

BITS

FINANCIAL SERVICES
R O U N D T A B L E

BITS CONSUMER CONFIDENCE TOOLKIT: DATA SECURITY AND FINANCIAL SERVICES

OCTOBER 2006

A PUBLICATION
OF
BITS
1001 PENNSYLVANIA AVENUE NW
SUITE 500 SOUTH
WASHINGTON DC 20004
(202) 289-4322
WWW.BITSINFO.ORG

BITS

FINANCIAL SERVICES
ROUND TABLE

BITS CONSUMER CONFIDENCE TOOLKIT: DATA SECURITY AND FINANCIAL SERVICES

TABLE OF CONTENTS

INTRODUCTION

WHY CARE?

Consumer Confidence

Risk Management and Regulatory Requirements

ROLE OF THE FINANCIAL SERVICES INDUSTRY

Financial Institutions' Leadership Role

Examples of Financial Services Sector's Leadership

Financial Institutions Are Highly Regulated and Supervised

CURRENT SECURITY ENVIRONMENT

Cybersecurity Threats and Vulnerabilities

Data Breaches and Notification

No Simple Solutions

Authentication

Encryption

Need for Uniform National Standards for Breach Notification

WHAT CONSUMERS SHOULD KNOW AND WHAT THEY CAN DO TO PROTECT THEMSELVES

What Consumers Should Know

General Security Tips

Online Security Tips

VOLUNTARY GUIDELINES FOR CONSUMER CONFIDENCE ON ONLINE FINANCIAL SERVICES

CRITICAL SUCCESS FACTORS FOR SECURITY AWARENESS & TRAINING PROGRAMS

POLICY DOCUMENTS

RECOMMENDATIONS FOR GOVERNMENT AND POLICY MAKERS

RESOURCES

INTRODUCTION

This **BITS Consumer Confidence Toolkit** provides information to support consumer confidence in the safety, soundness and security of financial services. Originally published in September 2005, this is a revised and updated edition. This is intended to be an educational resource—whether for use by consumers, policy makers, financial institutions or others with interest in the subject matter.

Special attention is placed on information security as well as online financial services transacted through the Internet. Data in support of the safety of online financial transactions is provided. Information about the proactive leadership of the financial services industry is included, as well as a description of the current environment and tips for consumers to help protect their financial security, including in the online environment. Recommendations for government agencies are also provided.

BITS is a non-profit industry consortium of 100 of the largest financial institutions in the United States. BITS shares membership with The Financial Services Roundtable. BITS and Roundtable member companies provide fuel for America's economic engine, accounting directly for \$50.5 trillion in managed assets, \$1.1 trillion in revenue, and 2.4 million jobs.

BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS focuses on key issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention and the safety of financial services. Major purposes are to develop and disseminate industry best practices for improving information security programs, reducing fraud, managing third party providers, managing risk and fostering innovation. BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Committee, BITS Advisory Board and BITS Advisory Council. For more information, go to www.bitsinfo.org.

WHY CARE?

Consumer Confidence

- There is a potential erosion in consumer confidence as a result of highly publicized losses and thefts of consumers' personally-identifiable information.
- Increases in security breaches, insider fraud, data losses and data thefts are heightening consumer concerns about the safety of their financial identity and financial assets.
- Increases in phishing incidents, attacks through use of virulent software, new forms of e-scams and online fraud are heightening consumer concerns about the security of the Internet for conducting financial transactions.

Risk Management and Regulatory Requirements

- Inaccurate information could lead to poor policy decisions, including attempts at solutions that create new burdens on industry and consumers without solving problems.
- There is a need for fact-based solutions to issues concerning data security and financial services.
- Regulators examine financial institutions for compliance with information security, third party outsourcing, fraud and identity theft prevention and mitigation controls. Financial institutions work proactively to demonstrate they have adequate controls in place to mitigate these risks.

ROLE OF THE FINANCIAL SERVICES INDUSTRY

Financial Institutions' Leadership Role

- The financial services industry implements rigorous procedures for protecting data security, in physical as well as electronic environments.
- Experts from financial institutions develop and share best practices and other voluntary guidelines to safeguard information and manage cyber security risks.
- The financial services industry works diligently and proactively to implement controls to combat fraud, identity theft and other forms of crime.
- Financial institutions use a variety of safeguards to ensure the reliability and security of financial transactions, and protection of financial privacy. Many of these safeguards are required of financial institutions by federal regulators.
- Financial institutions are implementing strong authentication practices in response to changing risks and regulatory guidance.
- Financial institutions use systems to monitor customers' account activity and analyze patterns to detect and prevent unusual or fraudulent activities.
- Financial institutions know that identity theft is a serious concern of consumers and are working proactively to prevent the crime as well as to assist those who fall victim to it.
- Fraudulent credit and debit card transactions are not identity theft and seldom lead to identity theft. True identity theft is using another person's personally identifying information to establish or take over a credit, deposit or other financial account.
- Many institutions provide a 100% online guarantee in the event of online fraud.
- Financial institutions are educating customers on steps they can take to secure their computers and to avoid the lure of fraudsters to supply confidential information or access information such as passwords or PINS.

Examples of Financial Services Sector's Leadership

Note: All BITS Publications listed below are available at the BITS web site, www.BITSinfo.org.

1. Assisting Victims of ID Theft

BITS and The Financial Services Roundtable established the Identity Theft Assistance Center (ITAC).

- True victims of identity theft are rarer than is widely reported. However, if such a theft occurs and financial fraud is perpetrated, BITS and Roundtable members help victims to restore their financial identity.
- ITAC provides a free victim assistance service for customers of member companies. ITAC helps victims of ID theft by reducing the delay and frustration that consumers often experience as they restore their financial identity.
- As of October 2006, the ITAC has helped more than 10000 consumers restore their financial identities.
- The ITAC information is shared with law enforcement to help prosecute the perpetrators.
- The ITAC is a cornerstone of our overall industry efforts to detect and prevent fraud, help victims, address the causes of identity theft and enable prosecution of fraudsters.

For more information, visit www.identitytheftassistance.org or contact Anne Wallace at anne@fsround.org.

2. Stopping Re-Hires of Employees Who Commit Fraud

BITS established the Early Warning® Internal Fraud Prevention Service.

- The project took more than four years from idea to implementation, largely because of the need to address human resources and legal issues.
- After resolving these issues and after an extensive request for proposal process, the BITS Fraud Reduction Steering Committee chose Primary Payments Systems, Inc. (PPS), an affiliate of First Data Corporation, to develop and manage this new insider fraud prevention service.
- The Service is now provided through Early Warning Services LLC, a division of PPS that is owned by financial institutions.
- The Service protects financial institutions from hiring employees who have been fired from other financial institutions for compromising consumer information and/or knowingly committing fraud.
- The service began on August 1, 2006 and is ongoing.

For more information, visit www.early-warning.com/internalfraud/ or contact [Tony Selway](mailto:Tony.Selway@primarypayments.com) at tselway@primarypayments.com.

3. Preventing and Stopping Phishing and Other E-Scams

BITS established a Phishing Prevention and Investigation Network.

- Phishing is the practice of luring consumers to provide bank account and other personal information to fraudsters through bogus email messages.
- In response to these and other online scams, BITS created a Phishing Prevention and Investigation Network in 2004.
- The BITS Phishing Prevention and Investigation Network provides member institutions with information and resources to expedite investigations and address phishing/spoofing incidents.

- The BITS Phishing Network includes a searchable database of information from other financial institutions on their phishing incident and response experience, including contacts at law enforcement agencies, foreign governmental agencies, and ISP Web administrators.
- The Network also provides data on trends to help law enforcement build cases and shut down identity theft operations.
- The BITS Phishing Prevention and Investigation Network: helps member institutions monitor and shut down e-scams faster and more effectively; reduces financial institution manpower costs and losses; increases phishing investigations and arrests of perpetrators; and facilitates communication among fraud specialists at financial institutions, service providers and law enforcement agencies.

4. Protecting Data in Storage and Transport

BITS published a tool in April 2006 to help financial institutions evaluate the risks associated with the transport, storage and destruction of physical media.

- The *BITS Key Considerations for Securing Data in Storage and Transport* paper provides financial institutions with a framework to evaluate the risks associated with the transport and storage of physical media and the destruction or erasure of data on various media.
- This framework is a reference tool that complements individual institutions' risk assessment and risk management policies.
- The framework helps risk managers and information security professionals by outlining key questions, identifying risks that can (and cannot) be mitigated, educating key vendors about the needs of financial institutions, implementing appropriately secure storage and transport procedures, and developing effective audit procedures.
- The framework is intended to address transport and storage of information for the purposes of archiving, processing, regulatory reporting, backup and recovery, and customer requirements.
- *The BITS Key Considerations for Securing Data in Storage and Transit* is an example of how the financial services industry is focusing on data security issues (in response to breaches and breach notification) through the development of voluntary best practices.

5. Responding to Security Breaches

BITS and the American Bankers Association (ABA) completed a guide in 2006 to help financial institutions develop and execute response programs when confidential and sensitive information is accessed or misused by unauthorized individuals.

- Breaches of sensitive customer information threaten to undermine customer confidence and the reputations of both individual financial institutions and the financial services industry. This threat is aggravated by the patchwork of state laws and federal regulations that govern breach notification.
- Despite these challenges, financial institutions are strengthening data security programs and improving customer notification programs.
- The "BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information" is a tool that may assist some financial institutions in developing and executing response programs when confidential or sensitive information is accessed and misused by unauthorized individuals.
- The genesis of this paper dates to 2003 when several BITS working groups initiated discussions among information security experts within BITS and The Financial Services Roundtable companies, the American Bankers Association, service providers, and regulators in response to emerging breach notification requirements. Since 2003, these experts have gained experience in

mitigating the risks of unauthorized access while legal and regulatory standards have continued to evolve.

- The paper is divided into several sections that cover the evolving legal and regulatory requirements, potential elements of a response program, and suggestions for managing third party service provider relationships as they relate to data security programs and customer notification.

6. Protecting the Elderly and Vulnerable from Financial Fraud

BITS released the BITS Fraud Prevention Toolkit: Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation.

- Published in 2006, the focus is on protecting the elderly and vulnerable.
- Led by BITS and Roundtable member, Wachovia Corporation, with support from a host of other member institutions and a strong array of partnering organizations, this is an unprecedented cooperative effort.
- Cooperating organizations include representatives of the US Administration on Aging, AARP, Credit Union National Association, National Adult Protective Services Association, and National Foundation for Credit Counseling.

7. Restoring Confidence in E-mail

BITS is working with member financial institutions and Internet Service Providers to improve the security of e-mail.

- E-mail is now a primary means of communication from financial institutions to their customers and from financial institutions to other financial institutions and service providers. However, E-mail is insecure and lacks confidentiality and integrity unless uniform and explicit controls are put into place.
- In early 2006, members of the BITS Security and Risk Assessment Working Group embarked on a project to enhance the security and integrity of e-mail communications.
- The goals of the BITS e-mail security project are to enhance the confidentiality and integrity of information exchange among financial institutions and between financial institutions and their customers and clients; to protect customers and their accounts from identity theft and account fraud; and to restore the reliability of the e-mail delivery channel for financial institutions.
- The BITS e-mail security group recommends the adoption of three specific technologies to enhance e-mail security. These technologies are Transport Layer Security (TLS), Sender Policy Framework (SPF), and Domain Key Identified Mail (DKIM). Each of these technologies is gaining wider acceptance, is becoming more transparent to the end user, and they are relatively inexpensive to implement and maintain. Each of these protocols addresses a particular problem and can be used in conjunction as part of a layered approach to security.

8. Retaining Tools to Respond to Cyber Crimes

BITS is urging continued and improved access to tools that help financial institutions respond to Internet scams.

- With the growth of the Internet and its fundamental role as a foundation for electronic commerce, including financial services, the role of the Internet Corporation for Assigned Names and Numbers (ICANN) and its significance has grown exponentially.
- ICANN is a non-profit corporation responsible for assigning IP addresses and Domain Name management.

- ICANN maintains a WHOIS data base that provides, on query, information about domain names and IP addresses associated with domain names. A change is being considered that might prevent financial institutions from being able to access the WHOIS data base. Access to this data base is crucial to preventing crimes of identity theft, stopping phishing attacks, and similar Internet-based crimes.
- BITS has taken a range of actions to convey the need for financial institutions to continue to have access to this data base for fraud-prevention services.

9. Engaging Government Agencies to Provide Fraud/ID Theft Tools

BITS and The Financial Services Roundtable are encouraging the Social Security Administration to provide a robust verification system that will help prevent fraud and identity theft.

- For many years, BITS and Roundtable companies have sought ways to verify the accuracy of Social Security Numbers in the interest of reducing fraud and complying with numerous legal requirements.
- In the interest of reducing fraud and complying with numerous legal requirements, BITS members support efforts by the Social Security Administration to establish a “consent-based social security verification program” (CBSV) that will allow institutions to affirmatively verify a consumer’s name, social security number and date of birth (DOB).
- Establishing a “Real Time” system capable of high volume at low cost would significantly reduce the incidence of identity theft. “True name” identity theft would become more difficult with the validation of date of birth and the optional gender code by financial institutions utilizing a verification program.
- Consumers would benefit from industry’s ability to verify SSN information by reducing the incidence of fraud and errors.
- BITS completed in July 2006 the *BITS Business and Technical Requirements for an Effective and Secure Social Security Verification Program to Combat Fraud and Identity Theft*. These requirements provide a framework for cooperation between the Social Security Administration and financial institutions to partner with the SSA on a consent-based verification program that meets the needs of the customers, the industry, and the agency.

10. Improving Security Through Increased Efficiencies

BITS established the Financial Institution Shared Assessments Program.

- The Financial Institution Shared Assessments Program was created by BITS and member financial institutions to improve the cumbersome and expensive service provider assessment process. The Program became available for participation in February of 2006, offering memberships to financial institutions and service providers of all sizes wishing to introduce unprecedented efficiencies and cost savings into their outsourcing programs. By October 2006, more than 30 financial institutions and service providers had joined the Program.
- The Shared Assessments Program currently has 12 major industry service providers slated for assessments, with one complete and a second underway. Once their assessments are complete, service providers may share the reports with a virtually unlimited number of client companies.
- The Financial Institution Shared Assessments Program is based on two essential documents:
 - The Standardized Information Gathering Questionnaire, or “SIG”, which gives financial institutions a detailed “snapshot” of the security controls at the service provider’s location.
 - The Agreed Upon Procedures, or “AUPs,” whose 45 control points can be used by assessment firms or qualified CPAs to create detailed reports.
 - These two documents are available at www.bitsinfo.org/fisap.

Financial Institutions Are Highly Regulated and Supervised

- The Congress has enacted numerous laws designed to protect the privacy and security of confidential or sensitive customer information. Examples include the Gramm-Leach-Bliley Act and the FACT Act.
- The financial services industry is both highly regulated and supervised by federal regulators (Federal Deposit Insurance Corporation, Federal Reserve System, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, Securities and Exchange Commission) and state regulatory agencies.
- Regulators issue and update requirements based on changing risks. In recent years, federal regulators have issued regulations or supervisory guidance on authentication, business continuity planning, customer notification following a security breach, identity theft prevention and mitigation, information security and outsourcing.
- Examiners from regulatory agencies routinely audit financial institutions and service providers and support the financial services industry. As part of these examinations, experts in information security assess the adequacy of controls that financial institutions have in place. When deficiencies are detected, the regulators mandate changes or impose sanctions on financial institutions.
- Federal and state examiners constantly evaluate the controls financial institutions have in place to protect the privacy and security of customers.
- When there is a security breach that could result in potential harm to a customer, the federal regulators require that financial institutions promptly contact those individuals.

CURRENT SECURITY ENVIRONMENT

Cybersecurity Threats and Vulnerabilities

- Cybersecurity threats are increasing.
- International crime rings, using the Internet for fraud and financial gain, are propagating.
- Criminals are writing and disseminating code to compromise systems.
- Hackers are closing the window between the discovery of a flaw and the release of a new threat.
- Software vulnerabilities and exploits are too high and increasing.
- Criminals have better tools for breaking into computer systems and networks.
- Law enforcement is doing more to investigate and prosecute crimes and to cooperate with foreign law enforcement agencies and international organizations.

Data Breaches and Notifications

- We are hearing more and more about security breaches and data losses. Data breach disclosures reflect the fact that organizations are required to report security breaches.
- Data breach disclosures are mandated by state laws and for financial institutions these are mandated by regulations linking back to the Gramm-Leach-Bliley Act. The Securities and Exchange Commission (SEC) has not signed onto the guidance so the guidance does not apply to broker-dealers who are not otherwise regulated.
- Most of these breaches are physical breaches or lost computers containing sensitive data as it was being shipped from one facility to another. There also have been hacking-related breaches and insider abuse.
- While news of these breaches sounds alarming, there is not a one-to-one correlation between the exposure of personal information in a breach and an incident of identity theft. The vast majority of compromised data never gets used.
- Notifying customers is a complicated and complex process and can, if poorly done, undermine confidence in the financial services industry and the economy overall.
- Care must be exercised in alerting consumers to steps they can take to protect themselves from ID theft and other forms of fraud while averting needless alarm.

No Simple Solutions

- Media reporting of cyber security issues often overstates the problems and implies simple solutions. The impact of media reports is a factor in undermining consumer confidence in the financial services industry.
- Consumer fear about online security is the number one reason that consumers give for not conducting financial transactions online. Yet, monitoring financial accounts online and using electronics rather than paper can actually reduce consumers' risk of identity theft.
- Protecting privacy and maintaining security is an ongoing process. It requires constant vigilance. There are no simple solutions.
- A robust information security program has three major components: people, processes and technology.
- An effective information security program includes an ongoing risk assessment process to evaluate the impact of changing risks and the necessary risk-based controls to mitigate these risks.
- In recent years, there have been increasing focus on authentication and encryption. Data breaches are drawing attention to the use of stronger authentication and more use of encryption technology. Both are important tools that financial institutions deploy based on the risks.
- It is important to bear in mind that financial institutions must weigh several factors when using strong authentication and encryption.
- Calls for simple solutions such as mandating encryptions for storing or transmitting all forms of data or mandating dual or multi-factor authentication for electronic commerce should be analyzed carefully to ensure that they are not overly complicated or complex.

Authentication

- On October 12, 2005 the Federal Deposit Insurance Corporation, Federal Reserve Board, Office of the Comptroller of the Currency, Office of Thrift Supervision and the National Credit Union Administration jointly issued “Authentication in an Internet Banking Environment.” The regulators require covered financial institutions to assess the risk of authentication practices and implement more secure authentication practices by December 2006.
- Multi-factor authentication has many advantages and is used by many financial institutions based on risk factors. Multi-factor authentication methods for Internet Commerce may improve security but may not automatically prevent “phishing” or account takeover.
- Two-factor authentication might limit a criminal’s ability to immediately capitalize on the personal information he or she has stolen. Criminals could still induce an unsuspecting consumer to give up important financial information through “phishing” or some other scheme, and make use of that information in some other way.
- Multi-factor authentication methods involve serious practical problems and consumer acceptance hurdles. U.S. consumers of financial services have not accepted solutions that involve lengthy enrollment processes or complicated processes for using the technology. Implementing such schemes would involve an extensive process of consumer education and training to familiarize consumers with these new procedures.

Encryption

- Data breaches are drawing greater attention to the role of encryption.
- Encryption is an important and useful tool and a key component of a financial institution's information security programs.
- Encryption of data poses a number of significant challenges that must be considered.
- Encryption is not a simple solution and the issues are complex and multi-faceted. Its application must be measured against the need to access data today as well as to meet recovery and retention requirements in the future. Whether to use encryption depends on many factors, including how the data is stored, where it is transported, its intended usage, whether the data contains sensitive or confidential information, back-up or restoration requirements, retention requirements, etc. A major challenge is managing the encryption "keys" to the encrypted information. These challenges mount with increasing age of the information.
- Encryption does not protect data that is on paper, film or microfiche. Given that many of the publicly announced data breaches in recent years were from stolen paper documents or data sold to fraudulent businesses, it is important to recognize that encryption would not have prevented the information from being viewed or compromised.
- There are consequences to encrypting data that must be weighed against the benefits. For example, there are potential negative effects on computer networks, the ability to detect intrusions, the reduced speed of computing, and the ability to retrieve data for back-up restoration or business continuity requirements.
- Some government agencies or third parties require that data be provided in unencrypted formats. Further, even when information is shipped securely by the financial institution, it may not always be shipped securely on return.
- Despite best efforts by financial institutions to protect information, exchanges with customers and third parties oftentimes are outside of the financial institution's control.
- Encryption in itself cannot guarantee data security. It can be part of a broader, robust information security program, and it needs to be well-implemented. Decisions on what data to encrypt and at what points to encrypt data are based on risk of disclosure and the costs and risks of encryption, as well as the need to access data to serve customers.

Need for Uniform National Standards for Breach Notification

- Efforts by various states and regulatory agencies raise significant implementation problems for financial institutions. In a transient society, notification should occur uniformly regardless of which state the consumer may live in. Moreover, inconsistent application of inconsistent state law inevitably creates a compliance nightmare for institutions with a multi-state presence.
- A national standard should be risk-based and provide financial institutions with some flexibility in determining when and how to notify customers.
- Financial institutions should notify customers when there is some indication that the breach actually has the potential to cause harm or injury. If harm is demonstrably contained, for example, and no risk really exists, there should not be any reason to notify and scare people.
- Companies that discover breaches in security should be allowed first to notify law enforcement authorities, as well as consumer reporting agencies, so that law enforcement authority can get a jump on any existing criminality and Credit Reporting Agencies may be better prepared for the potential volume of consumer inquiries about the impact of any breach on consumer credit history.

WHAT CONSUMERS SHOULD KNOW AND CAN DO TO PROTECT THEMSELVES

What Consumers Should Know

- Hundreds of millions of financial transactions—both online and offline—occur each day.
- On the whole, Internet banking and other online financial transactions are safer than paper-based transactions.
- Identity thefts that occur online are generally smaller and take less time to resolve than paper-based thefts.
- Identity theft is a highly complex issue with many players and no simple solutions.
- Incidents of identity theft and identity fraud are often mis-characterized in the popular media.
- Fraudulent credit and debit card transactions are not identity theft and seldom lead to identity theft.
- Most cases of identity theft do not occur online. Where the method is known, most theft of personal information is through traditional rather than electronic channels.
- Resolving identity theft requires coordination among multiple federal, state and local agencies, and industry.
- Consumers are protected against financial losses from fraud by laws and regulations.
- Customers will be held harmless in almost all circumstances in which fraud occurs.
- Financial institutions use sophisticated systems to flag unusual activity and protect consumers against fraud. These systems allow financial institutions to monitor activities in real time.
- Many of these controls are kept “invisible” for security reasons.

What You Can Do to Protect Yourself: General Security Tips

- **Know your merchant.** Ensure you know the person or entity to which you are giving information over the Internet, phone, or fax. Do not provide your personal information unless you have initiated contact with the merchant. Only do business with Internet companies that use a secure form, often indicated by a padlock in the lower corner of the website, to capture private information such as account numbers or credit card numbers.
- **Order copies of your credit report at least once a year** from each of the three major credit bureaus and ensure all of the information is accurate. Stagger the process so you can check your records three times each year.
Equifax 1-800-685-1111
Experian 1-888-EXPERIAN (397-3742)
Transunion 1-800-916-8800
- **Monitor your accounts and statements frequently and thoroughly**, ensuring that all activity is accurate. If your account statements are late, immediately contact your financial institution(s) to ascertain if and when the statements were mailed. If your institution offers online banking, check your account frequently and regularly, rather than waiting for monthly statements. Reporting fraud as soon as possible helps stop further occurrences of fraud.
- **Always thoroughly tear or shred documents with personal information**, such as pre-approved credit offers, which may contain account information, Social Security numbers, date of birth, etc. Shredding such documents protects you against “dumpster diving.”
- **Always protect your account information.** Don't write your personal identification number (PIN) on your ATM or debit card. Don't write your Social Security number and/or credit card number on a check.
- **When using your ATM, cover your hand when entering the PIN number** to protect the information from “shoulder surfers.”
- **Carry only those pieces of identification you absolutely need**, and keep them secure.
- **Discard unused instant credit offers**, ensuring they are properly shredded.
- **Safeguard your receipts, account numbers and account expiration dates.** Don't leave credit card records, including your transaction receipts, or anything else with credit card numbers and expiration dates in unsafe locations.
- **If you suspect your identity has been stolen or you have shared any personal financial data, including your account username and password, contact your financial institution and the authorities immediately.** U.S. consumers should:
 - File a police report with their local police department and call the Federal Trade Commission at 1-877-ID-Theft.
 - Complaints can also be reported to: the Internet Fraud Complaint Center (IFCC), www.ifccfbi.gov.
 - Contact the three credit reporting agencies to place a fraud alert on your record.
 - Maintain a log of all contacts you make with the authorities regarding the matter, including the name, title, phone number and police case number, in case future contact is required.

What You Can Do to Protect Yourself: Online Security Tips

- **Ensure your computer(s) are equipped with a security toolkit** to help keep trespassers out. A security toolkit includes personal firewalls, antivirus and virus detection software, anti-spyware software, and adware and spywareblocking software. Viruses and spyware are different, so you need to protect yourself against both. Update the toolkit frequently, and periodically check your firewall settings. Install security patches issued by your software (operating system and browser) vendor. Update software applications as well as operating systems and browsers, and be sure to patch the entire suite of applications that have the same type of vulnerability operating system.
- **Consider installing a Web browser toolbar to help protect you from known phishing websites.** A number of Internet service providers (ISPs) offer toolbars to help identify fraudulent sites. Please contact your ISP to determine which is best for you.
- **Always back up your data.**
- **Change your passwords periodically, using strong passwords that could not be easily guessed. Do not use names (like your mother's maiden name) or dates (like your birthday) or your Social Security number (SSN).**
- **Always log off from your online banking session.**
- **Shut off/disconnect your computer from the Internet when not in use.**
- **Avoid purchasing products from online merchant or auction sites if the deal looks "too good to be true."** If it looks too good to be true, it probably is.
- **Be cautious and skeptical.** If you get an unsolicited email from your financial institution asking for personal information, including your account number, contact the institution to verify its validity. Most financial institutions will NOT request such information from you via email or phone.
- **Don't click the link.** If you are concerned about the authenticity of an email, contact your financial institution directly by phone. You may also go directly to your institution's site by typing the URL in the browser. Should you choose to go directly to the site, check for indicators that the pages are secure. A secure site will have a padlock symbol at the bottom of the page and a URL that begins with "https" instead of "http."
- **Verify Online Security Certificates.** These certificates are used to indicate a site is secure. A certificate is what is behind the padlock symbol at the bottom of the page. If the certificate was issued by an independent certificate authority, due diligence has been performed on the business. If someone has cloned a site, the site will not have a certificate. If the certificate name does not match the site, do not use it and notify the institution.
- **If you use a wireless network, deploy proper encryption, password protection and secure firewalls.**
- **Be suspicious of requests for personal information.** Due to the increase of phishing and online scams, financial institutions have altered their practices and are unlikely to ask you for

personal information in an email. Be especially cautious of “urgent” requests, as phishers try to excite or upset customers so they will react immediately.

- **Be careful who you trust.** Unfortunately, identity theft and other forms of fraud often are perpetrated by friends, employees, and family members.
- **Visit your financial institution’s website online.** Most now carry detailed information about security safeguards, how to protect yourself against fraud, and how to get help should a problem occur.

BITS

FINANCIAL SERVICES
R O U N D T A B L E

VOLUNTARY GUIDELINES FOR CONSUMER CONFIDENCE IN ONLINE FINANCIAL SERVICES

**Approved by the Board of Directors of
The Financial Services Roundtable
September 16, 2005**

- Put consumer education about security and fraud prevention in a prominent place on your institution's website home page.
- Establish a single point of contact within your institution for serving any customers with fraud, security or identity theft issues.
- Strongly encourage the move to "online" financial services—even if only to monitor accounts on a frequent and regular basis.
- Encourage customers to "turn off" paper bills, checks and statements, and shred any paper documents with personal information.
- Encourage customers to keep their computer software updated to repel attacks, including updating software and installing security programs.
- If a breach occurs, address it immediately—with your communications systems coordinated to assure that your institution speaks with "one voice."
- Use diverse communication channels to spread the same consistent message, from facts about online security to consumer protections.
- If you are not already a member, join the Identity Theft Assistance Center.
- Make sure ALL your financial institution personnel have a basic understanding of the facts concerning the safety of online financial services.
- Incorporate security awareness and education, fraud reduction education, and safety of online financial services education into your corporate wide training programs.

BITS

FINANCIAL SERVICES
ROUND TABLE

CRITICAL SUCCESS FACTORS FOR SECURITY AWARENESS & TRAINING PROGRAMS
ENDORSED AS VOLUNTARY GUIDELINES
BY THE BOARD OF DIRECTORS
OF THE FINANCIAL SERVICES ROUNDTABLE
SEPTEMBER 16, 2005

Developing a comprehensive security awareness and training program is a regulatory requirement and an effective risk management practice. Here are a few critical factors for success.

Consider the Corporate Culture

- Establish a program where security awareness and training are designed to maintain an appropriate balance between revenue, risk and reputation.

Engage Senior Management Support

- Gain senior management approval and communicate the messages and policies to the entire company. Developing a culture of security awareness and individual responsibility is most effective when the messages are driven by senior management.

Enforce Policies

- Develop well-written, understandable and current policies to reflect the corporate, threat and regulatory environment. Awareness and training programs should address the importance of adhering to policies, as well as the potential financial and reputational impact to the organization from security events.

Establish a Comprehensive Program

- Whether run centrally or de-centrally, the program should be staffed with experienced individuals and properly funded to develop, maintain and track the program's effectiveness.
- Understand that awareness is not training. Awareness focuses attention. Training provides employees with appropriate skills and knowledge. Effective programs contain both.

Communicate, Communicate, Communicate – But Target!

- Develop the required messages and create a strategy to communicate them through multiple channels targeted at different learning styles and levels.
- Utilize multiple touch points. From new hires to lines of business to corporate communications and the human resources department as well as senior management, everyone has an opportunity and a responsibility to stress the importance of security.
- Recognize that each employee has a role in protecting the organization's information assets. Segmenting employees based upon risk and responsibility for their roles provides an opportunity to focus on the policies, controls and consequences of poor information security behavior.
- Communicate the importance of controls and security to the individual's life outside of work. Today's risks and threats extend beyond the corporate environment.

Track Effectiveness and Update Your Program As Needed

- Use both qualitative and quantitative metrics to obtain feedback, measure and benchmark the effectiveness of your security awareness and training program. Make change a part of your process because the risks are constantly changing. Security Awareness and Training is a long-term, ongoing process.

POLICY DOCUMENTS

The following policies have been approved by the BITS Committee and the Board of Directors of the Financial Services Roundtable.

Authentication Mandates

As e-commerce continues to grow and new forms of fraud (e.g., phishing) rise, regulators and legislators are exploring a number of responses, including potentially mandating that financial institutions implement multi-factor authentication methods. BITS and Roundtable members are working individually to assess and address the underlying risk issue, and are collectively engaging regulators, legislators, third party vendors, and law enforcement agencies to develop constructive responses.

The members of BITS and The Financial Services Roundtable believe:

- **Financial institutions have a strong track record in protecting customer information and in deploying broadly accepted authentication methods.** As an example of protection, many financial institutions aggressively monitor account activity to detect and prevent fraudulent activities. As an example of effective deployment, customers have broadly accepted the use of ATM access cards and a personal identification number.
- **Financial institutions apply layered controls to protect consumers and financial institutions.** Authentication is an important element in a robust information security program, but it is one of many elements. Instituting new controls must be part of a managed process involving information, cost and installation study, analysis, and consumer education.
- **Perception, more than reality, is driving policymakers' concern and their consideration of multi-factor authentication for retail e-commerce.** Further, the media and many self-interested parties have exaggerated the phishing and identity theft problems, compounding confusion and exacerbating public fear.
- **There are many practical challenges involved in deploying multi-factor authentication technologies in real-world situations.** These challenges include customer acceptance, the maturity of the technology, cost, scalability, interoperability and dependence on government-issued credentials.
- **Consumer acceptance is a top concern.** Authentication methods that are overly complex or unwieldy for customers will not be accepted and may result in greater risks or deterioration in the use of online financial services. Further analysis should be conducted to investigate customer preferences, and the results should be given substantial consideration by policymakers.
- **Proposals mandating multi-factor authentication may not eliminate various forms of fraud such as "phishing."** Stronger authentication alone will not solve account takeover and is not the only or best tool for combating phishing. Criminals could still induce an unsuspecting consumer to give up important financial information through "phishing" or some other scheme, and make use of that information outside the realm of on-line financial services.
- **Applying multi-factor authentication requirements on US financial institutions that regulators in some countries mandate raises civil and privacy protection concerns in the US.** It is important to note that some foreign countries have more robust national identity schemes than the U.S. These schemes are linked to school attendance, tax, immigration, driving

license and other records that are associated with citizens in these jurisdictions. U.S. laws and consumer attitudes to such approaches are at odds and often viewed as an infringement of civil rights and privacy.

- **Regulators should work with the financial services industry before developing and issuing new regulatory or supervisory requirements.** Additional research and collaboration is needed before policymakers supplement the existing framework specified by the Bank Secrecy Act, Gramm-Leach-Bliley, the USA PATRIOT Act, Sarbanes Oxley, and the FACT Act. Any additional legislation, regulation or guidelines should be risk-based, technology neutral, and flexible enough to encourage continuous improvement.

The members of BITS and The Financial Services Roundtable further resolve to:

- Strive to develop enterprise-wide solutions that take into account the holistic picture and not just specific aspects of identity management and related issues.
- Strive to make authentication easier and more acceptable to users and consumers.
- Educate consumers to use safe on-line computing practices.
- Support research into customer preferences for authentication.
- Engage in discussions among financial institutions and leading software and hardware providers, Internet service providers, law enforcement agencies, and regulatory agencies on how to address cyber security challenges.
- Urge legislators and regulators to support risk-based approaches for evaluating the risks, deploying controls and offering convenient solutions to consumers.

Continue to respond aggressively to the escalation in identity theft and on-line fraud through the BITS Fraud Reduction Program and the Identity Theft Assistance Center (ITAC).

Fraud Reduction

Fraud against accounts continues to be a challenge to financial institutions and their customers. The adoption of new payment methods and tools for commerce has offered a new medium for fraud, including check, credit card, debit card, loans, identity theft and e-scams. New technologies are essential to economic growth but some are being used by criminals for illegal and destructive purposes, such as the e-scam called phishing. Phishing is the use of fraudulent emails that appear to be from legitimate companies in order to trick customers into providing personal information. Phishing is sometimes used as a precursor to identity theft and is an example of a crime that is facilitated by some of the new technologies. New technologies also have the power to deter and sometimes prevent these fraudulent activities.

The members of the Financial Services Roundtable and BITS believe:

- Technology brings both opportunities and risks.
- Technology brings convenience to consumers. It also increases some risks of financial loss and damage to credit history, including by identity theft.
- Among the risks are that nefarious individuals will harm others through fraud. Fraud perpetrated against financial institutions and their customers is not only economically damaging, but also can create cruel hardships for customers.
- To ensure the economy's continued growth and health, financial institutions must take reasonable actions to reduce these risks by identifying and preventing fraud.
- Financial institutions attempt to identify, control and prevent fraud through the use of systems and processes to detect patterns indicative of fraudulent behavior, e.g., identification of people posing as legitimate customers or people with histories of defrauding financial institutions.
- Shared use of selected demographic and historical information, needed to make these programs effective, is fundamental to the protection of financial institutions, their customers and the growth of the economy.
- Opportunities to use information and combine case data enable law enforcement agencies to successfully prevent and prosecute criminal activity.
- Fraud reduction is not a competitive issue. The fight against fraud requires the financial services industry to implement fraud management strategies based on a zero-tolerance-to-fraud spirit and continuous information sharing.

The members of BITS and The Financial Services Roundtable are encouraged to:

- Assure that the sharing of customer information to deter fraud and similar activities is promoted in ways that are consistent with applicable regulatory requirements, maintain appropriate confidentiality of the customers' and institutions' information, while continuing to be effective.

- Promote the sharing of successful strategies for combating fraud with institutions that are willing to form cooperative partnerships.
- Endorse current fraud prevention techniques by seeking information on the latest emerging fraud prevention technologies.

Promote the sharing of legal and regulatory information that impacts the fraud reduction programs used in the financial services industry.

Information Security

The safety, soundness and security of the financial infrastructure of this country are supported and assured by the integrity and commitment of the members of the financial services industry. The demands of the economy require that these trusted guardians of resources—and enablers of the payments and settlements systems—bring their expertise and conviction to the Internet and e-commerce environment, while maintaining the integrity of existing and valued traditional systems. The financial services industry is also dependent on the other core infrastructures—electric power, telecommunications, transportation—and they depend on financial services for their core operations. This interdependency is a key concern of both the private sector and the federal government and requires strong cross-sector involvement. Consumer confidence rests on a foundation of security as does privacy of consumer confidential information.

The members of the Financial Services Roundtable and BITS believe:

- Security is a bedrock of the economy.
- Security is a baseline for the industry, not a competitive issue. Cooperation is needed to ensure the stability, safety and soundness of our nation's financial services and e-commerce infrastructure.
- Security knows no geography; it is a global issue.
- The financial services industry is the most prepared and experienced of all sectors in the economy with respect to managing risk, protecting information and assuring financial soundness.
- The financial services industry must continue its leadership, vigilance, commitment to innovation, and practice of the discipline of improving systems to assure security—serving and protecting individual customers and the economy overall.
- Public/private sector partnerships are required to address the nation's e-commerce security challenges.

The members of BITS and The Financial Services Roundtable are encouraged to:

- Support initiatives to assure that new participants and third party providers in e-commerce recognize the framework of commitments and trust upon which the delivery of financial products and services depends; that they protect against risks; and bear appropriate responsibility for losses if, and when, they participate in financial transactions.
- Support BITS' industry-based security initiatives to establish controls and security into products and services by endorsing the BITS Product Certification Program, the BITS Framework for Managing Technology Risk in Information Technology (IT) Service Provider Relationships, the BITS Voluntary Guidelines for Aggregation Services and the BITS Mobile Financial Services: Recommendations for Business Requirements and Technical Guidelines.

- Use the BITS Tested Mark where possible, incorporate the product profile security criteria into your security policies, and encourage technology vendors to test products to meet the industry-endorsed security criteria.
- Participate in the Financial Services Information Sharing and Analysis Center (FS/ISAC).

Spyware

The term “spyware” refers to any software that covertly gathers user information through the user's Internet connection without his or her knowledge. While there are some operations that can assist users in ensuring smooth operations of their systems (e.g., auto-updates, antivirus scans) and provide targeted customer service to clients, there are classifications of spyware which are intent on gathering information or taking control of a user's system with privacy and security implications.

Spyware programs are often bundled with freeware or shareware and may be used for advertising purposes. When installed, the spyware software can access the system and monitor user activity as well as gather e-mail addresses, passwords and financial information. Some spyware is installed without user action or consent through exploitation of software vulnerabilities. This type of spyware may masquerade as a benign application and may install keystroke-logging software. Keystroke-logging software is of particular concern to financial institutions because it may provide criminals access and control over the user's host computer for the purpose of transmitting proprietary information, sometimes leading to identity theft and other forms of fraud.

However, types of applications commonly referred to as “cookies” or “web beacons” are often employed for legitimate business purposes and to provide added convenience to customers seeking web-based services. For example, many retailers – be they financial firms or otherwise – will employ applications to “remember” a customer's log-in, user ID, and his or her purchase history. In this way, the retailer can make a web-based relationship more convenient and target products and services to individuals.

The members of BITS and The Financial Services Roundtable believe:

- Some forms of spyware represent a significant threat to the ability of financial services institutions to meet their regulatory obligations to maintain the privacy of customer information.
- Spyware can decrease user productivity, system performance, and network bandwidth.
- Legislation must not retard the online relationship that financial firms have developed with their customers.
- Any legislation should:
 - Define “spyware” appropriately to protect legitimate business applications;
 - Ensure that notice and consent regimes are based on the principle of “opt-out”;
 - Provide for functional regulation by financial regulators;
 - Create a strong federal preemption to ensure that commercial firms operate under a uniform set of standards.

Comprehensive strategies can be developed to minimize the risk of sensitive data being compromised by spyware. Such strategies should involve all stakeholders including financial services and software development industries, regulatory agencies and state and federal government. Any legislation proposed to address problems associated with spyware should not trespass on the legitimate business models of firms who, everyday, seek to close the digital divide between retail operations and customers.

Internet Fraud and Phishing

Fraud and theft are age old tricks that fraudsters apply to new channels, such as the Internet, as they come along. One new form of Internet fraud is what is commonly referred to as “phishing.” Phishing is an electronic scam, delivered via the Internet, that is used to solicit personal information for fraudulent purposes.

The members of BITS and The Financial Services Roundtable believe:

- Identity theft and phishing are serious issues for consumers. Financial institutions take these issues seriously and must continue ongoing customer and consumer education programs around these issues.
- Overstating the problem can potentially damage consumer trust overall. It is important to put the risks of online security into perspective. Consumer fear about online security is the number one reason that consumers give for not conducting financial transactions online. Yet, monitoring financial accounts online and using electronics rather than paper can actually reduce consumers’ risk of identity theft.
- Financial institutions use a variety of safeguards to ensure the reliability and security of financial transactions. Many of these safeguards are required of financial institutions by federal regulators. The financial services industry is both highly regulated and supervised. Additional safeguards are adopted voluntarily by financial institutions as sound business practices. Many institutions provide a 100% online guarantee in the event of online fraud.
- Phishing targets are not limited to financial institutions, as Internet service providers, online retailers and the federal government have all been targeted. These entities often do not have the level of data security in place that financial institutions do, and are not subject to the same regulatory scrutiny as financial institutions.
- The lack of security at unregulated Internet service providers and hosting companies has facilitated the growth of phishing by providing an on-going source of easily accessible sites for criminals to use to perpetrate these scams.
- Consumers are becoming increasingly vigilant about the risks and ways to protect themselves from identity theft and other forms of fraud. However, there is a need for public education delivering a consistent message from the financial services industry.

The members of BITS and The Financial Services Roundtable further resolve to:

- Support education, such as through customer service e-mails and marketing, to financial services customers to assist in protecting themselves from Internet fraud, including phishing and spoofing of web sites.
- Take care not to fuel consumer fears with scare stories that do not provide a realistic portrayal of the relative risks of online versus offline and the ways that online can actually be an important tool for preventing and detecting fraud.
- Support development and dissemination of a coordinated message to maintain public confidence in the safety and soundness of online financial services.
- Urge Internet Service Providers (ISPs) to exercise a higher duty of care to protect against phishing and other forms of Internet fraud, and if appropriate, encourage regulation and legislation to achieve this result.

Encourage law enforcement to prosecute cyber criminals and identity thieves, and publicize US government efforts to do so. These efforts help to reassure the public and businesses that the Internet is a safe place and electronic commerce is an important part of the Nation’s economy.

Security Breach Customer Notice

Legislatures and regulatory agencies have enacted or proposed laws and regulations mandating that financial institutions notify customers in response to security breaches.

The members of BITS and The Financial Services Roundtable believe:

- Financial institutions have a strong track record in protecting customer information and in communicating with customers when security concerns arise.
- Protecting customer information is of paramount concern and our member institutions have taken a proactive approach in this regard. Examples of these efforts include the creation of the Identity Theft Assistance Center (ITAC) as well as guidelines and best practices for reducing fraud, managing third party providers, engaging law enforcement agencies, and communicating with customers.
- Financial institutions should have the flexibility to develop their own risk-based approaches toward dealing with unauthorized access to customer information, whether at their own operations or with a third party service provider, within the current guidelines set forth in section 501b of GLBA. For example, financial institutions should be given flexibility in determining a course of action when they “flag” and secure accounts that have been threatened.
- Notifying customers is a complicated and complex process and can, if poorly done, undermine confidence in the financial services industry. Care must be exercised in alerting consumers to steps they can take to protect themselves from ID theft and other forms of fraud while averting needless alarm.
- Efforts by various states and regulatory agencies raise significant implementation problems for financial institutions. In a transient society, notification should occur uniformly regardless of which state the consumer may live in. Moreover, inconsistent application of inconsistent state law inevitably creates a compliance nightmare for institutions with a multi-state presence.

The members of BITS and The Financial Services Roundtable further resolve to:

- Urge legislators and regulators to support risk-based approaches for determining when and how to notify customers.
- Urge legislators and regulators to adopt uniform national standards to avoid serious implementation problems and inconsistent applications.
- Urge legislators and regulators to mandate notification only when there is some indication that the breach actually has the potential to cause harm or injury. If harm is demonstrably contained, for example, and no risk really exists, there should not be any reason to notify and scare people.
- Urge legislators and regulators to require companies that discover breaches in security to immediately notify law enforcement authorities, as well as consumer reporting agencies, so that law enforcement authority can get a jump on any existing criminality and Credit Reporting Agencies may be better prepared for the potential volume of consumer inquiries about the impact of any breach on consumer credit history.
- Support measures to impose caps on damages. Any allowable damages should have firm caps and there should be no damages absent a showing of intent or actual harm. Absent negligence, an affirmative defense should be available if the company can demonstrate that it is a victim of fraud.

- Support measures that provide “safe harbors” from lawsuits. Companies should be afforded some form of safe harbor from lawsuits if they have instituted reasonable internal notification procedures.
- Continue to work with service providers, law enforcement agencies, and regulatory agencies to develop efficient and effective means of notifying customers while ensuring that appropriate steps are taken to investigate crimes.
- Continue to respond aggressively to the escalation in identity theft and online fraud through the BITS Fraud Reduction Program and the Identity Theft Assistance Center (ITAC).

RECOMMENDATIONS FOR GOVERNMENT AND POLICY MAKERS

BITS is sought to provide expert testimony, including at Congressional Hearings, on issues related to critical infrastructure protection, cyber security, and other topics at the intersection between technology, commerce and financial services in the US economy. BITS provides input to the Federal Government's efforts to strengthen cyber security and consistently urges the Government to implement provisions outlined in the "National Strategy to Secure Cyberspace." BITS also participates in an ongoing dialogue on cyber security issues among financial institutions, leading software providers, Internet service providers, and government officials, including law enforcement and regulatory agencies. BITS has developed the following recommendations.

What Government and Policy Makers Can Do to Strengthen Cybersecurity: PREPARE©

The following are seven elements of steps the Government can take to strengthen cybersecurity. Any easy way to remember this is by the acronym, PREPARE.

Promote. Government can play an important role in promoting the importance of secure information technology. Also, government should do more to facilitate collaboration among critical infrastructure sectors and government. Some sectors, such as financial services, are heavily regulated and supervised to ensure that customer information is protected and that financial institutions operate in a safe and sound manner. Examples of actions the government can take include:

- Government should lead by example by ensuring that the issue of cyber security receives adequate attention in the Department of Homeland Security.
- Strengthen information sharing coordination mechanisms, such as the Information Sharing and Analysis Centers (ISACs), by ensuring adequate funding is made available to Federal agencies sponsoring such organizations. Information sharing and trend analysis within a sector is essential to protecting information security and responding to events. Information sharing among sectors is equally important as cyber threats sometimes reach some sectors before others.
- Create an emergency communication and reconstitution system in the event of a major cyber attack or disruption of information networks. Such an attack or disruption could potentially cripple many of the primary communication channels. To allow maximum efficiency of information dissemination to key individuals in such an event, a thorough and systematic plan should be in place. The financial services industry employs a system for industry-specific events through the BITS/FSR Crisis Communicator. Other organizations have developed similar communication mechanisms. These emergency communications programs should be examined as potential models for a national cyber security emergency communication system.
- Reform of the Common Criteria/National Information Assurance Partnership (NIAP). The current software certification process is costly, inefficient, used on a limited basis by the Federal government, and virtually unknown to the private sector. NIAP should be reformed so that it is more cost effective for vendors to seek certification while ensuring consistent Federal procurement practices and expanded commercial adoption of NIAP-certified products. The BITS Product Certification Program may well be able to serve as a model.

Responsibility. Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products. Examples of actions the government can take include:

- Provide tax or other incentives for achieving higher levels of Common Criteria certification. Incremented incentives would help to compensate companies for the time and cost of certification. This should encourage certification and increase the overall security of hardware and software.

- Provide tax or other incentives for certification of revised or updated versions of previously certified software. Under Common Criteria, certification of updated versions is costly and time consuming. Incentives are necessary to ensure that all software is tested for security
- Require software providers to immediately notify ISACs of newly discovered cyber threats and to provide updated information on such threats until an effective patch is provided. It is vital that critical infrastructure companies receive immediate notice of serious vulnerabilities.
- Establish requirements that improve the patch-management process to make it more secure and efficient and less costly to organizations.

Educate. Communicate to all users of information technology the importance of safe practices. Public confidence in e-commerce and e-government is threatened by malicious code vulnerabilities, online fraud, phishing, spam, spyware, etc. Ensuring that users (home users, businesses of all sizes, and government) are aware of the risks and take appropriate precautions is an important role for government and the private sector.

Procure. Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the IT industry to deliver and implement more secure systems. Examples of actions the government can take include:

- Require high levels of cyber security in software purchased by the government through procurement procedures. Extend such requirements to software used by government contractors, subcontractors, and suppliers.
- Provide NIST with adequate resources to develop minimum cyber security requirements for government procurement. NIST should include software developers and other stakeholders in the standard-creation process.

Analyze. Government should collect information and analyze the costs and impact of information security risks, vulnerabilities and threats and provide this analysis to policy makers. Examples of actions the government can take include:

- Assign to the Commerce Department or another appropriate agency the responsibility of tracking and reporting such costs and their impact on the economy. Measuring and making these costs transparent will aid law makers and regulators as they assign resources to cyber security programs.

Research. Government can play an important role in funding R&D in the development of more secure software development practices, testing and certification programs. In addition, training future generations of programmers, technicians and business leaders that understand and manage information security can be accomplished by establishing university and educational/certification programs. Government can help by facilitating collaboration with the users and suppliers of IT to develop standards for safe practices. Examples of actions the government can take include:

- Enhance DHS, NSF, and DARPA cyber security R&D funding.
- Carefully manage long- and short-term R&D to avoid duplication.
- Establish a mechanism to share educational training and curricula.

Enforce. Law enforcement must do more to enforce, investigate and prosecute cyber crimes here and abroad. Examples of actions the government can take include:

- Enhance criminal penalties for cyber crimes.
- Make cyber crimes and identity theft enforcement a higher priority among law enforcement agencies.

RESOURCES

BITS Website, www.bitsinfo.org

ITAC website: <http://www.identitytheftassistance.org/home/index.cfm>

BITS Publications

BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information (October 2006) See
<http://www.bitsinfo.org/downloads/Publications%20Page/bitsaba.pdf>

BITS Key Considerations for Securing Data in Storage and Transport: Securing Physical Media in Storage, Transport, and for Data Erasure and Destruction (April 2006). See
<http://www.bitsinfo.org/downloads/Publications%20Page/bitsdatatrans.pdf>

BITS Fraud Prevention Toolkit: Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation (February 2006). See
<http://www.bitsinfo.org/downloads/Publications%20Page/bitstoolfeb06.pdf>

BITS Critical Success Factors for Security Awareness and Training Programs (September 2005). See
<http://www.bitsinfo.org/downloads/Publications%20Page/bitssecaware.pdf>

BITS Fraud Reduction Guidelines: Strategies for Identity Theft Prevention (July 2003). See
<http://www.bitsinfo.org/downloads/Publications%20Page/bitsfraudguidelinesJUL.Y03.pdf>

Financial Identity Theft: Prevention and Consumer Assistance (June 2003). See
<http://www.bitsinfo.org/downloads/Publications%20Page/bitsidtheftwhitepaper.pdf>

Fraud Prevention Strategies for Internet Banking (April 2003). See
<http://www.bitsinfo.org/downloads/Publications%20Page/mointernetwp.pdf>

Federal Resources

Federal Trade Commission <http://www.consumer.gov/idtheft/>

Department of Justice <http://www.usdoj.gov/criminal/fraud/idtheft.html>

U.S. Postal Inspection Service <http://www.usps.gov/postalinspectors/>

U.S. Secret Service <http://www.secretservice.gov/>

Federal Deposit Insurance Corporation <http://www.fdic.gov/consumers/>

Credit Reporting Bureaus

Equifax <http://www.equifax.com/>

Experian <http://www.experian.com/>

TransUnion Corporation <http://www.tuc.com/>