicy italian sausage, mushroom, bell pepper, marinara sauce, mozzarella cheese* 12.00

Panini

Panini Served On Freshly Baked Foccacia Bread with Choice of French Fries, Cup of Soup or Salad

Panino Con Pollo *grilled chicken, tomato, red onion, lettuce, bacon, aioli* 11.00
Panino Grosso *sliced prosciutto, roasted bell pepper, basil, fresh mozzarella cheese* 12.00
Panino Funghi *portobello mushroom, caramelized onion, sundried tomato, goat cheese* 13.00

Secondi

Fettucini Alfredo *classic alfredo cream sauce, parmesan cheese* 12.00
Linguini Vongole *sautéed manila clams, fresh oregano, white wine sauce* 14.00
Fusilli Mediterranean *seared chicken breast, eggplant, olives, marinara sauce, ricotta salata cheese* 14.00
Linguini Frutti Di Mare *rich tomato seafood stew, green olives, fresh herbs, white wine* 15.00
Spaghetti Bolognese *hearty meat sauce, fresh herbs, shaved parmesan* 14.00
Ravioli Con Granchio *dungeness crab filled ravioli, herb butter broth, parmesan cheese* 15.00
Pollo Alla Parmigiana *seared chicken breast, parmesan crust, marinara sauce, mozzarella cheese, roasted rapini* 16.00
Merluzzo Arrosto *pan roasted rock cod, yukon potatoes, rapini, pinenuts, lemon caper butter sauce* 21.00

Dinner

Antipasti

Bruschetta *grilled country bread, fresh tomato, basil, garlic, olive oil, parmesan* 8.00
Insalata Mista Gorgonzola *mixed seasonal greens, balsamic vinaigrette, gorgonzola cheese, caramelized walnuts* 8.00
Insalata Di Cesare *hearts of romaine, anchovies, garlic croutons, shaved parmesan* 8.00
Zuppa Vongole *creamy clam chowder* 7.00
Minestra Di Verdura *classic vegetable soup* 7.00
Calamari Fritti *lightly fried squid, lemon, chipotle garlic aioli* 11.00
Cozze Bollito *pei mussels, garlic, fresh herbs, white wine sauce* 9.00
Seafood Antipasti *skillet roasted mussels, clams, tiger prawns, lemon, garlic butter sauce* 14.00
Torte Di Granchio *dungeness crab cakes, cucumber, micro greens, lemon caper butter sauce* 13.00

Primi

Verdi Pizza *baby spinach, red onion, pesto sauce, mozzarella cheese* 13.00
Margherita Pizza *fresh tomato, marinara sauce, mozzarella cheese, basil* 12.00
Rustica Pizza *spicy italian sausage, mushroom, bell pepper, marinara sauce, mozzarella cheese* 13.00
Fusilli Mediterranean *seared chicken breast, eggplant, olives, marinara sauce, ricotta salata cheese* 17.00
Fettucini Frutti Di Mare *rich tomato seafood stew, green olives, fresh herbs, white wine* 19.00
Spaghetti Bolognese *hearty meat sauce, fresh herbs, shaved parmesan* 16.00
Ravioli Con Granchio *dungeness crab filled ravioli, herb butter broth, parmesan cheese* 17.00

Secondi

Branzino Al Zafferano *roasted seabass, pinenut crust, whipped potatoes, saffron cream sauce* 23.00
Tonno Alla Tuscana *seared tuna, tuscan white beans, escarole, pancetta, whole grain mustard vinaigrette* 21.00
Merluzzo Arrosto *pan roasted rock cod, yukon potatoes, rapini, pinenuts, lemon caper butter sauce* 21.00
Gamberi Fra Diavolo *wood oven roasted jumbo prawns, spicy tomato compote, fried polenta cake* 22.00
Chicken Marsala *seared chicken breast, whipped potatoes, baby spinach, marsala mushroom sauce* 19.00
Bistecca *grilled herbed rib eye, whipped potatoes, creamy spinach, port wine sauce* 25.00
Garetto Di Agnello *braised lamb shank, whipped potatoes, garlic gremolata* 24.00

Dolci

Tiramisu *rum- soaked sponge cake with mascarpone cream* 7.50
Pear Bread Pudding *fresh pear, raisins, bourbon caramel sauce* 6.95
Panna Cotta *topped with berries in ruby port* 6.50
Trio Of Sorbets *seasonal fruits of sorbet with house made biscotti* 5.95
Gelato *chocolate or vanilla* 5.95
Chocolate Tort *with raspberry sauce and vanilla gelato* 7.50
Biscotti *house made pistachio and chocolate italian cookies* 4.95

Espresso Bevande

Tuscan Cappuccino *baileys, brand and amaretto* 9.50
Ciao Bella *godiva chocolate and grand marnier* 9.50
Italian *sambuca and espresso* 9.50
Firenze *amaretto, kahlua and cream* 9.50
Non-Alcoholic *cappuccino, latte, mocha* 3.95
Mighty Tea Leafs *organic earl grey, green tea tropical, organic breakfast chamomile citrus, africa nectar, organic mint melange* 3.95

Specialty Cocktails

Harvest Moondrop *house infused harvest spiced rum, white peach puree, lime squeeze* 10.00
Maker's Manhattan *maker's mark bourbon, sweet vermouth, angostura bitters* 11.00
Negroni *plymouth gin, campari, sweet vermouth* 11.00
Strawberry Ginger Drop *tanqueray 10 gin, domaine de canton ginger liqueur, fresh strawberry, fresh lime juice, sugar rim* 12.00
Raspberry Citrus Crush *absolut citron vodka, fresh lemon & orange juice, fresh raspberry* 10.00
Woodford Sazerac *woodford reserve bourbon, peychaud's bitters, absinthe* 13.00
Mediterranean Margarita *partida blanco tequila, cointreau, fresh lime juice, house infused syrup* 13.00
Cucumber Mint Martini *belvedere vodka, fresh lime juice, mint leaves, cucumber* 12.00
10 Cane Caipirissima *10 cane rum, acai juice, fresh lime, club soda* 13.00
San Francisco Rum Punch *flor de cana 7 yr rum, fresh lime juice, angostura bitters, pineapple juice* 10.00
Winter Smash *bulleit bourbon fonseca bin 27 port, mint, maple syrup and angostura bitters* 12.00
Rush Hour *russian standard vodka, coffee liqueur, espresso, sprinkled with cinnamon & sugar* 12.00
Agave Honey *cuervo traditional reposado tequila, cranberry, grapefruit, honey & fresh ginger* 12.00

Draft Beers $6

Peroni
Blue Moon
Anchor Steam
Sam Adams Seasonal
Fat Tire

Imported Beers

St. Pauli's Girl *non-alcoholic* 5.
Moretti 6.
Moretti Dark 6.
Guinness 6.00
Pilsner Urquell 6.00
Heineken 6.00
Amstel Light 6.00
Corona 6.00

Domestic Beers $5

Budweiser
Bud Light
Sierra Nevada

Happy Hour

Appetizers $5

Calamari Fritti *lightly fried squid, lemon, cocktail sauce, garlic aioli*
Bruschetta *grilled country bread, diced tomato, basil, garlic, olive oil, parmesan*
Pizza Margherita *fresh tomatoes, marinara sauce, mozzarella, basil*
Pizza Rustica *spicy italian sausage, mushrooms, peppers, marinara sauce, mozzarella*

Beer $3

Draft *blue moon*
Bottled *bud, bud light*

Wines $3

Sycamore Lane *cabernet sauvignon chardonnay*

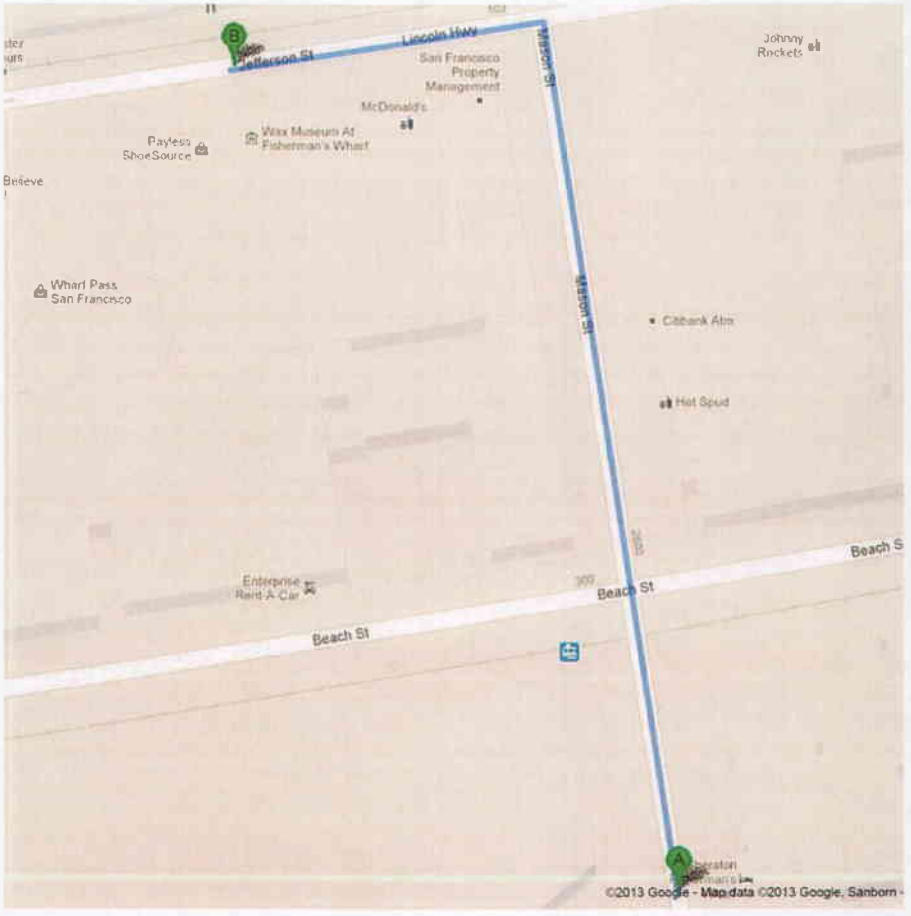
Well Drinks & Cocktail

Vodka, Gin, Scotch, Bourbon, Tequila Or Rum *with choice of mixer* 3.00
Martini, Cosmopolitan, Manhattan 7.

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

BISTRO BOUDIN (SEAFOOD)



1. Head north on Mason St toward Beach St - 0.1 mi .
2. Turn left onto Jefferson St - 187 ft.
3. Destination will be on the right, Bistro Boudin, 160 Jefferson St.

Route Time: 3 minutes.

Bistro Boudin
160 Jefferson St
San Francisco, CA 94133
At Taylor St

415 351-5561
Fax: 415 351-5579

YOUR AD HERE
MenuPages ***PRIME*** Advertising
for more info: www.menupages.com

Starters

Dungeness Crab Cake *roasted corn salad and whole grain mustard aioli* 14.95

Baked Artisan Goat Cheese *garlic roasted tomatoes, pesto and toasted sourdough* 12.50

Fried Calamari *classic with tartar and cocktail sauce* 12.95

Classic Shrimp Cocktail *classic presentation with homemade horseradish cocktail sauce, lemon and garlic croutons* 14.75

Dungeness Crab, Spinach & Artichoke Dip *and creamy parmesan with toasted sourdough* 13.50

Mussels Marniére *garlic, white wine and sourdough* 14.95

Garlic Fries With Parsley *our thin-cut fries with gilroy garlic* 6.95

Chilled Oysters *on the half shell with mignonette sauce* (6) 16.00 (12) 30.00

BBQ Oysters *bistro bbq butter* (4) 12.00

Oysters Rockefeller *spinach, onion, pernod, butter, pecorino cheese and sourdough bread crumbs* (4) 12.00

Manila Clams *braised with white wine, crispy pancetta, parsley and garlic butter* 13.95

Mission Street Shrimp Cocktail *san francisco tradition, spicy with cilantro, avocado, lime and tortilla crisps* 14.95

Dungeness Crab Cocktail *on a bed of butter lettuce with homemade horseradish-cocktail sauce* 14.95

Soup & Salads

Boudin Sourdough Breadbowl *choice of traditional clam chowder or crab & corn bisque* petite 8.50 13.95

French Onion Soup *gratinéed with emmenthal cheese and sourdough croutons* 10.25

Iceberg Wedge Salad *homemade blue cheese dressing, crisp applewood smoked bacon, grated egg and tomatoes* 10.95

Bistro Shrimp Salad *grilled shrimp, grilled avocado, chopped romaine, orange supremes, red peppers, jalapeño and cilantro vinaigrette* 15.95

Smoked Chicken Waldorf *smoked chicken, apples, celery, walnuts, dried cranberries, swiss cheese with sweet and sour mustard dressing* 15.95

Caesar Salad *romaine lettuce, parmesan cheese and our own sourdough garlic croutons* 8.95

Herbed Greens *organic greens, cherry tomatoes and our black pepper-shallot vinaigrette* 8.95

Cobb Salad *grilled chicken, hard boiled egg, smoked bacon, tomato, avocado, blue cheese and crisp romaine in a cobb salad vinaigrette dressing* 15.95

Dungeness Crab Louis *fresh picked dungeness crab with deviled eggs, avocado, bibb lettuce, asparagus, ripe tomatoes and louis dressing* 26.95

Grilled Vegetable Harvest *marinated butternut squash, grilled zucchini, asparagus and radicchio with cherry tomatoes, capers, almonds and salsa crudo* 19.95

Dungeness Crab Feast $34.95

Freshly Steamed And Served With Our Famous Sourdough Bread, Linguine With Slow Roasted Tomato Arrabiata Sauce And Caesar Salad.

Meat & Poultry

We Feature Aged Black Angus Beef From Creekstone Farms.

Red Wine Braised Beef Stew *slow braised beef shortrib topped with dijon mustard with glazed carrots, pearl onions and creamy garlic mashed potatoes* 20.95

Organic Free Range Chicken 'Frites' *our signature half boneless chicken roasted under a brick with natural jus and our thin cut fries* 20.95

Simply Grilled Flat Iron Steak *rubbed with sea salt, black pepper and chargrilled with parsley-garlic butter, asparagus and creamy garlic mashed potatoes* 23.95

Charred 14oz Ribeye *smoked onion butter and watercress with blue cheese scalloped potatoes - or- simply grilled with salt & pepper and grilled jumbo asparagus* 29.95

Pasta

Dungeness Crab Mac & Cheese *cheddar cheese, fresh cream and freshly picked dungeness crab with buttered sourdough bread crumbs* 21.50

Linguine And Clams *manila clams, rapini, garlic and shaved parmesan* 21.95

Roasted Mushroom Risotto *fresh organic mushrooms slow braised with white wine, shallots and thyme. drizzled with black truffle essence and shaved pecorino romano* 18.50

Angel Hair Pasta With Herb Grilled Shrimp *vine ripened tomato arrabiata and garlic* 22.95

Sourdough Gnocchi Al Pesto With Lobster *fresh homemade sourdough potato gnocchi in creamy pesto sauce with citrus zest and chives* 24.95

Sandwiches

Served With French Fries.

Sourdough Baguette Burger *creekstone farms beef, toasted sourdough baguette, lettuce, tomato, onions and choice of cheese* 14.95

Classic Chicken Club *toasted sliced sourdough, grilled chicken, avocado, bacon, lettuce, tomato and basil mayonnaise* 14.95

Char Grilled Ribeye Sandwich *on a french baguette with melted brie and arugula* 18.95

Dungeness Crab Cake Sandwich *toasted sourdough, lettuce, tomato, avocado and lemongrass mayonnaise* 18.95

Hot Smoked Salmon Club *sliced sourdough, lettuce, tomato, avocado, bacon and basil mayonnaise* 16.95

Sourdough Pizza

Featuring Our Homemade Sourdough Thin Crust

Margherita *fresh mozzarella, basil and tomato sauce* 12.95

Pepperoni *tomato sauce, roasted peppers, sweet onions and grilled scallions* 13.95

Dungeness Crab & Shrimp *fresh pesto, mozzarella and tomato confit* 15.95

Fish & Seafood

At Bistro Boudin, We Believe In A Close Relationship With Our Local Purveyors. We Try Hard To Ensure That All Our Seafood Is From Safe Ecologies And Sustainable Sources.

Sourdough Tortilla Tacos *grilled rock cod, dungeness crab or spicy grilled shrimp. avocado, red and green cabbage, crema fresca, cilantro, pico de gallo and roasted tomato salsa* (3) 14.95

Fish & Chips *anchor steam beer batter, cole slaw and homemade tartar sauce with our thin cut fries* 19.95
substitute with jumbo shrimp 24.95

Brown Buttered Trout *crispy skinned with capers, lemon, brioche crumbs and sauteed green beans* 21.95

Crispy Skinned Sea Bass *gnocchi, crispy bacon, brussel sprouts and olives in lemon chive velouté* 26.95

Pan Roasted Petrale Sole *white wine and lemon-butter sauce with garlic mashed potatoes and sauteed spinach* 24.95

Wild Caught Halibut *pan roasted with crisp polenta, sauteed spinach and a slow roasted tomato broth* 26.95

Grilled Salmon Al Tagine *clams, spinach, cherry tomatoes, morroccan olives, capers and white wine sauce with a sourdough crostini* 26.95

Cioppino *dungeness crab, shrimp, calamari, mussels, and fish simmered in a spicy saffron-tomato broth* 32.95

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

YOUR AD HERE
MenuPages ***PRIME*** Advertising
for more info: www.menupages.com

Sides

Cheddar "Mac & Cheese" 7.95
Blue Cheese Scalloped Potatoes 6.95
Sauteed Green Beans *lemon, shallots and buttered almonds* 6.95
Garlic Mashed Potatoes 6.95

Kid's Menu

Must Be 12 Years Or Under. Includes: Soft Drink Or Milk.

Grilled Cheese *french fries* 7.95
Butter Noodles *with parmesan* 7.95
Mac & Cheese 8.95
Cheese Pizza 8.95
Fish And Chips 9.95
Hamburger *french fries* 9.95
add cheese 0.50
Grilled Chicken *mashed potatoes and carrot sticks* 9.95
Grilled Fish *rock cod, mashed potatoes and carrot sticks* 10.95
Kid's Sundae *vanilla gelato, chocolate sauce and whipped cream* 1.95
Substitute Fresh Berries $1.

Desserts

Sourdough Crust Apple Pie *fuji apples, caramel sauce and cinnamon gelato* 7.95
Chocolate Lava Cake *callebaut chocolate, crème anglaise and vanilla gelato* 8.50
Sourdough Upside-Down Bread Pudding *fresh baked with caramel sauce, vanilla whipped cream and berries* 6.95
Assorted Berries *with crème anglaise* 5.95
Gelato *vanilla, cinnamon or pistachio, served with a crispy wafer cookie* 6.95
Vanilla Crème Brulee *with a crispy wafer cookie* 6.95

Oyster Bar

Served With Mignonette Sauce. (Cocktail Sauce Available Upon Request)

Raw Oysters

(6) / (12).

Hama Hama *hood canal, wa* 16.00 30.00
Marin Miyagi *tomales bay, ca* 16.00 30.00
Kumamoto *humboldt bay, ca* 18.00 32.00

Baked Oysters $12

(4).

Barbeque *bistro bbq butter*
Traditional Rockefeller *spinach, onion, pernod, butter, pecorino and sourdough bread crumbs*

Draft Beer $5.95

Blue Moon *hefeweizen*
Peroni *lager*
Anchor Steam
Fat Tire

Bottled Beer

Corona 5.50
Heineken 5.50
Karl Strauss *red trolley ale* 5.50
Lagunitas, IPA 5.50
Sapporo 5.50
Sierra Nevada 5.50
Clausthaler *non-alcoholic* 5.50
Budweiser 4.95
Bud Light 4.95
Coors Light 4.95

Specialty Drinks $10

Ruby Red Cosmo *finlandia grapefruit vodka, cointreau, fresh lime and cranberry juice*
Basil Gimlet *bombay sapphire gin shaken with fresh basil leaves and lime juice*
Boudin Bloody Mary *stolichnaya vodka, secret boudin bloody mary mix, and all the fixins*
The Wooler *woodford reserve bourbon and diet coke on the rocks*
Bistro Margarita *el jimador tequila, cointreau and sweet & sour on the rocks with a salt rim*
Poma-Rita *our bistro blend with pomegranate juice*
Strawberry-Rita *our bistro blend with fresh strawberry puree*
Citrus Breeze *finlandia tangerine vodka, orange and cranberry juices and a splash of sprite*
Spiced Cider-Tini *sailor jerry rum, apple juice and simple syrup with a pinch of cinnamon*
Mai Tai *bacardi rum, amaretto, orange and pineapple juices and float of meyer's dark rum*
Blackberry Lemonade *stolichnaya vodka, blackberry simple syrup, sweet & sour and sprite*
Perfect Mojito *two ways: bacardi superior rum muddled with mint leaves, fresh lime juice and cane sugar or bacardi dragonberry rum and fresh strawberries*

White Wines By The Glass

Sparkling

Kenwood "Yulupa" Cuvée Brut *california, nv* 9.00

Pinot Grigio

Caposaldo *veneto, italy, 2011* 9.00

Riesling

Pacific Rim *columbia valley, 2010* 8.00

Sauvignon Blanc

Geyser Peak *california, 2011* 9.00
Joel Gott *california, 2011* 10.00
Matanzas Creek *sonoma county, 2011* 12.00

White Zinfandel

Buehler *napa, 2011* 8.00

Chardonnay

Bistro House White *california, 2010* 8.00
Geyser Peak *alexander valley, 2010* 10.00
La Crema *monterey, 2010* 12.00

Red Wines By The Glass

Pinot Noir

Hahn Winery *california , 2011* 9.00
Cambria "Julia's Vineyard" *santa maria valley, 2009* 12.00

Merlot

Irony *napa, 2009* 9.00
Geyser Peak *alexander valley, 2006* 10.00

Shiraz

Peter Lehmann *barossa, australia, 2008* 8.00

Zinfandel

Xyzin *california, 2009* 9.00

Red Blend

Geyser Peak "Uncensored" *california, 2010* 10.00

Cabernet Sauvignon

Bistro House Red *california, 2011* 8.00
Geyser Peak *alexander valley, 2008* 11.00
Hess "Allomi" *napa valley, 2009* 13.00

Sweet Wines By The Glass

Dessert Wine

Roche, Late Harvest Chardonnay *carneros, 2009* 10.00
Pacific Rim, Vin De Glaciere Riesling *columbia valley, 2010* 12.00

Port

Fonseca "Bin 27", NV 8.00
Warre's Otima 10 Year Tawny, NV 10.00
Taylor Fladgate Fine Ruby Porto, NV 12.00

Geyser Peak Wines By The Glass

Winery.

Sauvignon Blanc *california, 2011* 9.00
Chardonnay *alexander valley, 2010* 10.00
Red Blend "Uncensored" *california, 2010* 10.00
Merlot *alexander valley, 2006* 10.00
Cabernet Sauvignon *alexander valley, 2008* 11.00

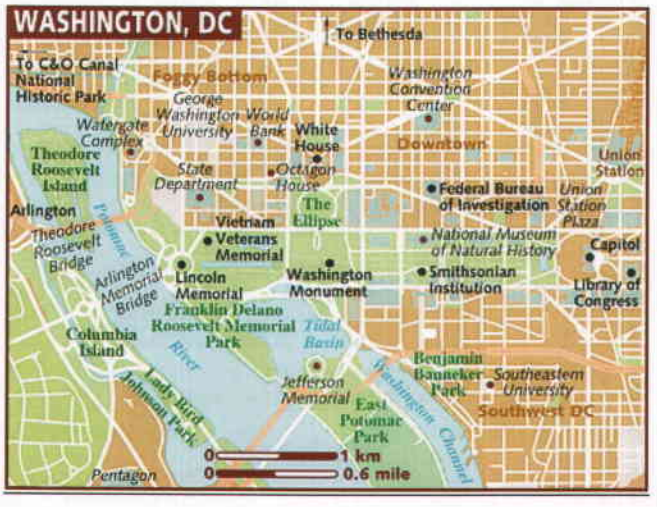
Geyser Peak Has Been At The Forefront Of Quality Wine Production And Today Is One Of The Most Award-Winning Wineries In Sonoma County, Having Been Named "Winery Of The Year" By Wine & Spirits Magazine An Unprecedented 9 Times Since 1993.

Menu Items and Prices subject to change. Information related to this restaurant is provided solely for informational purposes only and is not an endorsement or guarantee by MenuPages.com or any Listed Restaurant.
© 2009 Slick City Media, Inc. www.MenuPages.com

MENUPAGES

ENTERTAINMENT OPTIONS

WASHINGTON, D.C.



Site Seeing in Washington, DC

To best enjoy Washington's most celebrated monuments, the local trolley tours help you navigate through the city to each of the sites. After visiting one of the sites, you can get back on the trolley and move on to the next sites. Trolley tours are available both during the day time, as well as at night.

Washington Site Seeing Trolley Tours Stops include:
National Mall and Downtown Loop: Union Station - U.S. Capitol/Supreme Court - Air and Space Museum/Museum of the American Indian - Jefferson Memorial - FDR Memorial - Lincoln Memorial/Vietnam Memorial/Korean Memorial/WWII Memorial (Transfer to Arlington Cemetery Shuttle) - Museum of American History/Washington Monument - Museum of Natural History/National Archives - Washington Welcome Center (Transfer Station - Mall/National Cathedral) - White House Visitors Center

Monuments by Moonlight Tour Stops include: the Washington Monument, Thomas Jefferson Memorial, Franklin D. Roosevelt Memorial, Korean War Memorial, Abraham Lincoln Memorial, Vietnam Memorial and the newly-dedicated National World War II Memorial.

Additional sites worth visiting:

Decatur House 748 Jackson Pl. NW, Washington, DC; Tel: 202-842-0920; OPEN: Tues.-Sat. 10-5, Sun. noon-4; tours every hour

International Spy Museum 800 F Street NW, Washington, D.C.

National Air and Space Museum Independence Avenue at 6th Street, SW, Washington, DC 20024

National Zoological Park 3001 Connecticut Ave NW, Washington, DC

PAKISTAN
BANKING INFORMATION TECHNOLOGY MODERNIZATION REVERSE TRADE MISSION
FEBRUARY 4 - 13 • 2013
WASHINGTON DC • NEW YORK • CALIFORNIA

Suggested Restaurants in Washington, DC – American & Contemporary Cuisine

Bangkok Joe's
3000 K St. NW
(Thomas Jefferson St.)
Washington, DC
202-333-4422

Butterfield
Garfinkle's
600 14th St. NW,
Washington, DC 20005
Tel: 202-BU9-8810

Chopsticks
1073 Wisconsin Ave. NW
(M St.)
Washington, DC
202-338-6161

CityZen
Mandarin Oriental,
Washington DC
1330 Maryland Ave. SW
Washington, DC 20024
202-787-6006

Daily Grill
1200 18th Street NW
Washington, DC 20036
202-822-5282

DC Coast
1402 K St. NW
Washington, DC 20007
202-216-5988

Haad Thai
1100 New York Ave. NW
(bet. 11th & 12th Sts.)
Washington, DC
202-682-1111

Meiwah
1200 New Hampshire Ave. NW, Washington,
D.C. 20036
202-833-2888

Nora
2132 Florida Ave. NW
Washington, DC 20008
202-462-5143

Palena
3529 Connecticut Ave. NW
Washington, DC 20008
202-537-9250

Perrys
1811 Columbia Rd. NW
(Biltmore St.)
Washington, DC
202-234-6218

Restaurant Kolumbia
1801 K St. NW
Washington, DC 20006
202-331-5551

TenPenh
1001 Pennsylvania Ave. NW
(10th St.)
Washington, DC
202-393-4500

Uni Sushi Place
2122 P Street, N.W.
Washington, DC 20037
202-833-8038

Zentan
1155 14th St. NW
(Masschusettes Ave. NW)
Washington, DC
202-379-4366

Suggested Restaurants in Washington, DC – Halal (Zebihah)

Red Toque Café
"Indian - Pakistani dine-in, carry out, and delivery restaurant that serves fresh halal kabobs and curry dishes, in addition to vegetarian and vegan dishes. We make our bread (naan) in-house. We are open from 11 am to 10 pm."
1701 6th Street NW
Washington, DC 20001
1003 Wisconsin Avenue NW
Washington, DC 20007

Afghan Kabob House
"'Honest food' at an 'honest price' is the deal at this Arlington Afghani 'quick-service' eatery where 'wonderful' kebabs, 'interesting rice options' and other 'excellent' eats trump its 'hole-in-the-wall' appearance; night owls note that 'it's one of the few late-night spots in the [Courthouse] area' on Friday and Saturday (till 3 AM)."
2045 Wilson Boulevard
Arlington, VA 22201

Kabob Palace
"'People in the know' come to this Arlington Mideasterner for 'authentic' kebabs of 'unfailing' quality plus an 'excellent' lunch buffet at affordable prices; it's 'always busy' despite 'no decor' and 'informal' service, bringing 'all ages, races and creeds together in pursuit of awesome food.'"
2318 South Eads Street
Arlington, VA 22202

Figs Lebanese Café
"Welcome to Figs Lebanese Café! Not your traditional Lebanese restaurant, Figs offers a wide selection of healthy comfort foods adapted from a variety of international cuisines with a Lebanese and Moroccan twist. Everything is made fresh daily and our specials are seasonally influenced. Many of our delicious dishes are vegan- and vegetarian-friendly as well. This is a great neighborhood spot for healthy, flavorful foods."
4828 MacArthur Blvd NW
Washington, DC 20007

Istanbul Café
"Here at Cafe Instanbul Restaurant in Washington DC, we specialize in Middle Eastern and pizza meals. We offer a relaxed, inviting ambience where you can feel at home and enjoy your food with family and friends. Our foods are prepared with the finest and freshest ingredients that set us apart from our competition. Appetizers, soups, salads are great starters. We also offer delicious bistro pitas filled with falafel, turkey, chicken hummus with veggies, as well as vegetarian pitas. Our delightful kebabs are our signature platters made with either lamb, beef, chicken, seafood or veggies. Our bistro pizzas are a mainstay and are prepared right in our kitchen. Our easy online ordering system and delivery service will bring your meal right to your door."
2001 L Street NW, Suite 100
Washington, DC 20036

Ravi Kabob House
"'Mouthwatering', 'wonderfully tasty' kebabs with 'all the fixin's' rave devotees of these Greater Arlington Pakistani joints practically across the street from one another; 'decor and ambiance are non-existent', and service is only fair, but no one argues as it's so 'cheap', with 'quality' that's 'much higher than the cost'; P.S. cash only."
305 North Glebe Road
Arlington, VA 22203

East West Grill
"Located in the heart of the Rosslyn-Ballston corridor, in one of Northern Virginia's trendiest neighborhoods, East West Grill helps keep this neighborhood real with Pakistani-style kabobs. You'll get generous helpings of veggie side dishes along with your chapli kebabs, but it's the fresh naan that is a real standout here."
2721 Wilson Blvd
Arlington, VA 22201

NEW YORK, NY

New York was briefly the U.S. capital from 1789-90 and was state capital until 1797. By 1790 it was the largest U.S. city, and the opening (1825) of the Erie Canal, linking New York with the Great Lakes, led to even greater expansion. In 1898 a new charter was adopted, making the region now known as Greater New York, a metropolis of five boroughs.

Major Attractions

Empire State Building
Tired of staring up at New York City skyscrapers? Check out the view of New York City from atop the Empire State Building. You can avoid waiting in the ticket line for the Empire State Building if you buy your tickets online in advance.

Statue of Liberty
The Statue of Liberty was a gift to the United States in honor of the friendship established during the French Revolution. The Statue of Liberty has become an American symbol of freedom and welcome to the immigrants who come to the USA looking for a better life.

Grand Central Terminal
Renovations since its opening in 1913 have turned Grand Central into more than just a hub for transportation -- there are shops, dining and more available to visitors. There are group tours available, as well as free tours for individuals on Wednesdays and Fridays.

Rockefeller Center
The Rockefeller Center in midtown Manhattan, is known for its Christmas tree, ice skating, Top of the Rock Observation Deck, Radio City Music Hall and numerous shopping and dining opportunities. Rockefeller Center is a great destination for visitors any time of year.

Ellis Island Immigration Museum
The Ellis Island Immigration Museum offers visitors a fascinating look into the immigrant experience. Interactive exhibits, walking tours and movies reveal the hardships and challenges faced by immigrants passing through Ellis Island.

Staten Island Ferry
The Staten Island Ferry is a free ferry from lower Manhattan to Staten Island, used by commuters and tourists wanting a view of the harbor and the Statue of Liberty.

American Museum of Natural History
Since opening to the public in 1869, the American Museum of Natural History has evolved and grown. In addition to the Rose Center planetarium and regular exhibits, the American Museum of Natural History hosts a revolving series of new exhibits, so there is always something new to see.

Central Park
Central Park has offered a welcome escape from the concrete jungle of New York City for over 150 years. Take a walk, a boat ride or just enjoy a picnic in Central Park and discover for yourself why Central Park is so popular.

Metropolitan Museum of Art
Over 2 million works of art from around the world and throughout history are housed at the Metropolitan Museum of Art. The Metropolitan Museum of Art is an iconic art museum that is well worth a visit.

The Museum of Modern Art (MoMA)
Founded in 1929 as the first museum dedicated entirely to contemporary art, the MoMA is host to an impressive collection of modern artistic efforts. From painting and sculpture to film and architecture, the Museum of Modern Art's diverse collection has something for everyone.

United Nations
Behind the 192 waving flags representing the member countries stands a 39 story monolith known as the Secretariat Building. Along with the General Assembly Building, conference buildings and Dag Hammarskjold Library, the United Nations attempts to maintain peace, protect human rights and promote development throughout the world on a 6 block stretch of land along the East River. When you enter the gates of the United Nations, you're actually leaving New York City. These 18 acres are an international territory belonging to all the member countries.

Suggested Restaurants in New York – American & Contemporary Cuisine

Aldea
After toiling anonymously at places like Wallsé and Tocqueville, journeyman chef George Mendes steps into the spotlight with an Iberian-accented menu.
31 W. 17th Street
212-675-7223

Artichoke
The restaurant famous for its artichoke topped, charred bottom slices has spun into three locations, each serving riffs on the original menu.
111 MacDougal Street/328 E. 14th Street
646-278-6100/212-228-2004

Brother Jimmy's BBQ
A Manhattan mini-chain turns out tasty barbeque in an earsplitting, frat-happy setting.
116 E. 16th
212-673-6465

Chat 'n Chew
Don't tell mama, but Chat 'n Chew's home cookin' is better than anything that ever came out of her kitchen.
10 E. 16th Street
212-243-1616

Chipotle
Award-winning decor and a fixation for freshness only add to these famous foil-wrapped burritos.
864 Broadway/117 E. 14th Street
212-253-7860/212-260-0641

Edo Japanese Restaurant
A budget gem with classic and fusion sushi rolls.
9 E. 17th Street
212-989-2938

Express Manna Kitchen
Take your donburi or ginseng chicken soup for delivery or to go at this Korean fast-food joint.
28 E. 18th Street, #4
212-228-1044

Flavaboom
A high-design frozen yogurt (fro-yo) shop that boasts ten flavors and at least forty toppings.
600 Sixth Avenue (Avenue of the Americas)
212-414-0010

Hollywood Diner
The only diner in town where you can order a Howard Stern with extra cheese.
574 Sixth Avenue (Avenue of the Americas)
212-691-8465

Laut
There's little opportunity to order wrong at this Malaysian-Thai-Singaporean refuge.
15 E. 17th Street
212-206-8989

Maoz Vegetarian
Union Square falafels are being challenged with Maoz Vegetarian, the first New York outpost of an Amsterdam chain.
38 Union Square East
212-260-1988

Rainbow Falafel & Shawarma
The herb-tinged falafel and fresh fixings draw lunchtime throngs.
26 E. 17th Street
212-691-8461

Republic
This once scene-y Thai spot has become a neighborhood staple.
37 Union Square West
212-627-7172

Suggested Restaurants in New York – Halal (Zebihah)

Mamoun's Falafel Restaurant
Situated in the heart of Greenwich Village in New York City, Mamoun's Falafel has been serving high quality Middle Eastern Food since it first opened its doors in 1971. It is the oldest falafel restaurant in New York and one of the first Middle Eastern establishments in the U.S.
119 MacDougal Street/22 St. Mark's Place
212-674-8685/212-387-7747

Lahori Kabab Restaurant
Lahori Kabab is a Halal Pakistani cuisine located in a convenient place in Manhattan a short distance to the Manhattan mall and the Empire State Building.
124 Lexington Avenue
212-400-1166

Punjab Palace
Punjab Palace is an Indian restaurant that is open 24 hours.
11 W. 30th Street
646-454-1369

Pars Grill House & Bar
Enjoy Pars Grill House in the heart of New York City, a restaurant inspired by the Persian culture and heritage. All signs suggest that this Chelsea Persian with lots of "savory dishes", weekend belly dancing and "Farsi being spoken" is a bona fide "real deal"; "reasonable" tabs offset iffy service and "not particularly comfortable" digs.
249 W. 26th Street
212-929-9860

Larosh
Larosh's buffet serves Indian food, salad bar, desserts, soda, tea and more. You pay only $9.99 for all you eat. This restaurant is owned by Muslims and serves only halal food.
37 E. 29th Street
212-213-3311

Gourmet Palace
Dine-in Halal Indian and Pakistani food.
13 W. 29th Street
212-213-1314

SILICON VALLEY AND SAN FRANCISCO, CA

At just 49 square miles, San Francisco packs as much into its tiny water-bound area as most cities three times its size. The city was established in the mid 1700s by Spanish explorers, who sailed through the Golden Gate, eventually displacing the Ohlone Indian population who had lived here for hundreds of years. Originally a sleepy port town called Yerba Buena ('good herb'), things really got spirited in the 1840s when gold was discovered in the foothills of California. The population swelled and the city, now San Francisco, became a veritable den of iniquity, teeming with disillusioned prospectors, wayward sailors, and put-upon immigrants. This chapter in history can be relived by strolling the streets of Chinatown, along Grant Avenue or Stockton Street between Pine Street and Pacific Avenue. Stop in at the Chinese Culture Center (750 Kearny Street, CA 94108, Tel: 415-986-1822, www.c-c-c.org) for guided tours. Chinatown's next-door neighbor is North Beach, where the Barbary Coast history can be traced along Columbus Avenue and great coffee and Italian food can be had at nearly any café or restaurant.

After being shaken (and burned) to the ground by the great earthquake of 1906, San Francisco began to take its modern shape. Many of its most functional additions have become its most popular attractions. The Golden Gate Bridge, at the northern edge of the Presidio, was completed in 1937 and is visited by some nine million people annually. East of the bridge in the middle of the Bay, and flanked by the Bay Bridge, is Alcatraz (Golden Gate National Recreation Area, CA 94123, Tel: 415-705-5555), the infamous prison but now a major visitor draw and worth the quick boat trip from Fisherman's Wharf to see it.

Beyond the charm of the major attractions, San Francisco's cultural cadre has much to brag about. Among them are the Museum of Modern Art (151 Third, CA 94103, Tel: 415-357-4000) and the Palace of the Legion of Honor (100, 34th Ave and Clement St, CA 94122, Tel: 415-863-3330), which has a world-class collection and hosts top-notch exhibitions, and the Asian Art Museum (200 Larkin St, CA 94102, Tel: 415-581-3500), which has one of the largest collections of its kind in the Western world.

Shopping

Union Square (Geary and Stockton streets) is top dog for San Francisco shopping. It's retail heaven, featuring flagship stores like Macy's (Tel: 415-397-3333), Neiman Marcus (Tel: 415-362-
The Embarcadero Center (Sacramento Street between Battery and Drumm Streets, CA 94111, Tel: 415-772-0550) offers an urban shopping adventure, complete with bars and cafes for retail refueling. Less crowded and a little more hip are upper Grant Avenue in North Beach and Hayes Street between Laguna Street and the Civic Center, where you'll find host of trend-setting alternative retailers.

Restaurants – American & Contemporary Cuisine

San Francisco is renowned for trend-setting fare and for making the reputation of many a chef. Cuisine here takes its cues from the abundance of fresh ingredients within ready reach. 'California Cuisine' was born at Alice Waters' restaurant in Berkeley but lives richly now on the other side of the bay at such places as Zuni Cafe (1658 Market St, CA 94102, Tel: 415-552-2522) and Globe (290 Pacific St, CA 94111, Tel: 415-391-4132). The city's extensive Asian influence can be found at the many dim-sum parlors – one of the best is Yank Sing (101 Spear St, Tel: 415-957-9300). Great sushi is nearly incidental to the charged atmosphere at the Marina District's Ace Wasabi (3339 Steiner St, CA 94123, Tel: 415-564-0903). For a mellower mood and perfect sashimi head to the Sunset District for Ebisu (1283 9th Avenue, CA 94122, Tel: 415-566-1770). Italian food is not limited to North Beach but if you are there do stop in for the lasagna at Tommaso's (1042 Kearny Street, CA 94133, Tel: 415-398-9696). The Mission District is home to some of the hottest tables in town and Luna Park (694 Valencia, CA 94110, Tel: 415-553-8584, www.lunaparksf.com) is always reliable and affordable. The best way to eat on the cheap in San Francisco is at a Mexican Tacqueria, preferably in the Mission District – La Cumbre (515 Valencia, CA 94110, Tel: 415-863-8205) is one of the best.

Suggested Restaurants – Halal (Zebihah)

Tikka Masala
Tikka Masala, a taste of India and Pakistan downtown San Francisco and a gateway to superb Indian and Pakistani cuisine, invites you to stop by, sit back, relax, and enjoy your visit.
425 Ellis Street
415-345-1028

Urban Curry
Urban Curry has warm, traditional surroundings and have taken pleasure to ensure that you will enjoy your meals in the most pleasant and atmospheric surroundings. At Urban Curry we emulate the style the elegance and the variety reminiscent of earlier golden ages with a wide ranging menu that would cater to every taste. We only use halal meat and our spices are especially imported from India and Pakistan. We offer an off-menu-international culinary experience.
523 Broadway
415-677-9743

Yemeni's Restaurant
Yemeni Restaurant General Manager Ali Abu Baker grew up with the dream of one day opening a restaurant where his passion for good food and good friends could come together. Ali grew up in Yafa, an area the coastal countryside in Sothern Yemen. As a young man, however, he decided to leave for the land where any dream can become a reality, the United States. In 1973, Ali moved to Costa Mesa, California, where he labored building engines for large ships to earn a living. He bought and revamped a grocery store in New York after all of the years of hard work, just another step closer to realizing his dream. San Francisco was calling, and Ali came to work at a family-owned business. The Yemeni Restaurant opened in early 2010 and has become a favorite amongst the locals. Ali hopes to spread the love and world of authentic Yemeni cuisine to all.
1098 Sutter Street
415-441-8832

Shalimar
Deep in the heart of San Francisco's Tenderloin district, you can find dozens of Halal restaurants within a few blocks radius. Each one of these looks to Shalimar as the one that started it all. It's the reason they refer to this area as the "Tandoor-loin". But despite the proliferation of higher-quality restaurants and their varied styles (everything from Thai to Brazilian and everything in between, this institution keeps packing them in. It's still the favorite of Muslim cabbies everywhere, and intrepid lunchers from Market Street drag their work colleagues here to see how much heat they can stand. Fresh tandoori chicken & naan is doled out by the bagful (most people carry out rather than find a seat in this crowded place), and despite the volume the food still carries high marks.
532 Jones Street/1409 Polk Street
415-928-0333/415-776-4642

Sunrise Deli
In 1984, Sunrise Deli opened on Irving Street in the Sunset District of San Francisco introducing the delicious Middle Eastern cuisine to the Bay Area. Almost three decades later, Sunrise Deli continues to provide high quality Middle Eastern food to the Bay Area. Winning numerous awards along the way, Sunrise Deli has proved to be one of the best Middle Eastern cuisine options the Bay Area has to offer. This San Francisco family owned and operated business uses meat from local ranches and the vegetables are handpicked from local farms. None of their products are frozen or pre-packaged. They also have a large baking operation at the Irving Street location where they bake their famous round sesame bread daily along with spinach pies, Armenian pizzas, and Thyme pizzas. They also bake a variety of sweets that are available daily. Open Monday through Friday, 10 am to 3:00 pm.
89 Belden Place
415-362-2800

Naan 'N Curry
Naan 'N' Curry is a local restaurant chain that specializes in Indian and Pakistani food.
533 Jackson St./336 O'Farrell St./642 Irving St.
415-693-0499/415-346-1443/415-664-7225

Darbar
Located at the corner of Pine and Polk.
1412 Polk Street
415-359-1236

Karachi Classics
The management of Pakwan is proud to present Karachi Classics. Halal Food Standards Alliance of America-certified burgers, fried chicken, sandwiches, wings, wraps, charga, and more!
533 Jones Street
415-776-0160

Tayyibaat Meat & Grill
Afghan/American fusion grill restaurant and Halal meat shop, Tayyibaat provides 100% hormone-free, hand-slaughtered, unstunned chickens, California fresh halal goat, lamb, and beef, kabobs, Mexican cuisine and rotisserie chickens.
366 Golden Gate Avenue
415-913-7012

Oasis Grill
Oasis Grill is a halal Mediterranean restaurant on the corner of Howard and 4th. Located in a house built at the turn of the century, Oasis Grill is a proven Mediterranean favorite of both locals and visitors to San Francisco.
91 Drumm Street/200 4th Street
415-543-3232

Felucca—a Lanteen rigged Italian design fishing boat —Circa 1909

What makes Fisherman's Wharf an exciting place to visit is its thriving historic fishing port. The Wharf is one of those rare locations where history, culture and ethnic pride form a distinctive blend that gives it a strength and vitality all its own.

Al Baccari
Fisherman's Wharf Historian

Crab vendors have harvested their waters since the early 1920s. Above a small bounty of Dungeness crab are caught every season.

Complete schedules of events, coupons, area restaurants and Wharf information at: www.fishermanswharf.org
For more information or to order bulk copies of this brochure, call 415/674-7503
San Francisco Convention and Visitors Bureau: www.sfcvb.org
Hours and rates may change without notice.

©Fisherman's Wharf Merchants Association 2005
All rights reserved.

www.sfport.com

Fisherman's Wharf San Francisco

POINTS OF INTEREST

Accommodations

Argonaut The 4-Diamond Argonaut Hotel, perched on the edge of the Bay at Fisherman's Wharf, features 252 deluxe, luxurious and spacious guest rooms many with views of the Golden Gate Bridge and Alcatraz Island. PH 415/563-0800 TOLL FREE 866/415-0704 FX 415/563-2800 WWW.ARGONAUTHOTEL.COM 495 Jefferson St. D-4

The Best Western Tuscan Inn is a unique boutique Hotel that combines warm European ambiance with exceptional service. While evoking the charm of an Italian countrywide villa, the Hotel is ideally located in the heart of Fisherman's Wharf. PH 415/561-1100 TOLL FREE 800/648-4616 FX 415/561-1199 WWW.TUSCANINN.COM 425 North Point St. G-5

Hilton San Francisco Fisherman's Wharf has the largest guest rooms in the Fisherman's Wharf area. Close to all attractions and amenities, 24 Hour Fitness room and Business Center available, High Speed Internet Access. Full Breakfast Buffet in Vintner's Restaurant. Room Service for all meal periods and Cocktails in Vintner's Lounge. Concierge Service and much more. PH 415/885-4700 TOLL FREE 800/228-8408 FX 415/771-8945 WWW.SANFRANCISCOFISHERMANSWHARFHILTON.COM 2620 Jones St. F-5

Holiday Inn Express Hotel & Suites This 252 room hotel features 36 suites, complimentary breakfast, local phone calls and a location that is convenient to all Fisherman's Wharf attractions. Stay smart at Holiday Inn Express. PH 415/409-4600 TOLL FREE 888/501-7757 FX 415/409-5111 WWW.HIEXPRESS.COM/SFWHARFEXPRESS 550 North Point St. F-5

Holiday Inn Fisherman's Wharf Located adjacent to the Cannery and Anchorage, this full service hotel is in the heart of Fisherman's Wharf, featuring 585 guest rooms, two restaurants, a lounge, an outdoor heated pool, a fitness center and a tour desk. PH 415/771-9000 TOLL FREE 800/WHARF-IT FX 415/771-7006 WWW.HOLIDAY-INN.COM/SFO-FISHERMANS 1300 Columbus Ave. E-4

Hyatt At Fisherman's Wharf Steps from the Cable Car Line, featuring 312 rooms, an outdoor heated swimming pool, jacuzzi, fitness center, concierge, and Knuckles Historical Sports Bar & Grill, serving fresh Krispy Kreme Doughnuts daily. PH 415/563-1234 TOLL FREE 800/233-1234 FX 415/563-2218 WWW.FISHERMANSWHARF.HYATT.COM 555 North Point St. F-5

Radisson Fisherman's Wharf Magnificent location with inspiring waterfront view from many of the 355 guest rooms. Featuring wireless high speed internet, outdoor heated pool, exercise room, and concierge service. Only steps to the water and the most popular attractions The Wharf has to offer, explore the diverse dining and shopping outlets adjoining the hotel. PH 415/392-6700 TOLL FREE 800/333-3333 FAX 415/986-7853 WWW.RADISSON.COM 250 Beach St. G-4

San Francisco Marriott Fisherman's Wharf 285 room hotel within walking distance to the best of the City, just two blocks from the Wharf. Featuring Concierge Services, a full service restaurant, lounge and health club. PH 415/775-7555 TOLL FREE 888/236-2427 FX 415/474-2099 WWW.MARRIOTT.COM/SFOFW 250 Columbus Ave. E-5

Sheraton Fisherman's Wharf 4-Diamond full service hotel just one block from Fisherman's Wharf. Features cozy lobby with fireplace, restaurant, bar, fitness room, rental car desk, outdoor heated pool. High Speed Internet access. PH 415/362-5500 TOLL FREE 800/325-3535 FX 415/ 956-5275 WWW.SHERATONATTHEWHARF.COM 2500 Mason St. G-4

Attractions

Aquarium of the Bay Walk through 300-feet of crystal clear tunnels where visitors are within inches of marine animals indigenous to the Bay. 888/SEA DIVE WWW.AQUARIUMOFTHEBAY.COM *Discount Coupon on insert* Located at PIER 39, Beach St. & the Embarcadero. K-4

Blue and Gold Fleet This executive ferry provides service to Alcatraz, offers one hour San Francisco Bay cruises and excursions to Angel Island. Motorcoach tours of San Francisco, Napa/Sonoma Wine Country Muir Woods, Monterey/Carmel and Yosemite can be part of your Bay Area visit. Also ferry service to Alameda/Oakland, Vallejo, Sausalito and Tiburon. Tickets/Info 415/705.5555 WWW.BLUEANDGOLDFLEET.COM *Discount Coupon on insert* Departures from PIER 39 & Pier 41. H-3

Red & White Fleet One-hour cruise, sail under the Golden Gate Bridge & around Alcatraz. Foreign language translation. Daily, from 10:00 am at Pier 43, Fisherman's Wharf. Motorcoach sightseeing tours of San Francisco, Napa/Sonoma Wine Country, Muir Woods/Sausalito, Monterey/Carmel and Yosemite. Reservations/Info 415/673-2900 WWW.REDANDWHITE.COM *Discount Coupon on insert* G-3

SS Jeremiah O'Brien The World's most famous W.W.II Liberty Ship. The only ship out of 5000 that participated in the "D-Day" landings, to return 50 years later to Normandy, to represent the U.S. 415/544-0100 WWW.SSJEREMIAHOBRIEN.ORG *Discount Coupon on insert* Docked at Pier 45. K-2

The Wax Museum Step back in time and enjoy the ancient art of Wax Sculpting. You'll visit with Hollywood Celebrities, U.S. Presidents, Scientists, World Leaders and of course, our Chamber of Horrors. Come experience what has delighted more than 10 million visitors for more than 40 years. TOLL FREE 800/439-4305 WWW.WAXMUSEUM.COM *Discount Coupon on insert* 145 Jefferson St. G-4

Wharf Sport Fishing Fleet Join us for an unforgettable day fishing the Pacific Ocean beyond the Golden Gate Bridge or in San Francisco Bay. The Sport fishing boats are conveniently docked along Jefferson Street in the heart of Fisherman's Wharf. F-3

Bass Tub 415/456-9055 CELL 309-BASS
Butchie B 415/457-8388 CELL 302-1650
Captain Joey 415/892-2352
Chucky's Pride 415/564-5515
Happy Days CELL 415/752-5886
Lovely Martha 650/871-1691 CELL 415/509-5552
Miss Farallones 925/672-0115
Primetime CELL 415/706-4947
Wacky Jacky 415/586-9800 CELL 760-9359

Shopping Destinations

The Anchorage The Anchorage Shopping Center offers over 35 unique shops and restaurants, hotel accommodations, free entertainment and validated parking. 415/775-6000 WWW.ANCHORATTHEWHARF.COM 2800 Leavenworth St. between Jefferson St. & Beach St. E-4

THE CANNERY at Del Monte Square has been a SF destination since 1907 when it was Del Monte's Plant #1. An authentic San Francisco gathering place, today it is home to 35 shops, restaurants and nightclubs. 415/771-3112 WWW.DELMONTESQUARE.COM D-4

Dudley Perkins San Francisco's only authorized Harley-Davidson dealership. Gift Store open 7 Days. 415/776-7779 WWW.DPCHD.COM *Discount Coupon on insert* 2595 Taylor St. at North Point F-5

Ghirardelli Square Historic Ghirardelli Square features intriguing specialty shops, award-winning restaurants, live entertainment and breathtaking Bay views. Free parking with validation. 415/775-5500 WWW.GHIRARDELLISQ.COM 900 North Point St. B-4

PIER 39 San Francisco's #1 Attraction, is a festival marketplace offering 11 full-service restaurants, 110 specialty shops, family fun and postcard views of San Francisco Bay. 415/981-PIER WWW.PIER39.COM Beach St. & The Embarcadero. J-2,3,4

Restaurants

Alioto's Restaurant Finally, a place where the food is as good as the view! Serving Sicilian delicacies and seafood, fresh from the sea and perfectly prepared since 1925. Open 11AM–11PM daily. 3 hours free parking with validation. 415/673-0183 WWW.ALIOTOS.COM #8 Fisherman's Wharf at Taylor & Jefferson F-3

Ben & Jerry's Come visit our 2 Wharf area scoop shops at Pier 41 and at 475 Jefferson St. in the Argonaut Hotel. Also, visit us at Macy's Cellar. 415/263-7233 WWW.ICECREAM4U.COM *Discount Coupon on insert* D-4, G-4, H-3

Blue Mermaid The Blue Mermaid Chowder House and Bar, a lively dining destination serves casual San Francisco fare, including a variety of homemade chowders and classic preparations of fresh seafood. The Restaurant also features courtyard dining for warm weather. 415/771-2222 WWW.BLUEMERMAIDSF.COM 471 Jefferson St. at Hyde St. D-4

Buena Vista Celebrating over 50 years of our world famous Irish Coffee. The Buena Vista serves breakfast, lunch, Dinner and cocktails all day. Open Monday–Friday 9am–2am. Weekends 8am–2am. Gift shop on Hyde St. 415/474-5044 WWW.THEBUENAVISTA.COM 2765 Hyde St. at Beach St. D-4

Boudin at the Wharf The new must see attraction includes an expanded bakery; a Boudin Cafe; Bistro Boudin, a full-service restaurant; a demonstration area for hands on workshops; a Private Dining Room, perfect for business and social gatherings; and the Boudin Museum & Bakery Tour. 415/928-1849 WWW.BOUDINBAKERY.COM 156 Jefferson St. G-4

The Crab House–PIER 39 Home of the World Famous "Killer Crab®" A whole Dungeness Crab roasted in our secret garlic sauce "Voted Best Crab in San Francisco." The Crab House offers stunning views of the bay, the Golden Gate Bridge, and Fisherman's Wharf. Two hours complimentary parking at PIER 39 garage. 415/434-CRAB (2722) WWW.CRABHOUSE39.COM Located on PIER 39, 2nd floor, West side J-3

Hornblower Cruises & Events Savor, indulge, and unwind. Enjoy the finest in gourmet cuisine, surrounded by breathtaking views of the Bay Bridge, San Francisco Skyline, Angel Island, Tiburon, and Alcatraz. Sail under the magnificent Golden Gate Bridge. Choose from a 3-hour dinner/dance cruise or 2 hour weekend Champagne Brunch cruise. Live entertainment on all cruises. 415/788-8866 ext.7 WWW.HORNBLOWER.COM Departs Pier 33

Nonna Rose A Wood-grilled Sicilian style seafood, plus unique pasta dishes, salads and sandwiches. Italian and American wine list. Open 11AM–11PM daily. 415/359-1200 3 hours free parking with validation. WWW.NONNAROSE.COM #7 Fisherman's Wharf at Taylor & Jefferson F-3

Rainforest Cafe Escape into a tropical adventure alive with cascading waterfalls and exciting animatronics. The menu offers a variety of specialty items from seafood, beef and chicken to pastas and pizza. The fun new Kids Menu has a variety of fresh tastes and old favorites. Our very own Sparking Volcano dessert lights up any meal! 415/440-5610 WWW.RAINFORESTCAFE.COM *Discount Coupon on insert* 145 Jefferson St. G-4

Scoma's Restaurant Located off the beaten path on Pier 47 and Al Scoma Way, Scoma's is backed by a long family tradition of serving the freshest seafood available daily. Complimentary parking. 415/771-4383 WWW.SCOMAS.COM D-4

Sightseeing Tours

San Francisco Sightseeing/Gray Line "Let San Francisco's most experienced and respected tour guides entertain you with their insight and knowledge." Several tour packages available: City/Muir Woods, Alcatraz, Wine, Monterey with Aquarium, and Yosemite. PH 415/434-8887 TOLL FREE 888/428-8834 WWW.GRAYLINESANFRANCISCO.COM Pier 43, Embarcadero F-3

Tower Tours Fully narrated sightseeing tours offered daily including Deluxe City Tours, Wine Country, Muir Woods/Sausalito, Monterey/Carmel, Yosemite and Alcatraz & Bay Cruise packages. PH 415/345-8687 TOLL FREE 866/345-8687 WWW.SFTOWERTOURS.COM *Discount Coupon on insert* 865 Beach St., 1st level at Ghirardelli Sq. G-4