



BITS

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

January 19, 2007

To: Federal Identity Theft Task Force
Via e-mail: Taskforcecomments@idtheft.gov
Identity Theft Task Force (P065410)
Federal Trade Commission/Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Dear Sir/Madam,

The Financial Services Roundtable (Roundtable) and BITS, on behalf of our member companies, appreciate the opportunity to comment on the Federal Identity Theft Task Force report which was released for public comment on December 28, 2006. The purpose of this letter is to provide the Federal Trade Commission (FTC), the Department of Justice and the interagency working group with comments on each of the sections of the public notice document. We have inserted the text of the public notice followed by our comments in the attachment. We also have included additional information in the appendices on BITS, the Roundtable, and our activities in preventing fraud and identity theft, assisting victims of identity theft, and securing sensitive information.

General Comments

Financial institutions have always been a favorite target for perpetrators of fraud and identity theft. Financial institutions have long answered this challenge with reliable business controls as required by regulation, advanced technology, knowledge sharing, and cooperative efforts with government and law enforcement agencies. Our members view our statutory data protection requirements as dynamic. Our member institutions work continuously to improve risk management systems and implement business practices to combat fraud and fight identity theft. Experts from Roundtable and BITS member institutions constantly cooperate with each other to analyze threats, create business practices and tools, and urge the software and technology industries to provide more secure products and services.¹

As the Task Force deliberates on policy solutions to the identity theft problem, we believe it is critically important that the Task Force use an accurate and practical definition of identity theft in addition to relying on accurate statistics of the problem and its impact on society. We do not believe that identity theft should be confused with simple fraud. Suggesting that

¹ Roundtable and BITS membership is comprised of 100 of the largest integrated financial services companies providing banking, insurance, investment products, and other financial services to American consumers. Please see Appendix C for a list of members.

every instance of fraud is identity theft exaggerates the identity theft problem and leads to conclusions that this serious crime is a far more pervasive crime than is supported by reality. 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.

In September 2006, BITS and the Roundtable submitted a comment letter to the FTC and other agencies on the proposed "Red Flags Rule" which implements sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).² In that letter, we urged the agencies to consider applying the following definition of "financial identity theft" that the BITS Identity Theft Working Group and BITS Fraud Reduction Steering Committee developed.

"Identity theft" is the unlawful act of capturing, transferring and/or using one or more pieces of another person's personal identifying information (including, but not limited to name, address, driver's license, date of birth, Social Security number, account information, account login credentials, or family identifiers) and using or attempting to use that information to establish or take over a credit, deposit, or other financial account ("account") in that person's name. Identity theft falls into one of two categories:

True name fraud: Establishing (or attempting to establish) an account(s) using another person's identity.

Account takeover: Establishing (or attempting to establish) control of an existing account(s) without authority of the account holder. Account takeover does not include solely the posting of unauthorized transactions against an existing account, such as, forged maker signature, counterfeit, credit card misuse.

Identity theft does not include identity manipulation/fraud, which is creating a fictitious identity using fictitious data combined with real information from multiple individuals, and then using this fictitious identity to establish (or attempt to establish) an account(s).

There are numerous statistics on fraud and ID theft cited by the media. Many statistics are not accurate. Including accurate statistics in the Task Force's report is critically important because it will have a significant influence on policy positions and government resource allocations. Among organizations that have developed credible statistics is Javelin Strategy and Research who reported that the number of U.S. adult victims of identity fraud declined from 10.1 million people to 8.9 million people between 2003 and 2006³. In this same study, Javelin reported that 47 percent of all identity theft is perpetrated by friends, neighbors, in-home employees, family members or relatives. The perpetrator is typically someone who the

² See

<http://www.bitsinfo.org/downloads/Comment%20letters/BITS&RoundtableRedFlagsCommentLetterFINAL.pdf>

³ From The 2006 Identity Fraud Survey Report released by the Council of Better Business Bureaus and Javelin Strategy & Research

victim can identify as the perpetrator of the data compromise. Further, we understand that the Justice and Homeland Security Departments are working on a National Cyber Security Survey (via The RAND Corporation). Our understanding is that the results will provide the most accurate picture to date of cyber crimes (including ID theft).

We appreciate the Task Force's focus on law enforcement efforts to address significant investigative and jurisdictional issues. Greater focus on the problems that financial institutions and victims have with jurisdiction (e.g., where the crime occurs versus where the victim lives, difficulty victims have in getting a particular law enforcement agency to take the report and begin an investigation, threshold for when law enforcement agencies will initiate an investigation or prosecution, conflicts about which agency has primary jurisdiction) will ultimately help victims and help law enforcement agencies coordinate better and allocate resources appropriately.

Please see our detailed comments in the attachment, as well as the information on industry efforts to address the identity theft problem in appendix B. If you have any further questions or comments on this matter, please do not hesitate to contact us or John Carlson, Executive Director of BITS, at john@fsround.org or 202.589.2442.

Sincerely,

Handwritten signature of Catherine A. Allen in cursive script, followed by a vertical red line.

Catherine A. Allen
CEO, BITS

Handwritten signature of Richard M. Whiting in cursive script.

Richard M. Whiting
Executive Director and General Counsel
The Financial Services Roundtable

Attachments

ATTACHMENT: SPECIFIC COMMENTS ON THE PUBLIC NOTICE DOCUMENT

I. MAINTAINING SECURITY OF CONSUMER DATA

The Task Force Interim Recommendations addressed data security in the public sector by calling for examination by federal agencies of their collection and uses of Social Security numbers (SSNs), the piece of information that is often most effective in committing identity theft. The Task Force also recommended that the Office of Management and Budget conduct a survey to assess how well agencies protect the sensitive consumer data they maintain, and recommended that the Office of Personnel Management identify and eliminate the gratuitous use of SSNs in human resources forms used by federal agencies. The Task Force is considering whether additional measures, including the following, should be taken to further enhance the protection of sensitive consumer information and thus keep it out of the hands of identity thieves:

1. Government Use of SSNs

Because SSNs are frequently used to facilitate identity theft, the Task Force currently is exploring ways to achieve reduced reliance on SSNs by federal, state, and local government. To the extent this is important, what steps (including working with state and local governments to highlight and discuss the vulnerabilities created by the use of SSNs and to explore ways to eliminate unnecessary use and display of SSNs) could help to achieve this goal? On a related issue, please provide any comments that you may have on what information could be used as a substitute for SSNs.

BITS and Roundtable Comments: In recent years, the financial services industry has assessed the need to use SSNs in customer and employment relationships and has reduced the use of SSNs in many situations as well as applied technologies and procedures to protect them (e.g., greater use of encryption technology, data masking). The industry supports similar efforts by federal, state and local governments to examine their use of SSNs and to reduce their reliance upon them. At the same time, SSNs continue to serve a vital business function. Financial institutions and other legitimate organizations would be concerned if new limits were placed on those institutions' abilities to use SSNs as identifiers, particularly for purposes of protecting against fraud.

While financial institutions want to reduce access to and use of SSNs by fraudsters and other criminals, the simple fact is that SSNs have a special status as the only truly unique, nationwide individual identifier. For example, name alone is inadequate because there are so many duplicates (and so much room for ambiguity with initials, diminutives, Jr., Sr., etc.), and even name plus address often fails because of frequent address changes. Without a national identifier, it will make it harder for legitimate businesses to identify or verify the identity and thus make it easier for fraudsters to perpetrate crimes. If SSNs become unavailable to government and legitimate businesses as a unique identifier, society will need another national identifier.

There are some alternatives worth exploring including restricting the use of the complete SSN for most purposes, particularly when it is used for verification rather than identification purposes, for which the last 4 or 6 digits is usually sufficient.

Further, the government should take into account the use of SSNs for tax reporting and auditing purposes and what impact the restriction of SSNs might have on this important requirement.

Until there is a reasonable alternative, it is important for the government to work with legitimate businesses to develop solutions. For example, the financial services industry would like an enhanced ability to verify SSNs used in new account opening procedures against those held by the Social Security Administration (SSA). BITS has submitted a document to the SSA outlining financial services industry's business requirements for such a process. (See comments below under "comprehensive record on private sector use of SSNs.")

Whatever proposed solutions and alternatives are considered, we ask the Task Force to weigh heavily any possible unintended consequences, and particularly those that could inadvertently increase fraud and reduce the overall security of the financial services infrastructure and protection for consumers. Further, any restrictions on the use of SSNs must ensure the continuation of legitimate law enforcement uses and also consider business uses including the sale, merger, or acquisition of companies.

2. Comprehensive Record on Private Sector Use of SSNs

The Task Force, in seeking to address the extent to which the availability of SSNs to identity thieves creates the possibility of harm to consumers, is considering whether to recommend that the Task Force investigate and analyze how SSNs are currently used in the private sector, and how these uses could be modified or limited to help minimize the unnecessary exposure of SSNs and/or to make them less valuable in committing identity theft. Would such an effort be helpful in addressing the problem of identity theft? To what extent would such an effort be the appropriate way to gather this information?

BITS and Roundtable Comments: In the interest of reducing fraud and complying with numerous legal requirements, our members support efforts by the Social Security Administration (SSA) to establish a verification program that will allow financial institutions to affirmatively verify a consumer's name, social security number and date of birth (DOB). Establishing a "real-time" verification system capable of processing high volumes at a 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. Erroneous data entry of consumer's SSNs would also be easily determined, reducing the incidence of erroneous tax reporting on interest earned and deductible interest expense and reducing the quantity of consumers required to be subjected to annual solicitation for a corrected SSN due to mismatches submitted to the IRS and misrepresentation. Consumers would also benefit from the industry's ability to

verify SSN information by reducing the incidence of fraud as well as errors from erroneous data entry of consumer's SSNs.

In July 2006, BITS authored 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 on the development and use of a consent-based verification program that meets the needs of the customers, the industry, and the agency.

During a July 2006 meeting with BITS and the SSA, BITS was tasked with gathering information from our member financial institutions regarding their anticipated participation in a Consent Based Social Security Number Verification (CBSV) program. BITS asked members to provide information regarding:

- Estimated daily request volume-processing capacity for SSN verification inquiries;
- Number of times the financial institution (FI) contacts the SSA local field office for information related to and/or confirmation of an SSN;
- Whether the FI would participate in the proposed CBSV program when it becomes available;
- Estimated average cost to the financial institution of fraud transactions that could be prevented with a CBSV program; and
- Anecdotes to support the importance of such a CBSV system.

In November 2006, BITS transmitted the results of the survey to members and the SSA. The survey revealed strong interest from US financial institutions for a consent-based verification program. However, financial institutions that responded to the survey indicated there are several impediments to broader participation in a verification program. Financial institutions noted that more would participate in the CBSV program if it:

- Is automated;
- Does not require paper consent forms;
- Has minimum delays in verifications;
- Includes a reasonable cost for verification;
- Has reasonable record keeping requirements; and
- Addresses the need for ID verification processes for non-US citizens.

Participants indicated that the greatest value to the financial institutions via an enhanced CBSV program would be the ability to:

- Verify the identity of an applicant;
- Reduce instances of identity theft;
- Facilitate compliance with the Customer Identification Program (CIP) as required by Section 326 USA PATRIOT Act);
- Reduce losses due to fraud or loan defaults;
- Enhance customer service, as financial institutions would not have to ask customers to go to their local SSA office to validate their SSN; and
- Detect and reduce erroneous tax reporting.

3. National Data Security Standards

The Task Force is considering whether to recommend that national data security requirements be imposed on all commercial entities that maintain sensitive consumer information. Would such national requirements be helpful in addressing any deficiencies in current data security practices? If so, what would be the essential elements of such a requirement? Does the need for such a national standard, if any, vary according to economic sector, business model, or business size? On a related note, please provide any comments that you may have on the costs of imposing a national data security requirement on businesses.

BITS and Roundtable Comments: We urge legislators and regulators to adopt uniform national standards for both information safeguards and notice on all entities that maintain sensitive consumer information. It is crucial that such standards not be limited to commercial entities, but also apply to other organizations (e.g., universities) that maintain significant amounts of sensitive personal information.

Financial institutions have long been required to employ dynamic data protection safeguards to protect sensitive data. The functional financial regulators regularly examine institutions for their compliance with information security and privacy protection safeguards that were included in the Gramm-Leach-Bliley Act of 1999 (GLBA). Given that many organizations (not just financial institutions) store, transmit or process sensitive information today, all of these organizations should be required to guard this information as stringently as entities compelled by GLBA.

4. Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information

The Task Force is considering whether to recommend that a national breach notification requirement be adopted. Would such a breach notification requirement be helpful in addressing any deficiencies in the protocols currently followed by businesses after they suffer a breach? If so, what would be the essential elements of such a national breach notification requirement? Does the need for such a national standard, if any, vary according to economic sector, business model, or business size?

BITS and Roundtable Comments: We urge the Task Force to recommend a national breach notification requirement. A national standard will avoid serious implementation problems and inconsistent applications. 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 varying state law inevitably creates a compliance challenge for institutions with a multi-state presence.

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.

We support risk-based approaches for determining when and how to notify customers and 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 customers or law enforcement and create unwarranted concern.

We advocate reporting security breaches to law enforcement only when the breach itself constitutes criminal activity, or there is a likelihood that the compromised information will be used for criminal purposes. There are numerous situations that may be classified as "security breaches" under current law and regulations where there is only the potential, but no reasonable chance, of harm. An extreme example would be the mis-delivery of an account statement by the Post Office. This may be classified as a "breach" under some regulations, even if the mistaken unintended recipient reports the error to a financial institution and promptly destroys or returns the statement. In our opinion, this example would not warrant law enforcement notification.

Further, we also support measures that provide "safe harbors" from lawsuits where reasonable notification procedures have been implemented and followed. We urge legislators to support measures to impose caps on damages from breaches or from failure to notify. 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 individual can demonstrate that it is a victim of fraud.

BITS and the American Bankers Association jointly released in November 2006 the "BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information." This paper is another proactive and positive action to prepare financial institutions to manage the risks associated with data breaches and to maintain consumer confidence. The 20 page paper: provides suggestions that may help financial institutions manage and respond to state laws and federal regulations that govern breach notification and response requirements; addresses various notification triggers and timing, notification methods and content, response team elements, including coordination with law enforcement and regulators, and plans for managing third party relationships prior to and after a security breach; and includes a list of guides and tools for data security, fraud reduction, ID theft prevention and assistance, and third party outsourcing.

The full document and press release are attached and are also available on the BITS and ABA websites: http://www.bitsinfo.org/p_publications.html or www.aba.com.

5. Education of the Private Sector and Consumers on Safeguarding Data

The Task Force is considering whether there is a need to better educate the private sector on safeguarding information and on what private sector entities should do if they suffer a data breach. Additionally, the Task Force is considering whether there is a need to better educate consumers on how to safeguard their personal data and how to detect and deter identity theft, through a national public awareness campaign. Are such education campaigns an appropriate way in which to address the problem of identity theft? If so, what should be the essential elements of these education campaigns for the private sector and consumers?

BITS and Roundtable Comments: Financial institutions have developed educational programs to train employees and raise awareness of customers with regard to safeguarding sensitive information. In addition, the federal financial regulators require financial institutions to develop education, awareness and training programs and examiners routinely assess the adequacy of these programs. As one example of many efforts, our member companies developed and endorsed the following voluntary guidelines.

Critical Success Factors for Security Awareness & Training Programs

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.

In November 2006, BITS published the *BITS Consumer Confidence Toolkit: Data Security and Financial Services*. This Consumer Confidence Toolkit is publicly available and provides information to support consumer confidence in the safety, soundness and security of financial services. Special attention is placed on Internet-based financial services. Data in support of the safety of online financial transactions are provided. Information about the proactive leadership of the financial services industry is included, as well as a description of the current environment and recommendations for government agencies and leadership. Tips for consumers to help protect their financial security, including in the online environment, are also provided. In addition, BITS developed the *Voluntary Guidelines for Consumer Confidence in Online Financial Services* as recommendations to member institutions for managing information security and consumer confidence issues.

II. PREVENTING THE MISUSE OF CONSUMER DATA

The Task Force is also considering how to make it more difficult for identity thieves, when they are able to obtain consumer data, to use the information to steal identities. In its interim recommendations to the President, the Task Force noted that developing more reliable methods of authenticating the identities of individuals would make it harder for identity thieves to open new accounts or access existing accounts using other individuals' information. The Task Force accordingly recommended that the Task Force hold a workshop or series of workshops, involving academics, industry, and entrepreneurs, focused on developing and promoting improved means of authenticating the identities of individuals. Those workshops will begin in early 2007. Are there any other measures that the Task Force should consider in addressing how to prevent the misuse of consumer data that has fallen into the hands of an identity thief?

BITS and Roundtable Comments: Financial institutions have a strong track record in protecting customer information and in deploying robust, risk-based, and dynamic information security programs that include authentication and encryption

technologies. We urge the Task Force to acknowledge the importance of a holistic approach based on risk modeling that takes all factors into consideration, not just authentication or other controls that may be part of a broader information security program. Here are some examples of efforts by financial institutions to develop robust, risk-based and dynamic information security programs:

- Developing enterprise-wide solutions that take into account the holistic picture and not just specific aspects of identity management and related issues.
- Making authentication easier and more acceptable to users and consumers.
- Applying encryption technology to protect sensitive information
- Making data more difficult to use even if it is disclosed.
- Educating consumers to use safe on-line computing practices.
- Supporting research into customer preferences for authentication (including multi-factor).
- Engaging 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.
- Supporting risk-based approaches for evaluating the risks, deploying controls and offering convenient solutions to consumers.
- Supporting and using the BITS Fraud Reduction Program and the Identity Theft Assistance Center (ITAC).

Further, we urge the Task Force to consider the important role government agencies play in issuing credentials that financial institutions and others use to identify, verify and authenticate uses. Financial institutions have many regulatory and legal requirements that have been implemented in recent years, including requirements from the Bank Secrecy Act (BSA), GLBA, the USA PATRIOT Act, Sarbanes Oxley Act, and the FACT Act. In order to comply with these requirements and changing risks, government agencies must issue credentials that are reliable and available to financial institutions customers. Financial institutions use these credentials to register customers.

We believe it is important for the Task Force to state that any additional legislation, regulation or guidelines should be risk-based, technology neutral, and flexible enough to encourage continuous improvement.

Stronger authentication is an important part of a risk-based information security and identity theft prevention program. However, there are many practical challenges involved in deploying multi-factor authentication technologies in real-world applications. These challenges include customer acceptance, the maturity of the technology, cost, scalability, interoperability and dependence on government-issued credentials. 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” or “man-in-the-middle” attacks. 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 various social engineering techniques such as “phishing”, and make use of that information outside the realm of on-line financial services.

Applying multi-factor authentication requirements on US financial institutions, as mandated by regulators in other countries, 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 US. These schemes are linked to school attendance, tax, immigration, driving license and other records that are associated with citizens in these jurisdictions. US laws and consumer attitudes to such approaches are at odds and often viewed as an infringement of civil rights and privacy.

III. VICTIM RECOVERY

The Task Force has been considering the barriers that victims face in restoring their identity. The Task Force has specifically addressed the following issues:

1. Improving Victim Assistance

The Task Force is considering ways in which to provide more effective assistance to identity theft victims, including, but not limited to, providing training to local law enforcement on how best to provide assistance for victims; providing educational materials to first responders that can be used readily as a reference guide for identity theft victims; developing and distributing an identity theft victim statement of rights based on existing remedies and rights; developing nationwide training for victim assistance counselors; and developing avenues for additional victim assistance through the engagement of national service organizations. Would these measures be effective ways to assist victims of identity theft? Are there any other ways to improve victim assistance efforts that the Task Force should consider?

BITS and Roundtable Comments: We urge the Task Force to take into account the experiences and success of the Identity Theft Assistance Center (ITAC), co-founded by BITS, The Financial Services Roundtable, and 50 of our member institutions,. In addition, the efforts of individual financial institutions can be helpful in providing training to law enforcement. We urge the Task Force to include information regarding the extensive work of the financial services industry to prevent all kinds of fraud, including ID theft, as well as assisting victims of identity theft. (See Appendix B for an overview of efforts by the financial services industry.)

2. Making Identity Theft Victims Whole

The Task Force has issued an interim recommendation that Congress amend the criminal

restitution laws to allow identity theft victims to seek restitution from the identity thief for the value of their time in attempting to recover from the effects of the identity theft. Are there other ways in which the government can remove obstacles to victim recovery?

BITS and Roundtable Comments: While this may be a good idea in theory, it is important to examine how it could be accomplished in practice. It is important that the Task Force recommends solutions that truly result in seeking restitution from the identity thief, especially given that many thieves today are foreign nationals living outside US law enforcement jurisdiction.

As noted above, we also urge the Task Force to take into account the experience and success of the Identity Theft Assistance Center.

3. National Program Allowing Identity Theft Victims to Obtain an Identification Document for Authentication Purposes

To give identity theft victims a means to authenticate their identities when mistaken for the identity thief in a criminal justice context, several states have developed voluntary identification documents, or “passports,” that authenticate identity theft victims. The FBI has established a similar system through the National Crime Information Center, allowing identity theft victims to place their name in an “Identity File.” The Task Force is considering whether federal agencies should lead an effort to study the feasibility of developing a nationwide system that would allow identity theft victims to obtain a document or other mechanism that they can use to avoid being mistaken for the suspect who has misused their identity. Would such a system meaningfully assist victims of identity theft? If so, what should be the essential elements of such a nationwide system?

BITS and Roundtable Comments: We believe this proposal has some merit and would be interested to learn more about it and how financial institutions can work with the government to develop such a program. In general, we support the idea of a feasibility study of a national system that would help ID theft victims avoid arrest for crimes committed in their name by imposters. In developing a pilot, we want to emphasize an earlier point that effective authentication is closely linked to reliable credentials. One of the government’s primary roles is to issue reliable credentials. It is important that the Task Force consider this and develop recommendations to improve the issuance of government credentials. During the past two years, BITS has hosted two conferences on various aspects of authentication and credentialing. Without a more thoughtful discussion of the broader issues with credentials, it is difficult to provide any meaningful comments on the proposal to “develop identification documents, or ‘passports’, that authenticate identity theft victims” without adequately explaining how this would be developed or implemented.

4. Gathering Information on the Effectiveness of Victim Recovery Measures

To evaluate the effectiveness of various new federal rights that have been afforded to identity theft victims in recent years, as well as various new state measures to assist identity theft victims that have no federal counterpart, the Task Force is considering whether to recommend (a) that the agencies with enforcement authority for the Fair and Accurate Credit Transaction Act (FACT Act) amendments to the Fair Credit Reporting Act assess the amendments’ impact and effectiveness through appropriate surveys or other means, and (b)

that agencies conduct an assessment of state credit freeze laws, including how effective they are, what costs they may impose on consumers and businesses, and what features are most beneficial to consumers. Are such studies important for formulating a national strategy on how to combat identity theft? Are there any other evaluations that should be done to assess the effectiveness of victim recovery measures?

BITS and Roundtable Comments: We believe additional study of the impact of state laws and implementation of amendments to the Fair Accurate Credit Transaction Act would be helpful. Compliance with state laws creates significant challenges for financial institutions given that the majority of financial institutions operate or have customers in multiple states. National uniformity, both geographically and across industries, is critical to preserving a fully functioning and efficient national marketplace. The differences in state laws create inconsistent standards that financial institutions must reconcile when undertaking notification following unauthorized access to sensitive customer information or mandated services such as credit monitoring to customers. We believe that the approach the financial regulators have taken with respect to implementation of the GLBA and other laws has been balanced and should be preserved. .

IV. LAW ENFORCEMENT: PROSECUTING AND PUNISHING IDENTITY THIEVES

The May 2006 Executive Order stated that it shall be the policy of the United States to use its resources effectively to address identity theft, including through “increased aggressive law enforcement actions designed to prevent, investigate, and prosecute identity theft crimes, recover the proceeds of such crimes, and ensure just and effective punishment of those who perpetrate identity theft.” The Task Force has accordingly examined various ways, including the following, by which this goal can be achieved.

1. Establish a National Identity Theft Law Enforcement Center

The Task Force is considering whether to recommend the creation of a National Identity Theft Law Enforcement Center, to better coordinate the sharing of information among criminal and civil law enforcement and, where appropriate, the private sector. Such a Center could become the central repository for identity theft complaint data and other intelligence from various sources received by law enforcement, as well as a hub for analysis of that information. The analyses could be used to provide support for law enforcement at state and federal levels in the investigation, prosecution, and prevention of identity theft crimes. The Center also could develop effective mechanisms to enable law enforcement officers from around the country to share, access, and search appropriate law enforcement information through remote access. The Center could also assist investigative agencies, before they begin a particular investigation, in determining whether another agency is already investigating a particular identity theft scheme or ring. Would the establishment of such a Center assist law enforcement in responding to identity theft? If so, what should be the core functions and elements of that Center?

BITS and Roundtable Comments: We encourage law enforcement to investigate and prosecute cyber criminals and identity thieves, and to publicize US government efforts to do so. These efforts would 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. An important consideration is the international implications of this proposal given that many identity thieves are located outside the US. It is important for US law enforcement officials to continue to make progress in working with foreign law enforcement agencies.

We also encourage the government to make sure that the proposed center has adequate security controls to avoid a situation where a criminal could breach the security controls by pretending to a victim.

The Identity Theft Assistance Center is referring data to law enforcement for further analysis beyond the resolution offered to victims through ITAC. We would be pleased to explore a similar relationship with this Center, were it to be established.

2. Ability of Law Enforcement to Receive Information from Financial Institutions

Because the private sector in general, and financial institutions in particular, are an important source of identity theft-related information for law enforcement, the Task Force is considering:

- (a) whether the Justice Department should initiate discussions with the private sector to encourage increased public awareness of Section 609(e) of the Fair Credit Reporting Act, which enables identity theft victims to receive identity theft-related documents and to designate law enforcement agencies to receive the documents on their behalf;
- (b) whether relevant federal law enforcement agencies should continue discussions with the financial services industry to develop more effective fraud prevention measures to deter identity thieves who acquire data through mail theft; and
- (c) whether the Justice Department should initiate discussions with the credit reporting agencies on possible measures that would make it more difficult for identity thieves to obtain credit based on access to a victim's credit report.

Would such measures meaningfully assist law enforcement efforts in combating identity theft and/or meaningfully assist in forming partnerships between law enforcement and the private sector? Are there any other measures that could be implemented to strengthen the relationship between the private sector and the law enforcement community in responding to identity theft?

BITS and Roundtable Comments: We support the notion of enhanced ability of law enforcement to obtain information from financial institutions provided that law enforcement can adequately safeguard the information and that financial institutions receive immunity for providing such information. Further, it is important to point out the need for law enforcement to protect the reputation of private sector organizations that are involved in investigations. There is a reluctance to engage law enforcement since their forensic and follow-up efforts can in and of themselves be more detrimental to a financial institution than any losses sustained.

In developing partnerships, the government should also focus on the leading causes of ID theft which includes friends, family and acquaintances as well as the impact of mail theft. In recent years, financial institutions have made significant progress in mitigating the impact of mail theft through change of address procedures.

3. The Investigation and Prosecution of Identity Thieves Who Reside in Foreign Countries

To address the fact that a significant portion of the identity theft committed in the United States originates in other countries, the Task Force is considering whether there are ways that the United States can work with foreign countries to better address this problem, including:

- (a) whether the Department of Justice and the Department of State should formally encourage other countries to enact suitable domestic legislation criminalizing identity theft;
- (b) whether the U.S. Government should continue its efforts to promote universal accession to the Convention on Cybercrime and assist other countries in bringing their laws into compliance with the Convention's standards;
- (c) whether the U.S. Government should encourage those countries that have demonstrated an unwillingness to cooperate with U.S. law enforcement in criminal investigations, or have failed to investigate or prosecute offenders aggressively, to alter their practices and eliminate safe havens for identity thieves;
- (d) whether the U.S. Government should recommend that Congress amend the language of 28 U.S.C. § 1782 and 18 U.S.C. § 2703 to clarify which courts can respond to appropriate foreign requests for electronic and other evidence in criminal investigations, so that the United States can better provide prompt assistance to foreign law enforcement in identity theft cases; and
- (e) whether federal law enforcement agencies should assist, train, and support foreign law enforcement through the use of Internet intelligence-collection entities. Would such measures meaningfully assist U.S. law enforcement in its ability to investigate, identify, and prosecute foreign-based identity thieves who are committing crimes in the United States? Are there any other measures that could be implemented to achieve this goal?

BITS and Roundtable Comments: Financial institutions have observed significant growth of organized cyber crime in recent years from countries with inadequate laws and/or corrupt or incompetent law enforcement officials. In 2006, the U.S. Senate ratified the Council of Europe's Convention on Cybercrime, which is the first and only international, multilateral treaty specifically addressing the need for cooperation in the investigation and prosecution of computer network crimes. This treaty requires global law enforcement cooperation with respect to searches and seizures and provides timely extradition for computer network based crimes covered under the treaty. BITS and The Roundtable had urged adoption of this treaty.

Improving law enforcement coordination within the US and with other governments is an important goal worth exploring further. Under current authority, there are significant challenges facing law enforcement agencies in terms of training, thresholds for investigating and prosecuting crimes, and how law enforcement works in partnership with legitimate business and individuals who are victims of crime. We believe that this specific focus on diplomatic and economic pressure has the potential of making a significant impact in the number of identity theft crimes committed by organizations that operate in foreign countries with limited enforcement efforts. We encourage the Task Force to continue to make progress in working with foreign governments and law enforcement agencies to tackle the law enforcement challenges.

4. Prosecutions of Identity Theft

The Task Force is considering whether steps can be taken to increase the number of state and federal prosecutions of identity thieves, including (a) requiring each United States Attorney's Office to designate an identity theft coordinator and/or develop a specific Identity Theft Program for each District, including evaluating monetary thresholds for prosecution, (b) formally encouraging state prosecutions of identity theft, and (c) creating working groups and task forces to focus on the investigation and prosecution of identity theft. Would these measures meaningfully assist in increasing the number of identity theft prosecutions? Are there any other measures that can be implemented that would increase state and federal prosecutions of identity thieves?

BITS and Roundtable Comments: We urge the government to develop more effective programs to investigate and prosecute identity theft cases as well as cyber crimes. As noted above, law enforcement agencies should focus on investigative and jurisdictional issues to make the process easier on victims and organizations that may be involved in the process (including financial institutions).

5. Targeted Enforcement Initiatives

The Task Force is considering whether to propose that law enforcement agencies undertake special enforcement initiatives focused exclusively or primarily on identity theft, including specific initiatives focused on (a) unfair or deceptive means to make SSNs available for sale; (b) identity theft related to the health care system; and (c) identity theft by illegal aliens. Additionally, the Task Force is considering whether to recommend that federal agencies, including the SEC, the federal banking agencies, and the Department of Treasury review their supervisory and compliance programs to assess whether they adequately address identity theft and create sufficient deterrence. Would these special initiatives be useful in prosecuting and punishing identity thieves? Are there any other such special enforcement initiatives that could make a difference in deterring and punishing identity thieves?

BITS and Roundtable Comments: We support federal law enforcement efforts to deter would be criminals. These deterrence efforts should explicitly cover electronic means of committing ID theft crimes. We also believe it is important to note that financial institutions already have numerous efforts and controls in place to prevent and mitigate ID theft. See appendix B for details and the link to our detailed comment letter on the proposed ID Theft Red Flags Rule (<http://www.bitsinfo.org/downloads/Comment%20letters/BITS&RoundtableRedF>)

[lagsCommentLetterFINAL.pdf](#)). While the FTC and the federal financial agencies have not released the final rule, we believe that implementation of the "red flag" guidelines under FACTA will be another major step in that direction.

6. Amendments to Federal Statutes and Guidelines Used to Prosecute Identity-Theft Related Offenses

The Task Force is considering whether to recommend that Congress amend the identity theft and aggravated identity theft statutes to ensure that identity thieves who misappropriate information belonging to corporations and organizations can be prosecuted, and add several new crimes to the list of predicate offenses for aggravated identity theft offenses, such as mail theft, uttering counterfeit securities, tax fraud, and conspiracy to commit those crimes. The Task Force is also considering whether to recommend that Congress amend 18 U.S.C. § 1030(a), the statute that criminalizes the theft of electronic data, by eliminating the current requirement that the information must have been stolen through interstate communications. Further amendments under consideration by the Task Force include:

- amending 18 U.S.C. § 1030(a)(5) by eliminating the current requirement that the defendant's key-logging or malicious spyware actions must cause "damage" to computers and that the loss caused by the conduct must exceed \$5,000;
- amending the cyber-extortion statute, 18 U.S.C. § 1030(a)(7), to cover additional, alternate types of cyber-extortion;
- outlawing pretexting by providing both criminal and civil penalties for such conduct;
- enacting legislation that would make it a felony for data brokers and telephone company employees to knowingly and intentionally sell or transfer customer information without prior written authorization from the customer, with appropriate exceptions for law enforcement purposes;
- amending the U.S. Sentencing Guidelines to ensure that an identity thief's sentence can be enhanced when the criminal conduct affects more than one victim; and
- amending the definition of "victim," as that term is used under United States Sentencing Guideline section 2B1.1, to state clearly that a victim need not have sustained an actual monetary loss.

Would such amendments meaningfully assist prosecutors in charging, convicting, and ensuring the just punishment of identity thieves? Are there any other potential amendments to the provisions of the United States Code or U.S. Sentencing Guidelines that the Task Force should consider?

BITS and Roundtable Comments: These proposals are worth further exploration with the caveat that there are often unintended consequences from statutory changes. In general, we encourage policy-makers to pursue legitimate uses and if we need to get input then determine what these uses might be. While "pretexting" is a

sensitive issue, it is important to bear in mind that pretexting may be useful for legitimate purposes, including law enforcement, collection, and fraud detection techniques. Most of the other proposals in this section are probably harmless or even desirable.

7. Training for Law Enforcement Officers and Prosecutors

The Task Force is considering whether to recommend enhancing the training for law enforcement officers and prosecutors who investigate and prosecute identity theft offenses, including by: (a) developing a course at the National Advocacy Center (NAC) focused solely on investigation and prosecution of identity theft; (b) increasing the number of regional identity theft seminars hosted by the U.S. Postal Inspection Service, Justice Department, Federal Trade Commission, U.S. Secret Service, and American Association of Motor Vehicle Administrators; (c) increasing resources for law enforcement available on the internet, including by ensuring that an Identity Theft Clearinghouse site could be used as the portal for law enforcement agencies to gain access to additional educational materials on investigating identity theft and responding to victims; and (d) reviewing curricula to enhance basic and advanced training on identity theft. Are these measures necessary or helpful to law enforcement officers and prosecutors? Are there any other such training initiatives that the Task Force should consider?

BITS and Roundtable Comments: We support increased training for law enforcement officers in electronic means of committing ID theft. We also encourage law enforcement agencies to develop better, more effective ways to “partner” with financial institutions.

8. Measuring Law Enforcement Efforts

Because there is limited data on law enforcement efforts in the area of identity theft, the Task Force is considering whether additional surveys and statistical analysis are needed, including whether to: (a) expand the scope of the National Crime Victimization Survey; (b) review U.S. Sentencing Commission data on identity theft-related case files every two to four years; (c) track federal prosecutions of identity theft and the amount of resources spent on such prosecutions; and (d) conduct targeted surveys in order to expand law enforcement knowledge of the identity theft response and prevention activities of state and local police. Would such surveys be helpful to the law enforcement community? Are there any other such surveys or measurements that the Task Force should consider? On a related issue, are the data sets that are currently available that relate to the frequency, cost, and type of identity theft sufficient to give us a full understanding of the problem of identity theft?

BITS and Roundtable Comments: There are many surveys on ID theft. Many of these surveys are not reliable. We encourage the Task Force to take into account the findings from a major cyber security study that Department of Homeland Security and the Department of Justice has sponsored (and managed by The RAND Corporation). In 2005 and 2006, The RAND Corporation asked BITS and other major associations to encourage members to complete the survey. The RAND Corporation indicated that the study will yield accurate information on cyber security risks and impact on the private sector as well as provide a sound basis for determining government funding for law enforcement and cyber security programs.

APPENDIX A: ABOUT THE FINANCIAL SERVICES ROUNDTABLE AND BITS

The Financial Services Roundtable is a national association that represents 100 of the largest integrated financial services companies providing banking, insurance, investment products, and other financial services to American consumers. 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 is a nonprofit industry consortium that shares its membership with The Financial Services Roundtable. BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect. 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. BITS' activities are driven by the CEOs and their direct reports—CIOs, CTOs, Vice Chairmen and Executive Vice President-level executives of the businesses.

Members of BITS are sharing information, analyzing threats, creating best practices, urging the software and technology industries to do more to provide more secure products and services, and combating fraud and identity theft. By sharing information, developing and disseminating guidelines and successful strategies, and fostering open dialogue, BITS members have helped to decrease the risks associated with fraud and identity theft. Where identity theft does occur, BITS members are proactive. BITS and the Roundtable, with fifty of our member institutions, co-founded the Identity Theft Assistance Center (ITAC) in 2004. As of January 2007, the ITAC has helped over 10,000 individuals to restore their financial identity. These services are provided free to consumers by ITAC members.

Within BITS there are two working groups that have a strong interest in identity theft and related issues—the information security experts who are involved in the BITS Security and Risk Assessment (SRA) Working Group and the fraud reduction experts who are involved in the BITS Fraud Reduction Steering Committee (FRSC). The mission of the SRA is to strengthen the security and resiliency of financial services by sharing and developing best practices to secure infrastructures, products and services; maintaining continued public and private sector confidence; and providing industry input to government agencies and regulators on policies and regulations. The mission of the FRSC is to identify fraudulent trend activity, reduce fraud losses, and foster new opportunities to reduce the impact of fraud on the financial services industry and our customers. Participants in the BITS Fraud Reduction Steering Committee include representatives from financial institutions, industry associations and the Federal Reserve.

Much of BITS' work is published for the entire financial services industry to use in efforts to combat fraud and tackle identity theft. Please see the BITS web site to access public documents on efforts to address fraud, identity theft, and a range of relevant security-related issues: http://www.bitsinfo.org/p_publications.html.

APPENDIX B: BITS IDENTITY THEFT PREVENTION, ID THEFT ASSISTANCE AND DATA SECURITY EFFORTS

PUBLICATIONS OF BEST PRACTICES AND GUIDELINES

- ***BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information***

On November 16, 2006, BITS and the American Bankers Association jointly released a new tool, "BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information." This paper is another proactive and positive action to prepare financial institutions to manage the risks associated with data breaches and to maintain consumer confidence. The 20 page paper: 1) provides suggestions that may help financial institutions manage and respond to state laws and federal regulations that govern breach notification and response requirements; 2) addresses various notification triggers and timing, notification methods and content, response team elements, including coordination with law enforcement and regulators, and plans for managing third party relationships prior to and after a security breach; and 3) includes a list of guides and tools for data security, fraud reduction, ID theft prevention and assistance, and third party outsourcing. The paper was endorsed by The Roundtable Board in September 2006. The document is available on the BITS and ABA websites: <http://www.bitsinfo.org/downloads/Publications%20Page/BITSABADBNov06.pdf> or www.aba.com.
- ***BITS Key Considerations for Securing Data in Storage and Transport: Securing Physical Media in Storage, Transport, and for Data Erasure and Destruction***

BITS released the "BITS Key Considerations for Securing Data in Storage and Transport" paper in April 2006. This framework helps financial institutions evaluate and mitigate the risks associated with the transport and storage of physical media and the destruction or erasure of data and 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 paper was endorsed by the Roundtable Board in March 2006 and is publicly available on the BITS website: <http://www.bitsinfo.org/downloads/Publications%20Page/bitsdatatrans.pdf>.
- ***BITS Fraud Protection Toolkit: Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation***

In February 2006, BITS released an updated "BITS Fraud Protection Guide: Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation." The toolkit helps financial institutions in implementing or improving a financial institution's internal program for education and awareness of abuse and exploitation against the elderly and vulnerable. The Toolkit includes a narrative Word document and a PowerPoint to support financial institution's internal education and training programs. In addition to use by financial institutions, state agencies have requested to use and reproduce the

Toolkit which is freely available at
<http://www.bitsinfo.org/downloads/Publications%20Page/bitstoolfeb06.pdf>.

- ***BITS Consumer Confidence Toolkit and Voluntary Guidelines***
In November 2006, BITS published an updated *Consumer Confidence Toolkit: Data Security and Financial Services*. This Consumer Confidence Toolkit is publicly available and provides information to support consumer confidence in the safety, soundness and security of financial services. Special attention is placed on online financial services transacted through the Internet. Data in support of the safety of online financial transactions are provided. Information about the proactive leadership of the financial services industry is included, as well as a description of the current environment and recommendations for government agencies and leadership. Tips for consumers to help protect their financial security, including in the online environment, are also provided. In addition, BITS has developed Voluntary Guidelines as recommendations to member institutions for managing information security and consumer confidence issues.
- ***Remote Deposit Image Capture: The Processes, Risks, and the Strategies used to Mitigate Them***
In September 2006, the BITS Electronification Working Group released a paper on Remote Deposit Image Capture (RDIC) services that identifies the benefits and the risks associated with offering RDIC and offers strategies to mitigate the risks. It is freely available at
<http://www.bitsinfo.org/downloads/Publications%20Page/BITSRDICFINALSept06.pdf>
- ***BITS Patch Management Guide***. *BITS Best Practices in Patch Management* provides critical recommendations for an enterprise approach to managing patches. Divided into 10 sections reflecting the components of effective patch management processes, the document provides considerations for defining roles, responsibilities and tools; developing and maintaining an inventory of IT infrastructure; developing a “standard build”; and verifying patch installation. While created for financial institutions, these recommendations may be applied to other industries. See
<http://www.bitsinfo.org/downloads/Publications%20Page/bitspatchmgmt2004.pdf>
- ***BITS IT Service Providers Expectations Matrix***. The *BITS IT Service Provider Expectations Matrix* provides financial institutions, service providers, and audit and assessment organizations with comprehensive and consistent expectations to reduce risk. Presented in an Excel spreadsheet, it outlines financial institution expectations for the security of information and personnel, as well as policies and processes for ensuring physical security. The expectations address critical disaster recovery/business continuity issues necessary to ensure products and services are supported by and coordinated with service providers.
- ***BITS Key Considerations for Global Background Screening Practices***. BITS released the *BITS Key Considerations for Global Background Screening Practices* in June 2005. This document is an outstanding tool for financial institutions and other critical infrastructure companies seeking to mitigate risks related to global outsourcing. The

paper is divided into three sections: 1) overview of the financial industry's legal and regulatory requirements; 2) strategies for evaluating the risks and mitigating controls for outsourced environments and activities; and 3) information to validate identity and background, listed by country. Each section outlines financial institutions' top considerations for global employee screening policies, programs and requirements. The paper is available on the BITS website at www.bitsinfo.org on the publications page.

- **Key Contractual Considerations for Developing an Exit Strategy.** Published in May, 2005, the *BITS Key Contractual Considerations for Developing an Exit Strategy* provides detailed suggestions for contracts with third party service providers. For all critical infrastructure companies, developing an exit strategy at the onset of the relationship can help the organization effectively manage risk and ensure continuity of service.
- **Fraud Prevention Strategies for Consumer, Commercial and Mortgage Loan Departments.** Loan fraud is a fast-growing problem. This Members' Only guide helps financial institutions catch loan frauds as they happen and recover from related losses. Members interested in obtaining a copy may access it via the BITS site, www.bitsinfo.org, in the Members Only area.
- **BITS Guide to Verification, Authentication and Financial Experience Information Technology for Online New Account Openings.** In January 2005 BITS published the *BITS Guide to Verification, Authentication and Financial Experience Information Technology for Online New Account Openings*. This Members' Only guide assists financial institutions in understanding technology to verify and authenticate online users and determine the level of risk users pose to the institution. This document was created to help financial institution fraud managers as they explore these technologies and identify those that may be appropriate for their needs. This paper focuses on technology solutions for:
 - Verification. These products screen data elements provided by a client to ensure the elements (Social Security numbers, addresses, etc.) are real.
 - Authentication. Once the data elements are verified, authentication products ensure the credentials given belong to the person providing them.
 - Financial experience information. Having verified the data elements and authenticated the customer, financial experience information determines the level of risk assumed by accepting the potential customer.
- **BITS Calculator: Key Risk Management Tool for Information Security Operational Risks.** The *Calculator* starts with a list of common information security threats and vulnerabilities and matches them with corresponding controls to mitigate those risks. Using the *Calculator*, financial institutions score their information security risks based on the likelihood of an incident, the degree to which the organization has defended itself against the threat, and the incident's possible impact. Companies can use the results to boost their ability to assess and mitigate risks. The *Calculator* is unique in that it brings together information security risk categories from international security standards and emerging operational risk regulatory requirements into one tool that can be easily customized.

- **Developing a KRI Program: Guidance for the Operational Risk Manager.** The document, *Developing a KRI Program: Guidance for the Operational Risk Manager*, helps operational risk managers establish and maintain strong KRI programs in an environment of increased operational risk regulation.

COMMENT LETTERS

- ***American Banker Editorial***
On September 22, 2006, The American Banker published an editorial by BITS CEO Catherine Allen on the “Defining and Designing the New Security.” The article outlined the challenges facing the financial services industry as well as efforts by the sector to cooperate, establish partnerships and develop best practices to respond to risks including the sector's dependence on other critical infrastructures.
- ***Comment on the Interagency Identity Theft Red Flags Rule***
On September 18th, 2006, the Financial Services Roundtable and BITS submitted a comment letter on the proposed "Red Flags Rule" to implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The 13 page letter urges the Agencies to: provide greater flexibility and explicitly state that the thirty-one red flags listed (and any others not enumerated) be regarded as "examples" only; clarify that the final rule should not be the basis for civil liability; make the final rule more consistent with other regulations; incorporate more realistic cost estimates of the impact of the regulation; modify several key definitions; and provide adequate time to implement a risk-based red flags program. The letter is available at <http://www.bitsinfo.org/downloads/Comment%20letters/BITS&RoundtableRedFlagsCommentLetterFINAL.pdf>.
- ***Input to Identity Theft Task Force.***
On July 27, 2006 BITS staff sent an 11-page memo to OCC and FDIC officials who are participating on the task force. The memo is in response to a request for information about what BITS and the financial services industry has done to address identity theft, information security, security breach, fraud, and insider threats.
- ***Comment on Proposal to Limit Information Collected and Maintained in WHOIS Data base***
On April 14, 2006 BITS sent a comment letter to the Internet Corporation for Assigned Names and Numbers (ICANN) regarding a proposal to limit the type of information collected and maintained in the WHOIS data base. BITS urges ICANN to adopt a formulation that will provide financial institutions with the information they need to respond to identity theft and account fraud. Throughout 2006, BITS engaged members, other financial associations, the US Government, and the Internet Corporation for Assigned Names and Numbers (ICANN) on compromise solutions to ensure financial institution access to the WHOIS database. In September, The Financial Services Roundtable's Board endorsed the “special circumstances” model, which provides unrestricted access to WHOIS information, while, at the same time, provides a mechanism to protect the privacy of vulnerable registrants. The BITS letter is available at

<http://www.bitsinfo.org/downloads/Comment%20letters/WHOISCommentBITSFINALApr06.pdf>

- ***BITS and Financial Services Roundtable Letter: Security of Municipal Broadband Networks***

On June 1, 2006, BITS and other associations sent a letter to the cities and towns that are developing municipal broadband networks to ensure that these networks are secure and not used to facilitate illegal activity or to violate cyber security, child pornography, or intellectual property laws. The letter is available on the BITS website:

<http://www.bitsinfo.org/downloads/Publications%20Page/Muniletter2.pdf>

- ***Social Security Number Verification***

On February 24, 2006, BITS and The Financial Services Roundtable submitted a joint comment letter to the Social Security Administration (SSA) in support of their Consent Based Social Security Number Verification (CBSV) Process. This process will allow institutions to affirmatively verify with the SSA a consumer's name, social security number and date of birth (DOB). While in support of this process, BITS and the Roundtable provided comment on issues such as full name matching, real-time vs. batch submissions, daily limitation of records and expectation of volume, and document requirements. The comment letter is available at

<http://www.bitsinfo.org/downloads/Comment%20letters/SSACommentBITSandRoundtableFINALccV2.pdf>

CONGRESSIONAL TESTIMONY

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. In April 2005, Catherine A. Allen, BITS CEO, testified before the House Committee on Homeland Security Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity on the importance of elevating the position of Cybersecurity Director at the Department of Homeland Security to an Assistant Secretary level. Her testimony included a description of the current cybersecurity landscape, and what BITS and the industry are doing to address threats. The testimony also included the BITS recommendations to the government to strengthen cybersecurity, referred to in detail and presented as the acronym PREPARE©.

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:

- 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.

- ***Statement of Erik Stein on Behalf of BITS: Role of Social Security Numbers (SSNs) in Identity Theft and Issues Relating to Enhancing Privacy***

BITS Fraud Reduction Steering Committee member, Erik Stein, testified in a March 30 hearing before members of the Committee on Way and Means' Subcommittee on Social Security. This hearing was the fifth in series of Subcommittee hearings on "Social Security Number High-Risk Issues" and it examined the role of SSNs in identity theft and issues related to enhancing SSN privacy. This testimony is available at <http://www.bitsinfo.org/downloads/Testimony/SteinTestimonyMar06.pdf>. Follow up information regarding the security practices of financial institutions and general business practices for securing information and protecting customer information after account or loan closure was submitted to Rep. Xavier Becerra on May 8. This information is available at <http://www.bitsinfo.org/downloads/Testimony/SSNAddInfo050806.pdf>.

- ***United State Congress House Committee on Financial Services Subcommittee on Financial Institutions Hearing on ICANN and the WHOIS Database: Providing Access to Protect Consumers from Phishing***

On July 18, 2006 BITS CEO Catherine A. Allen testified at the Subcommittee on Financial Institutions and Consumer Credit's hearing regarding the Internet Corporation for Assigned Names and Numbers (ICANN) proposal to restrict access to the WHOIS database. Catherine outlined the benefits of the WHOIS Database to financial institutions, including its use as a tool for investigating and responding to phishing attacks and attempts to commit identity theft using fraudulent websites. Written testimonies are available at <http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=491>.

- ***Cybercrime Treaty Support***

In August 2006, the U.S. Senate ratified the Council of Europe's Convention on Cybercrime. Signed by the United States in November 2001, the Convention on Cybercrime is the first and only international, multilateral treaty specifically addressing the need for cooperation in the investigation and prosecution of computer network crimes. It requires global law enforcement cooperation with respect to searches and seizures and provides timely extradition for computer network based crimes covered under the treaty. BITS and The Financial Services Roundtable had recommended adoption of this treaty in testimony before Congress in 2005 and had worked with the Cyber Security Industry Alliance in educating members of the Senate.

- ***Participation in Congressman Adam Putnam's Corporate Information Security Working Group (CISWG).*** Throughout 2004, BITS, The Business Roundtable, Business Software Alliance, Center for Internet Security, ITAA, US Chamber of Commerce, US ISP Association and many others participated in a series of meeting to develop recommendations on best practices& metrics, liability protection, incentives,

and awareness and training in order to bolster information security. BITS participated in the CISWG because it provided a substantive forum for associations representing IT users and suppliers, government executives and others to candidly discuss information security challenges, risks and ways the private sector can collaborate. BITS also participated in the National Cyber Security Partnership.

SUMMITS, FORUMS AND CONFERENCES

- ***Enterprise Payments Fraud and Cross Channel Payments Risk Forum***
On December 5, BITS hosted the Enterprise Payments Fraud and Cross Channel Risk Payments Forum in Washington, D.C. The forum focused on emerging payments risk issues and the efforts that financial institutions, payments networks, technology vendors, and government regulators are taking to address these issues. Comerica CIO John Beran keynoted the forum and outlined the emerging fraud trends across the various delivery channels and payments applications. Panel discussions focused on the current payments risk environment, steps being taken by industry today to enable better payments fraud detection across silos, emerging business techniques and technologies to address cross channel payments risks, and longer term enterprise payment risk mitigation approaches and structures. Attendees also received a progress update from the Partner Group regarding their efforts to address cross channel fraud.
- ***ITAC Data Breach Forum***
On November 16-17, the Identity Theft Assistance Center held a forum on Data Breaches: Preparation, Communication and Response. Industry experts, top analysts, Congressional staff, expert communicators and attorneys convened to discuss data breach fact vs. fiction; what breaches really mean to consumers; data breach management; crisis communication essentials; and the latest in legislation and regulation.
- ***5th Annual BITS/American Banker Financial Services Outsourcing Conference***
On November 13 and 14, BITS and American Banker hosted the 5th Annual BITS/American Banker Financial Services Outsourcing Conference presented with The Santa Fe Group. Keynoted by James H. Blanchard, retired Chairman and CEO of Synovus, and Catherine S. Brune, Senior VP and CIO with Allstate Insurance, the conference was well-attended. The program featured leading financial services executives, service providers and regulators discussing critical issues related to risk management, global outsourcing, regulations and legislation, and corporate boundaries.
- ***ID Management Forum***
On October 5, BITS hosted the "BITS ID Management Forum: A Strategic Look at Credentialing and Authentication" in Washington, DC. This one-day, invitation-only meeting focused on two key aspects of the identity management puzzle: credentials and authentication. Keynote presenters included BITS CEO Cathy Allen, who spoke to the trends and strategic challenges for identity management and RSA Security, Inc. CEO Art Coviello who provided the keynote entitled "Beyond Authentication: The Logic of layered Security." The forum included panels on credentialing in present and future

environments, long term strategic views of identity management, and compliance with the FFIEC authentication guidance.

- ***Anti-Money Laundering Forum***

The "BITS Anti-Money Laundering Forum: Bridging the Gap between Legislation and Implementation," was presented with The Santa Fe Group, July 13-14, 2006, in Washington, DC. There were many highlights in this well-attended event, with detail ranging from trends in the terrorist financing world to the most successful strategies for detecting and deterring financial crimes. Among the many knowledgeable speakers were Ann Jaedicke, Deputy Comptroller for Compliance Policy of the OCC; Dennis Lormel, former Chief of the Financial Crimes Section for the FBI's Criminal Investigative Division, with 30 years of government service; Douglas Freedman, Director for Bank Compliance and Regulatory Relations, Barclays Capital; John Byrne, SVP of AML Strategies, Bank of America; and Richard Clarke, Chairman, Good Harbor Consulting.

PILOTS AND PROJECTS

- ***Financial Institutions Shared Assessments Project (FISAP)***

The Financial Institution Shared Assessments Program was created by BITS and member financial institutions to fix the cumbersome and expensive service provider assessment process. The Program opened its doors 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. Today, more than 30 financial institutions and service providers have joined the Shared Assessments Program. As part of the Financial Institution Shared Assessments Program Working Group, these companies collaborate to ensure the program meets rigorous security standards.

- ***Internal Fraud Prevention Service***

The Internal Fraud Prevention Service® was launched on August 1. In development for several years, this outstanding new service is due to an unprecedented collaborative effort between internal fraud investigators, human resources groups, legal counsel and risk professionals from across the financial services spectrum. Members of the BITS Shared Database Working Group helped develop and pilot the concept of this service. The service enables institutions to screen employment candidates against a shared database of former financial services employees who were released for cause due to fraudulent acts committed against the institution. A group of participating financial institutions has begun to implement the solution and is jump-starting the service by contributing three years of historical data.

- ***Identity Theft Assistance Center (ITAC)***

The Identity Theft Assistance Center (ITAC) is a nonprofit membership organization sponsored by The Financial Services Roundtable and BITS. ITAC's free victim assistance service helps customers of member companies restore their financial identities. For more information, go to www.identitytheftassistance.org.

- ***E-mail Security Project.***

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 final deliverables will be available by spring of 2007.

- ***Social Security Verification Project***

BITS and The Financial Services Roundtable encouraged the Social Security Administration to provide a robust verification system that will help prevent fraud and identity theft. 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. During a July 24 meeting with BITS, The Roundtable and the SSA, BITS was tasked with gathering information from our member financial institutions regarding their anticipated participation in a Consent Based Social Security Number Verification (CBSV) program. On November 20, BITS transmitted the results of the survey to members and the SSA. The survey revealed strong interest from US financial institutions for a consent-based verification program. However, financial institutions that responded to the survey indicated there are several impediments to broader participation in a verification program.

- ***BITS Product Certification Program (BPCP)***

The BPCP provides product testing by unbiased and professional facilities against baseline security criteria established by the financial services industry. A product certification, the *BITS Tested Mark*, is awarded to those products that meet the defined criteria. An option is available for technology providers to meet the product certification requirements via the internationally recognized Common Criteria certification schema. In September 2006, the BITS Lab Governance Committee approved SafeBoot's Device Encryption v5.0 and Utimaco's SafeGuard Easy v4.20.1. SafeBoot and Utimaco's SafeGuard Easy v.20.1 are the fourth and fifth software products to receive the BITS Tested Mark. Also, BITS continued discussions with DHS to support efforts to enhance product certification programs, including the Common Criteria program run by the National Security Agency and National Institutes of Technology and Standards.

- ***Joint Work Plans with Major Software Providers***

BITS' efforts to improve the quality of software security have three overarching objectives. BITS wants vendors to provide a higher duty of care when selling to the financial industry and other critical infrastructure companies; ensure products comply with security guidelines before releasing products; and make the patch-management process more secure and efficient and less costly for organizations. To meet these objectives, BITS is urging vendors to comply with business requirements. Under the requirements, software vendors would use security criteria, like the BITS software

security criteria and the Common Criteria, in developing software products to ensure products meet minimum security standards. Companies would then test the products for security and conduct thorough code reviews prior to releasing them. To facilitate achievement of these objectives, BITS has implemented a joint work plan with one major software provider and is developing joint work plans with others.

- ***Mortgage Fraud Reduction Project***

In November, members of the BITS Fraud Reduction Steering Committee and Mortgage Fraud Reduction project group, and members from the Mortgage Bankers Association (MBA) met with officials from the Federal Bureau of Investigation (FBI) and the U.S. Department of Justice (DOJ) to discuss ways these groups can enhance their working relationships to combat mortgage fraud. Each organization provided updates on their efforts and agreed to meet on a quarterly basis to address issues and deliverables identified during the discussions.

- **BITS ID Theft Working Group efforts and BITS Forum on Identity Theft.** BITS was the first financial industry consortium to focus on the rising risks of identity theft. In 2002 and 2003, BITS convened a Forum involving industry fraud reduction experts, law enforcement, federal agencies and actual victims of identity theft to begin to dimension the problem and craft ways to address. The Forum led to the development of the BITS Fraud Reduction Guidelines in 2003, with a specific emphasis on reducing identity theft and assisting its victims. Those 2003 Guidelines included the concept of the Identity Theft Assistance Center, which became a reality in 2004, co-founded by BITS, The Financial Services Roundtable, and 50 member organizations. This is one of the first comprehensive white papers BITS produced on the topic, in 2003:
<http://www.bitsinfo.org/downloads/Publications%20Page/bitsidtheftwhitepaper.pdf>

SURVEYS AND RESEARCH

- ***Information Sharing***

Throughout 2006, BITS conducted dozens of information sharing surveys for members on a wide variety of information security, fraud reduction and outsourcing-related issues. In addition, BITS hosted several conference calls with members and regulators on the Federal Financial Institutions Examination Council's Authentication Guidance.

- ***Net Neutrality Discussions***

Throughout 2006, BITS engaged members and major telecommunications providers on implications of "net neutrality." "Network neutrality" is the principle that network operators should not be able to discriminate among network applications. Based on these discussions with technology and operations experts, there appear to be three major strategic concerns: competition and cost, regulatory requirements, and service provider impacts. BITS urged telecommunications service providers to meet the security and diversity/resiliency needs of the financial services industry.

- ***Rising Fraud Risk Discussion Forum***

The Rising Fraud Risk Discussion Forum was created in 2006 to serve as a cross-channel venue for fraud risk managers to discuss newly identified fraud schemes and types as

well as strategies for mitigating the losses associated with them. Since its creation in February the group has discussed topics such as: Internet-based "credit clinics" or "credit enhancers;" increased courier robberies in the Southeast; assisting victims of Internet/mail scams; online services that provide fraudulent employment and payment verification; fraudulent mortgage closings; and increases in counterfeit travelers checks.

FOR ADDITIONAL INFORMATION, CONTACT:

Catherine A. Allen

CEO, BITS

John Carlson

Executive Director, BITS

1001 Pennsylvania Avenue NW

Suite 500 South

Washington DC 20004

(202) 289-4322

cathy@fsround.org

www.bitsinfo.org