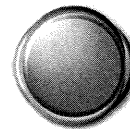


THE FINANCIAL SERVICES ROUNDTABLE



BITS

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

February 10, 2005

RE: FDIC Study on “Putting an End to Account-Hijacking Identity Theft”

To Whom It May Concern: IDTheftStudy@fdic.gov

The Financial Services Roundtable (FSR), BITS, and the Identity Theft Assistance Corporation appreciate the opportunity to comment on the Federal Deposit Insurance Corporation (FDIC) study, “Putting an End to Account-Hijacking Identity Theft.” The FDIC study raises a number of concerns about current practices for authenticating financial institution customers and monitoring fraudulent activities. The purpose of this letter is to provide the FDIC with comments on the study. We also review the activities of BITS, FSR, and the Identity Theft Assistance Center (ITAC) in preventing and mitigating fraud as well as efforts to work with the information technology (IT) community to address software security concerns.

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. BITS is a nonprofit industry consortium that shares its membership with The Financial Services Roundtable. BITS serves as the strategic “brain trust” for the financial services industry where commerce, financial services and technology intersect. BITS also facilitates cooperation between the financial services industry and other sectors of the nation’s critical infrastructure, government organizations, technology providers and third-party service providers. The Identity Theft Assistance Corporation, a not-for-profit membership corporation, is conducting a pilot of the Identity Theft Assistance Center or ITAC on behalf of the 48 founding member companies.

We appreciate the interest of the FDIC and the hard work that the authors of this study have devoted to research this issue. The study clearly demonstrates the FDIC’s interest in protecting consumers from various forms of on-line fraud and in ensuring that financial institutions continue to serve the financial needs of their customers.

We understand that the Federal Financial Institutions Examination Council (FFIEC) agencies will convene a two-week symposium on March 14-25, 2005 to assess the current risks, to identify potential or future risks, and to identify and evaluate controls associated with user authentication techniques in the e-commerce and e-banking environment. The FDIC study, as well as outreach from FFIEC members in preparation for the symposium on retail authentication, have stimulated extensive debate within the financial services industry.

Our general comments are provided in the body of this letter. Selected additional comments are offered in Appendix A. Appendix B provides an overview of BITS, FSR and ITAC efforts to respond to phishing attacks, prevent and respond to identity theft, reduce fraud, strengthen software security, and address risk management.

GENERAL COMMENTS

A Risk-Based Approach Is Appropriate. We believe that the FDIC study does not adequately take into account the fact that financial institutions are applying a risk-based approach for evaluating the risks, deploying controls and offering convenient solutions to their customers. The FDIC study does not acknowledge that many of the proposed solutions outlined in the study would be more expensive, overly complex or unwieldy for customers than the problem they are trying to address. Further, the study appears to rely too heavily on the views of vendors that market authentication products and services without showing the practical challenges involved in deploying these technologies in real-world situations.

The study does not take into account the fact that financial institutions apply layered controls to address account takeover risks. For example, many financial institutions aggressively monitor account activity to detect and prevent unusual or fraudulent patterns or activities. Information security is an ongoing concern involving multiple controls and layers. Instituting new controls must be part of a managed process involving information, cost and installation study, analysis, and consumer education.

In general, BITS, FSR and ITAC members believe that the FFIEC's Guidelines for Safeguarding Customer Information (as mandated by Section 501(b) of the Gramm-Leach-Bliley Act of 1999) strike the appropriate balance. They are flexible, risk-based, technology neutral, and rely on a continuously evolving information security program. We do not believe that regulatory action in the form of new regulation or new guidance is needed at this time. However, if the FDIC and the other FFIEC agencies believe that additional supervisory guidance or regulatory requirements are necessary, we strongly encourage the FDIC to work in cooperation with other FFIEC agencies to adopt uniform supervisory guidance and examination procedures and to follow the customary process of publication of proposed actions and solicitation of public comment.

Two Factor Authentication Is Not a Panacea. The FDIC study expresses the view that current authentication procedures for online retail financial services – relying most often on a user identification name and an associated password – are no longer adequate to secure customers' accounts against “phishing” attempts. The report suggests that the use of a two-factor authentication procedure must now be viewed as “industry best practice.” While authentication is an important element in a robust information security program, it is only one element.

Fraud is a risk to be managed. There are a number of solutions that should be looked at in conjunction with stronger authentication techniques, including: certifying e-mails that they are coming from a financial institution web site; addressing malicious code such as key

stroke loggers and other forms of spyware; and engaging Internet service providers to block fraudulent e-mail. The financial services industry is working diligently to implement controls to combat fraud and other forms of cyber crime. We also know that continued dialogue among financial institutions and engagement with leading software and hardware providers, Internet service providers, and law enforcement agencies is essential for addressing the challenges.

While two-factor authentication has many advantages and is used by many financial institutions for some high value transactions, we believe that two-factor authentication methods will not automatically prevent “phishing.” In fact, we believe that stronger authentication alone will not solve account takeover and is not the only or best tool for combating phishing. Two-factor authentication might limit a criminal’s ability to immediately capitalize on the personal information he or she has stolen. However, criminals could still induce an unsuspecting consumer to give up important financial information through “phishing” or some other scheme, and make use of that information in some other way. Also, two-factor authentication does not prevent “man in the middle” attacks. In addition, depending on the nature of the second factor, other problems could arise – for example, the process of issuing, and especially re-issuing, authentication tokens to consumers would be vulnerable to impersonation and interception. Further, rectifying a successful theft of a token would likely be highly complex. Social engineering tactics could also be used to induce an unsuspecting consumer to divulge details regarding the authentication arrangements.

Two-factor authentication methods involve serious practical problems and complexities. Many of the technologies involved are not at the state of maturity that appears to be assumed in the FDIC report, and could not, as a practical matter, be relied upon as a solution at this time. Others – such as the use of authentication tokens – may be more mature, but today are only practical – if at all – in a one-on-one implementation, where one customer interacts with one financial institution. Given the reality that customers interact with multiple financial institutions, either some means of centralizing token management and authentication needs to be devised – not something that exists today – or customers would be left with the responsibility of managing numerous tokens for their different financial accounts. This is not a practical solution by any means. As a practical matter, other industries would need to move forward with adopting two-factor authentication schemes concurrently with the financial services industry.

Terminology Should be Accurate and Consistent. Use of terminology is especially important. The media and many self-interested parties have hyped the phishing problem, compounding confusion and exacerbating public fear. This treatment of phishing in the popular media is only one example of instances where hyping of some threats and risks is occurring. This kind of overreaction clearly threatens to erode the public’s trust and confidence in the ability of financial firms (and others) to secure their customers’ online financial activities. “Account takeover” is the term universally used in the financial services industry to describe the event that is the subject of the study and we urge the FDIC to use this term. “Account takeover” is the assumption of another’s identity on a valid existing account. The FDIC study uses a highly charged term – “account hijacking” to describe account takeover. Use of the term “hijacking” not only causes confusion, it connotes violence. As a result, the language itself heightens consumer concerns.

FDIC's Conclusions Require Additional Support. The FDIC study cites statistics and studies conducted by the Federal Trade Commission (FTC) and others on the extent and impact of identity theft on consumers. However, the FDIC study does not adequately support several important conclusions or assertions. For example, the study offers no support for the statement that "[m]ost, if not all, large financial institutions and electronic bill paying services (PayPal) have been hit with phishing." Similarly, the FDIC does not provide a foundation for several observations about the vulnerability of electronic payments system including this comment: "the increasing number of access points, coupled with the anonymity afforded by electronic payments systems" has led to an increase in account takeover. The study also asserts, without any supporting reference, that "it has become increasingly apparent that single factor, password based authentication may no longer be sufficiently secure for consumer remote access to online banking systems" The same comment applies to the statement that "control has been diluted and security is more easily compromised."

We agree with the statement on page 11 of the study that the FTC statistics are of "limited value for estimating the incidence of account hijacking because the methodology does not report response rate or weighing of results." In addition, some of the sources relied on by the FDIC are for-profit entities that have an interest in promoting their goods or services.

While not available at the time the FDIC study was released, the FDIC should consider research released in January 2005 by Javelin Strategy & Research. The "2005 Identity Fraud Survey" report indicates that identity theft is less of a problem on the Internet than the FDIC alleges. The Javelin study states that most criminals obtain access to the personal information used in identity theft crimes by traditional rather than electronic channels. The survey shows that, of the consumers who knew how their personal information was obtained, 68 percent reported their information was compromised as a result of an offline incident, including lost or stolen wallets, where a checkbook or credit card was accessed as part of an offline transaction, or was taken from the garbage. Only one U.S. victim in 36, who knew how their information was compromised, cited an online financial transaction as the source of the loss.

The FDIC study fails to mention the larger context or recognition that industry segments outside financial services play a role in phishing. The study does a good job in distinguishing actions that customers should take to prevent account take over versus actions that financial institutions should take. This is important since many forms of online fraud (e.g., phishing) involve deception that is beyond the control of financial institution.

There Are Customer Acceptance Issues. U.S. consumers of financial services are not accustomed to using tokens or other two-factor authentication devices at this time. Moreover, customers have not accepted solutions that involve lengthy enrollment processes or complicated processes for using the technology. Implementing such schemes would involve an extensive process of consumer education and training to familiarize consumers with these new procedures. Unquestionably, any such mandate would significantly impede consumers' migration to the use of online financial services and could potentially impact current use of online financial services.

In recent months, regulators in Hong Kong and Singapore have mandated multi-factor authentication requirements on banks. It is important to note that these jurisdictions have more robust national identity schemes than the U.S. These schemes are linked to school attendance, tax, immigration, driving license and other records that are associated with citizens in these jurisdictions. U.S. laws and consumer attitudes to such approaches are at odds and often viewed as an infringement of civil rights and privacy.

The Financial Services Industry Has a Track Record and Commitment. The study does not fully acknowledge the commitment of the industry to fighting account takeover and identity theft and the industry's achievements in protecting customers. The reality is that financial firms have invested considerable effort and expertise to do so and these efforts have shown very positive results. Financial institutions have learned a great deal in the past several years. The time and cost associated with rehabilitating identity theft victims' financial status is improving while the industry continues to deal with the crime.

Consumer education also is a critical component. Financial institutions have devoted increasing resources to educating consumer on safe computing practices. The industry will continue to invest in these efforts given that a source of the problem is the fact that consumers continue to provide personally identifying information without full understanding of how and whether this information is protected.

While we appreciate the fact that the study references some of the work that BITS, FSR and ITAC have completed, it is not a complete listing of our activities. We would encourage the FDIC to refer to Appendix B which provides a more detailed accounting of our efforts.

Conclusion

We believe the FDIC and other FFIEC agencies could play an important role in working with the financial services community to urge software vendors to develop more secure software with fewer deficiencies and vulnerabilities, enlist the Internet Service Provider community to develop best practices to deter phishing, engage law enforcement to investigate and prosecute cyber crimes, and build on the consumer education efforts.

We appreciate your consideration of our comments. If you have any further questions or comments on this matter, please do not hesitate to contact us or John Carlson (BITS) at (202) 289-2442.

Sincerely,



Catherine A. Allen
CEO, BITS

Richard M. Whiting

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

Anne Wallace

Anne Wallace
Executive Director
Identity Theft Assistance Corporation

Cc: Robert E. Feldman, Executive Secretary, FDIC
Julie Williams, Acting Comptroller of the Currency
Richard Spillenkothen, Federal Reserve Board of Governors
James Gilleran, Director of the Office of Thrift Supervision
Becky Baker, Secretary of the Board, National Credit Union Administration

Appendix A: Selected Comments on the FDIC Study

The following are selected comments on the FDIC study from BITS and FSR member companies and BITS, FSR and ITAC staff.

On page 3, we suggest that the study look further at approaches to improving the effectiveness of single factor password based authentication, rather than dismissing it as a solution. Password based authentication can still be part of an overall risk based approach.

On page 4 in the Background section, there are many definitions of ID Theft. Some members believe it would be more concise to use one definition: ID Theft is viewed as the fraudulent establishment of credit.

On page 5, we would like to ask the FDIC, under sub-title Regulators can play a constructive role, would this include providing Internet Service Providers/law enforcement with the tools to recover phished information from unauthorized websites?

On page 7, the definition of phishing implies that the phishers are harvesting account information to take over accounts. This is not entirely true. Many phishing cases harvest full identities that the fraudsters are likely exploiting by opening new accounts in the victim's name.

On page 8, the study includes an example of a phishing attacking against a specific financial institution by name. We do not believe it is appropriate for the FDIC to so identify specific institutions. It could undermine consumer confidence in that financial institution or any other institution that the FDIC uses as an example.

On page 10, we suggest that the study acknowledge the important role of Internet service providers (ISPs) in responding to phishing. Through BITS' participation in the Federal Communications Commission (FCC)'s Network Reliability and Interoperability Council (NRIC), BITS has asked Internet service providers (ISPs) to increase their responsibility for protecting consumers from phishing and other forms of online fraud and to work cooperatively with financial institutions and other e-commerce companies to formulate solutions.

On page 10, the study does not give enough emphasis on spyware which is a serious threat and thus should be discussed in the study. Key-logging, which may be a byproduct of spyware, can exploit various operating system/browser vulnerabilities. Customers may be able to spot a phishing email and ignore it but will not be aware that a key-logger is running on their PC unless their anti-virus and/or spyware detects the key-logger.

The commentary regarding hacking into financial institutions' databases on page 10 leaves the reader concluding that this is common occurrence. There is no evidence in the study to support this conclusion

The study should mention plans by the Justice Department's Bureau of Statistics to conduct a nationwide survey of 36,000 businesses in April 2005 to assess cyber crimes.

On page 11, the statement, “Regardless of the method used to steal confidential information, once the necessary information is in hand, the fraudster’s goal is to gain access to a consumer or business account from which fund transfers can be executed” narrowly defines the fraudster’s intent. The information harvested can, and is, used for a variety of purposes from credit card fraud, Identity Theft, SSN fraud and a host of other crimes of which account hijacking is only one. We believe the FDIC should either indicate “one of the fraudster’s goals may be to gain access. . .” or to indicate other potential uses of the harvested information.

On page 19, the study refers to BITS as the “Banking Industry Technology Secretariat.” However, BITS is no longer an acronym. BITS is the full organization name.

On pages 22-37, the study does not adequately explain how the FDIC derived its “effectiveness” ratings in the “use of technology to mitigate account hijacking” section. The FDIC should explain how the rating came about, where the technology is used and how well it works for that purpose. More to the point, the “ease of use” and “implementation” ratings do not seem to fully consider the complexity, on going support, or cost of the proposed solutions, or the trade-off between risks addressed, ease of use, and cost of implementation. For example, one member company noted that scanning tools are neither “easy” nor “moderately effective,” in combating phishing. It is not possible to obtain the telecommunications bandwidth to scan the entire Internet in 2¼ days even if server and routing propagation delays were eliminated. In another example, a member company noted that log analysis is not “highly effective or even moderately useful” in combating phishing. This member also questioned how the “implementation” could be viewed as “easy” when the study acknowledges that a trained individual will be required to review log analysis results continually.

On pages 24-25, several members noted that the discussion concerning e-mail authentication is incomplete. The study only makes minimal discussion of the need for Mutual Authentication, the need for financial institutions to authenticate itself to the end user, as well as the end user to the financial institution. Specifically, this is an issue when the financial institution is sending emails or presenting web pages to the end user. Regarding the discussion on the use of Sender ID, Sender ID is only one solution. It is not the strongest approach and is only applicable for email not web pages, and to date has a mixed record of success. Also, Sender ID is not yet at a stage where it can be implemented industry-wide. Initiating Sender ID before the technology is equipped to handle implantation would be disruptive to overall communications and would inconvenience customers. Moreover, e-mail authentication must be implemented by ISPs and other industry vendors but that this technology is nascent today and thus should not be viewed as easy to implement.

One member company noted that the USB token device would require some type of software that communicates with the device to be installed on the client computer. Its effectiveness is dependent on a Customer properly hardening its PC because it relies on software executing properly on the Customer’s PC. The conclusion regarding the USB token being “easy to use” overlooks the fact that some customers would need to carry multiple tokens to conduct transactions with multiple financial institutions.

On page 29, one member noted that the Password-Generating Token, or OTP technology, can indeed be extremely costly when used to support millions of customers, however it is easier to implement and no more costly than the USB tokens. "Easy-to-use" overlooks the real-estate issue, when a customer needs to carry a 5th or 6th token.

On pages 32-36, several members noted that there are major concerns with the conclusion that biometric methods are highly effective, easy-to-implement, or easy-to-use. Fingerprints, which is one of the most mature and successful of the biometrics, is not highly effective or easy-to-use. Additionally, the study misrepresents the accuracy/effectiveness of many of the biometrics discussed. For example, keystroke recognition is portrayed as moderately effective, the same rating as for instance voice recognition, although there have been several successful deployments of voice recognition and none for the keystroke recognition. Biometric solutions must be carefully reviewed to consider the risk of identity theft, because recovery from biometric-based identity theft will be considerably more difficult than the challenges arising from today's identity theft. Moreover, several members also noted that customers do not readily accept solutions that involve lengthy enrollment or require the downloading of files in order to leverage the proposed mitigating technology. Additionally, biometrics comes with well-documented consumer privacy concerns and issues as well.

On page 28, the study does not state that smart cards require institution-side servers that associate a specific token to a specific user and ongoing administration of these associations. However, the study states that smart cards are "easy" and "moderate" to implement.

One member company noted that an important technology category that is missing from the FDIC study is the hardening of customer computers. Customers must assume some level of responsibility for maintaining the integrity of their computing system. Customers should be responsible for ensuring their workstation are equipped with updated anti-virus software, personal firewalls, spyware detection, and the latest patches for their browsers and operating systems. This can be conveyed through continued consumer education as well as through technologies to validate the security configuration of the consumer workstation.

Several members noted that the report misses an opportunity to explain steps that government/law enforcement can do to mitigate, detect and educate.

Appendix B: Overview of BITS, FSR and ITAC Activities

BITS Activities

BITS has significant expertise on authentication, fraud reduction, and software security issues and has engaged leaders from the financial services industry, law enforcement and the regulators in developing best practices and solutions to numerous challenges. BITS has engaged experts from the financial services industry through the Aggregation Working Group, Authentication Working Group, Fraud Reduction Steering Committee, IT Service Provider Working Group, and Security and Risk Assessment Steering Committee. Following are examples of BITS' initiatives with relevance to this FDIC study, "Putting an End to Account-Hijacking Identity Theft."

Identity Theft Mitigation. BITS and The Roundtable are responding to the escalation in identity theft with a series of steps to facilitate prevention of the crime and assist victims when it occurs. The goals of these efforts are to help maintain trust in the financial services system, assist member companies' customers, and mitigate fraud losses. BITS has also published several business practices guidelines and white papers on various aspects of identity theft and fraud reduction strategies. A 2003 BITS white paper on identity theft outlines the full identity theft landscape, establishing key terms as well as identifying factors that contribute to identity theft. Along with the white paper, BITS developed guidelines for financial institutions to use to prevent identity theft and restore a victims' financial identity. Included are processes for providing a "single point of contact" at companies to whom victims may report cases of identity theft.

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.

Ultimately, we hope this guide will help make the Internet a safer, sounder and more trusted environment for everyone.

Anti-Phishing Efforts. BITS is responding to "phishing" through its Fraud Reduction Program. Phishing is the practice of luring consumers to provide bank account and other personal information to fraudsters through bogus email messages. In response to these and other online scams, BITS created a Phishing Prevention and Investigation Network. The

BITS Phishing Network provides member institutions with information and resources to expedite investigations and address phishing/spoofing incidents. The BITS Phishing Network will include a searchable database of information from other financial institutions on their phishing incident and response experience, including contacts at law enforcement agencies, foreign governmental agencies, and ISP Web administrators. The Network will also provide data on trends to help law enforcement build cases and shut down identity theft operations. The BITS Phishing Prevention and Investigation Network will:

- Help member institutions monitor and shut down e-scams faster and more effectively.
- Reduce financial institution manpower costs and losses.
- Increase phishing investigations and arrests of perpetrators.
- Facilitate communication among fraud specialists at financial institutions, service providers and law enforcement agencies.

Software Security Initiative. In February 2004, BITS and The Financial Services Roundtable (the Roundtable) held a Software Security CEO Summit. The event launched BITS and Roundtable efforts to promote CEO-to-CEO dialogue on software security issues. We developed and disseminated to 400 BITS and Roundtable member company executives a “toolkit” with software security business requirements, sample procurement language, and talking points for discussing security issues with IT vendors. Since the Summit, BITS has worked with all the associations representing the financial services industry, The Business Roundtable and some sector-specific associations.

In April 2004, BITS and The Financial Services Roundtable announced a joint policy statement calling on the software industry to improve the security of products and services it provides to financial services customers. The policy statement calls on software providers to accept responsibility for their role in supporting financial institutions and other critical infrastructure companies. BITS and the Roundtable support incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products. BITS also has explored the possibility of seeking protection from US antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware that they purchase.

BITS is working with major software vendors to discuss business requirements. In June 2003, BITS announced it had successfully negotiated with Microsoft to provide additional support to BITS member companies for Windows NT. We have provided Microsoft and other software and hardware companies with the Software Security Business Requirements. BITS members agree that these requirements are critical to the soundness of systems used in the financial services industry. In addition, BITS is working with or has plans in early 2005 to work with Cisco, IBM and RedHat on software security issues.

Cyber Security Collaboration. BITS participated in the Corporate Information Security Working Group (CISWG) sponsored by Congressman Adam Putnam, Chairman of the House of Representatives' Subcommittee on Technology, Information Policy, Intergovernmental Relations on the Census. CISWG is made up of corporate, industry and academic leaders and is working to pursue a private sector-driven approach to enhancing the

protection of the nation's corporate computer networks. In addition, BITS participated in task forces set up by DHS and several technology associations.

Forums. On March 8, 2005, BITS will host a Forum entitled "A Strategic Look at Authentication" in Washington, DC. Authentication issues have emerged in a number of BITS' working groups. This strategic Forum will focus on the following issues: business issues that drive the need for authentication; business challenges to implementation; public policy implications; and emerging technologies in the authentication area.

Last October, BITS convened the forum, "Protecting the Core: Securing Your Technology Infrastructure." The forum brought together information security experts from financial services, software vendors, telecommunications, consulting and government to discuss how financial institutions can: create strategies for evaluating internal and external risk; deploy preventative measures in a dynamic environment; and identify incident-management best practices. During the forum, several speakers addressed authentication issues in the context of periodically evaluating authentication requirements and options. The question remains as to whether or not stronger levels of authentication have reached the point where they are usable, acceptable and scalable. And, while authentication should assure the party's identity, it is important that the risks be evaluated to ensure the correct level of authentication has been deployed.

Risk Management Tools. In June 2004, BITS published *Best Practices in Patch Management for the IT Practitioner*. Security issues aside, patch management and implementation alone can cost one financial institution millions of dollars annually. A BITS survey of member institutions, extrapolated to the financial services industry in total, yielded this estimate—costs to the financial services industry associated with software security, including patch management, are approaching one billion dollars annually. The best practices help companies mitigate these costs.

In July 2004, BITS published *The Calculator: BITS Key Risk Measurement Tool for Information Security Operational Risks*. This tool helps financial institutions evaluate critical information security risks to their businesses. The tool starts with a list of common information security threats and vulnerabilities and matches them with corresponding controls to mitigate those risks. Using the tool, financial institutions score their own information security risks based on the likelihood of an incident, the degree to which the organization has defended itself against the threat, and an incident's possible impact. An institution can use the results to boost its ability to assess and mitigate risks to its information security program. The tool brings together an extensive body of information security risk categories outlined in international security standards and emerging operational risk regulatory requirements and combines them in one tool. Financial institutions can modify the tool to meet their unique needs.

Product Certification. The BITS Product Certification Program is another important part of our work to address software security. 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. BITS has initiated discussions with DHS to support efforts to enhance product certification programs, including the Common Criteria program run by the National Security Agency (NSA) and National Institutes of Technology and Standards (NIST). DHS has expressed support for broad-based, not sector specific, certification programs. Moreover, DHS wants “buy in” from the broader user community. Consequently, BITS has been in discussions with The Business Roundtable, NIST, and the Cyber Security Industry Alliance (CSIA) to develop a joint proposal.

Outsourcing. BITS has hosted three conferences, held numerous roundtable discussions with our members, and published several ground-breaking best practices tools (BITS Framework for Managing Technology Risk for IT Service Provider Relationships and Expectations Matrix).

Overview of the Identity Theft Assistance Center

The section of the FDIC study titled “Industry Responses to Identity Theft,” describes several industry initiatives including the Identity Theft Assistance Center (ITAC). As the FDIC notes, the Roundtable and BITS facilitated the creation of the Identity Theft Assistance Corporation by 50 of their member companies. The Corporation is conducting a twelve month pilot of the Identity Theft Assistance Center (ITAC).

The ITAC has three functions. First, and foremost, the ITAC call center helps customers of participating companies who are victims of identity theft by walking the customer through his or her credit report, noting any suspicious new accounts or possible account takeovers, and notifying those companies of possible fraud. ITAC delivers a unique benefit by extending the customer service commitment of the consumer’s “home” financial institution beyond that company’s four walls to other companies where fraud may have occurred. The ITAC’s other functions are to share information relating to identity theft cases with the Federal Trade Commission and law enforcement agencies in order to catch and punish the perpetrators, and to use data collected by the ITAC to prevent new cases of identity theft.

The ITAC builds on earlier industry efforts, notably the 2003 Fraud Reduction Guidelines, which encouraged financial services companies to create a single point of contact within their company to ensure a rapid and coordinated response to a customer who experiences identity theft. The use of a Uniform Affidavit for identity theft, and the agreement by financial services companies to share that information, is a breakthrough for identity theft victims who previously endured the frustration of completing multiple affidavits.

Midway through the pilot, consumer reaction to the ITAC service is overwhelming positive. It is too early to predict the precise details of the post-pilot but, whatever the model, the members of ITAC are committed to reaching out to customers who fall victim to identity theft.