

BITS

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

1001 PENNSYLVANIA AVE., NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
TEL 202-289-4322
FAX 202-628-2507

April 14, 2006

To: Internet Corporation for Assigned Names and Numbers

e-mail address: <whois-comments@icann.org>

Re: WHOIS Data Base

Dear Sirs and Madams:

The purpose of this letter is to comment on the proposal before the Internet Corporation for Assigned Names and Numbers (ICANN) to limit the type of information collected and maintained in the WHOIS data base. Based on a review of the information provided in the January 18, 2006 task force report containing two opposing formulations of the “purpose of WHOIS,” and discussions among information security and fraud risk managers, we urge ICANN to adopt Formulation 2.¹ Formulation 2 will provide financial institutions with the information they need to respond to identity theft and account fraud. In addition to commenting on the two proposals, we want to outline the activities of BITS and our members in addressing information security and identity theft challenges.

Under formulation 1, the only purpose of WHOIS is to “resolve issues related to the configuration of the records associated with the domain name within a DNS nameserver” (i.e., narrow technical issues). Under formulation 2, the purpose of WHOIS is to help resolve a broader range of “technical, legal or other issues regarding registration or use of a domain name.” We believe the adoption of formulation 1 would make it more difficult and time-consuming for financial institutions to identify and stop domain-based scams and the identity theft and account fraud that result.

Financial institutions have always been a favorite target for perpetrators of fraud. Institutions have long answered this challenge with reliable business controls, advanced technology, information sharing, and cooperative efforts with government and law enforcement agencies. Further, financial institutions must also deal with other domain-based issues including, but certainly not limited to, trademark infringement, unauthorized and sometimes unlawful disclosure of confidential, proprietary or customer information, spam attacks, inappropriate content sent or received via email, staff harassment/stalking, and violation of intellectual property rights by web site operators. While our members’ foremost concern is to protect their customers and maintain their trust, they must also be mindful of the need to comply with the requirements set forth by numerous laws, regulations and supervisory guidance.

¹ <http://www.icann.org/announcements/announcement-18jan06.htm>)

We believe that formulation 1 (or other efforts to limit or narrow the information) in WHOIS could adversely affect the financial services industry's efforts to respond to identity theft and phishing attempts. Timely response to phishing attacks and identity theft is critical to protect customers, financial institutions, and innocent consumers who may not be aware of their victimization. In many cases, the only tool financial institutions have for identifying registrants or purported registrants of domain names in a timely manner is via the WHOIS contact information. Often times, the fraudsters will register a domain name in the name of innocent consumers without the knowledge of the consumer. In most instances, it is not until these unsuspecting consumers are contacted by the financial institution that they learn they may have been a victim of identity theft, giving them the opportunity to remedy the effects of identity theft sooner rather than later. In addition, most innocent victims have been and continue to be extremely helpful to financial institutions in taking down or transferring these domain names to the financial institution that is a target or potential target of a phishing attack. Also, agreement from the operators to take down websites quickly when there is clear violation of trademarks or indications of fraud is only a partial solution. Financial institutions still need the WHOIS information to address the other forms of abuse noted above.

About BITS

BITS is a nonprofit industry consortium of 100 of the largest financial institutions in the U.S. BITS is the non-lobbying division of 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' 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 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.

Within BITS there are two working groups that have an interest in the WHOIS data—the information security experts who are involved in the BITS Security and Risk Assessment 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 a) sharing and developing best practices to secure infrastructures, products and services; b) maintaining continued public and private sector confidence; and c) 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.

Efforts to Strengthen Cyber Security, Reduce Fraud and Mitigate Identity Theft

The financial services industry has been aggressive in its efforts to strengthen cyber security, reduce fraud, and mitigate identity theft. 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. As just one example of these efforts, the Identity Theft Assistance Center (ITAC), which BITS and the Financial Services Roundtable established in 2004, announced in March that it had helped over 5,000 individuals to restore their financial identity. These services are provided free to consumers by ITAC members.

We have included a detailed summary of BITS' efforts to address information security, fraud reduction and critical infrastructure protection in the appendix.

While we understand that the public comment period officially closed on February 8, 2006, we are hoping that ICANN will consider this input from information security and fraud risk experts of the largest financial services companies who are the "front lines" of the identity theft and Internet fraud battlefield. If you have any further questions or comments on this matter, please do not hesitate to contact me or John Carlson at john@fsround.org or 202-289-2442.

Sincerely,

A handwritten signature in black ink that reads "Catherine A. Allen". The signature is written in a cursive, flowing style.

Catherine A. Allen
CEO, BITS

Appendix: Protecting the Critical Infrastructure: BITS' Accomplishments in 2005

BITS

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

APPENDIX: PROTECTING THE CRITICAL INFRASTRUCTURE: BITS' ACCOMPLISHMENTS IN 2005

PUBLICATIONS OF BEST PRACTICES AND GUIDELINES

Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy

- The BITS study on “Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy” outlines inefficiencies resulting from regulatory overlap within:
 - The Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA);
 - The Gramm-Leach-Bliley Act of 1999 (GLBA);
 - The Sarbanes-Oxley Act of 2002 (SOX); and
 - The proposed U.S. Inter-agency Operational Risk Supervisory Guidance on Operational Risk Advanced Measurement Approaches (AMA) for Regulatory Capital (applying the International Convergence of Capital Measurement and Capital Standards: A Revised Framework, also referred to as Basel II), July 2003.
- The study includes specific recommendations for implementation by member institutions to increase efficiencies, and further provides recommendations for regulators to work with the financial services industry to reduce unnecessary burdens and eliminate inconsistent requirements. The study was made available in hard copy and jointly distributed by BITS and the Roundtable to key regulators as well as member institutions in a public launch event held October 11.

BITS Consumer Confidence Toolkit and Voluntary Guidelines

- BITS has developed a *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.

Protecting the Elderly and Vulnerable

- BITS released a new tool in October 2005 to help reduce fraud. The publication, “BITS Fraud Protection Guide: Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation,” describes the growth of this fraud, highlights ways to detect and prevent it, and urges financial institutions to work proactively to reduce it. “This new BITS publication serves to protect some of our nation’s most vulnerable populations and reinforces our member institutions’ 24/7 commitment to safe and secure financial transactions,” said BITS CEO Catherine A. Allen. In the coming months, BITS will release a toolkit for educating financial center and loss management personnel on ways to identify and prevent this type of financial crime. The Financial Services Industry Toolkit provides information to support the implementation or improvement of a financial institution internal prevention program for education and awareness to protect the elderly and vulnerable from financial fraud.

E-Scams

- BITS formed a subcommittee under the auspices of the Internet Fraud Working Group to address the various scams operating throughout the Internet today. The BITS e-Scams Subcommittee was comprised of e-commerce specialists from more than 30 financial institutions. The e-Scams Subcommittee’s goal was to provide information and best practices to BITS members and the financial services community in order to protect customers and enhance confidence in the Internet as a medium for online financial services. The result is a Members Only document that: defines the current landscape; assesses the impact of e-scams on financial institutions; reviews current industry technology solutions; provides an overview of an e-scam program with an emphasis on e-scam investigations; discusses outsourcing e-scams management; and outlines internal and external education and awareness programs. A final document is due for release in December 2005.

Back-Up Power Issues

- The *BITS Guide to Business-Critical Enterprise Power* (the *Guide*) is in draft. It provides financial institutions with industry business practices for understanding, evaluating and managing risks if the availability of the electrical system is disrupted. Further, it outlines ways financial institutions can enhance reliability and ensure uninterrupted back-up power, referred to as “enterprise power.” The *Guide* is written for interested parties—from CEOs to business managers, risk managers to business continuity professionals, procurement experts to facilities managers—as they analyze risks, conduct due diligence for enterprise power and integrate evolving regulatory and building code requirements into business continuity plans. The final *Guide* will be available early in 2006. The full draft, completed in 2005, is being used and vetted currently.

BITS Critical Success Factors for Security Awareness & Training Programs

- Under the auspices of the BITS Security and Risk Assessment Program, BITS developed a description of critical factors for establishing and maintaining a comprehensive security awareness and training program for financial institution personnel. Developing a comprehensive security awareness and training program is a regulatory requirement and an effective risk management practice.

BITS Key Considerations for Global Background Screening Practices.

- BITS released the *BITS Key Considerations for Global Background Screening Practices* on June 29, 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:
 - Overview of the financial industry's legal and regulatory requirements;
 - Strategies for evaluating the risks and mitigating controls for outsourced environments and activities; and
 - 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.

Strategies for Mitigating Fraud Risks Associated with the Check Clearing for the 21st Century Act

- This paper provides informed analysis of the risks and benefits associated with implementation of the Check 21 Act. Strategies for mitigating risks are included as well as a matrix that describes Check 21-related risks and mitigants from the standpoint of three major parties affected by the Act: the business customer that truncates checks before deposit, the bank of first deposit, and the paying bank.

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.

Best Practices in Patch Management for the IT Practitioner

- *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.

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 Guide to Business-Critical Telecommunications Services

- On November 15 of 2004, BITS released the *BITS Guide to Business-Critical Telecommunications Services*, however it has received continued use and additional visibility in 2005, including as a helpful tool in the aftermath of Hurricanes Katrina, Rita and

Wilma. The *BITS Guide* highlights questions business continuity planners and other risk managers should ask themselves as well as an overview of key points to consider in risk assessment, due diligence, contracting, testing and monitoring processes of their telecommunications services.

COMMENT LETTERS

Comment Letter on FDIC Study, “Putting an End to Account-Hijacking Identity Theft”

- BITS, The Financial Services Roundtable and the Identity Theft Assistance Corporation jointly submitted a comment letter, raising concerns about the proposed approach to remedies for fraud-related security risks. The study did 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 and recommended solutions that are complex, unwieldy, and, in some instances, will not provide the intended remedy.

Comment Letter on Department of Homeland Security (DHS) Interim Rule on Procedures for Handling Critical Infrastructure Information

- BITS and The Financial Services Roundtable submitted a comment letter to DHS on a rule to establish “uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal government through the Department of Homeland Security.” The letter outlines concerns about the scope and implementation of the procedures. It states that DHS must implement robust controls to adequately protect employees and customers of financial institutions.

TESTIMONY

Hearing on “Continuity of Operations in the Financial Services Sector Post a Major Event,” to the House committee on Government Reform Subcommittee on Government Management, Finance, and Accountability

- On September 26, BITS CEO Catherine A. Allen testified at a field hearing in New York City on the current status of financial market preparedness for wide-scale disasters and disruptions. The hearing was held by the House Committee on Government Reform Subcommittee on Government Management, Finance, and Accountability. Cathy’s testimony focused on actions the financial services sector has taken in response to the 9/11 terrorist event and natural disasters such as Hurricanes Katrina and Rita. She praised the financial services’ sectors preparedness and responsiveness and offered recommendations for additional steps that need to be taken by the Federal government and all critical infrastructure sectors. Cathy made specific recommendations for maintaining diverse and resilient communications channels, investing in the power grid, recognizing the dependence of all critical infrastructures on software operating systems and the Internet, and improving coordination among all critical infrastructures and with federal, state, and local government when events occur. She emphasized the importance of addressing the interdependence of all critical infrastructure sectors. Those of greatest concern to the financial services sector are interdependencies with telecommunications, energy and transportation sectors. For access to Cathy’s full testimony, go to http://www.bitsinfo.org/p_public_testimony.html.

**“The Department of Homeland Security Cybersecurity Enhancement Act of 2005”
to House Committee on Homeland Security Subcommittee on Economic Security,
Infrastructure Protection and Cybersecurity**

- Catherine A. Allen, BITS CEO, testified in April, 2005 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©.

SUMMITS, FORUMS AND CONFERENCES

Critical Infrastructure Protection

- BITS CEO Catherine A. Allen participated as one of four panelists at an event convened by George Mason University's Critical Infrastructure Protection Program at the National Press Club on November 29, 2005. Award-winning journalist Frank Sesno moderated the panel, "After the Storms, Repairing the Damage." James Lee Witt, former FEMA Director, keynoted the event. Other panelists were Dennis Barbour, Mayor of Carolina Beach, NC and J. Michael Hickey, Verizon. Catherine drew on lessons learned by the financial services sector, and stressed the continuing need to address issues of interoperability, interdependence with other sectors, implementation of lessons learned, and consumer confidence.
- BITS Senior Director John Carlson participated in the Vanderbilt University-hosted US Japan Critical Infrastructure Protection Forum on November 29 and 30, 2005 in Washington, DC. John spoke about BITS' efforts in cross-sector coordination among critical infrastructure sectors and cybersecurity and participated in a panel discussion on business continuity planning and response from a multi-day regional power outage scenario. The forum fostered dialogue between US and Japanese industries on how best to protect infrastructures that support those nation's economies. Speakers included senior US and Japanese government and private-sector officials and experts in financial services, information technology, power, telecommunications and transportation. For more information, contact John Carlson, john@fsround.org.
- John Carlson represented BITS at three meetings on July 11, August 12 and September 30, 2005 with senior Department of Homeland Security officials and over a dozen associations representing the business, IT and telecommunications industries. The purpose of the meetings was for the Department of Homeland Security to get input and recommendations from association leaders who are active in cyber security issues and to discuss how best to assess cyber security risks, improve the public/private partnership, expand information sharing, and develop public and private incentives to encourage government and the private sector to enhance cyber security.
- On June 17, 2005 Dartmouth's Institute for Information Infrastructure Protection (I3P) hosted a forum on "Financial Services Challenges in the Cyber World" at New York University in New York City. BITS participated in a panel discussion along with representatives from BITS member companies and key federal government agencies. Approximately 25 government and academic leaders involved in research on cyber security and critical infrastructure issues participated in the meeting.

- BITS held conference calls with senior business continuity planning and fraud reduction officials of member companies to discuss the impact of Hurricane Katrina on members and the financial services sector overall as well as relief efforts. BITS disseminated daily updates to members beginning on September 1, serving as a repository and conduit for timely information. BITS worked closely with the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and disseminated key information to our members from regulatory agencies, Treasury and the Department of Homeland Security. Topics included assessment of impacts from the storm, efforts to deliver adequate cash supplies, FEMA's distribution of debit cards to victims of Katrina, talking points for consumer assistance, guidance from regulatory agencies, and important contacts for additional support. BITS also helped develop a press release that was issued by the FSSCC and outlined the sector's efforts to respond to the crisis. This information-sharing and coordinating role continued through Hurricanes Rita and Wilma on an as-needed basis. BITS also worked with the FSSCC to develop a memo on lessons learned from the Hurricanes that was sent to Treasury and the FBIIC.

A Strategic Look at Authentication

- On March 8, 2005, BITS hosted 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 focused 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.

BITS Regulatory Forum

- The BITS Regulatory Forum was held on April 26, 2005 and established a dialogue among regulators and financial services firms on the impact of regulatory requirements and supervisory processes. Many of those requirements relate to critical infrastructure protection and security issues. Participants reviewed steps to be taken by all parties to increase efficiency in the regulatory and supervisory process. Senior level regulators and BITS members took part in this session, the first step in an iterative, cross-sector process. The Forum was the first public release of the study, developed on BITS' behalf by KPMG, "Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy"

BITS/American Banker Financial Services Outsourcing Conference

- The Fourth Annual BITS/American Banker Outsourcing Conference, presented with The Santa Fe Group in 2005, was held on November 7 - 8 at the Renaissance in Washington D.C. This year's agenda followed four key themes:
 - Governance: Best practices of financial institutions and service providers.
 - Compliance: Strategies for negotiating the current landscape and requirements for privacy and security.
 - Risk Management: Strategies, controls and processes to coordinate risk management across the enterprise.
 - Change: Practical guidance for managing today's dynamic relationships.

POLICY DEVELOPMENT

NOTE: BITS serves as a source of fact-based information in the development of policy positions. Following are recent examples, resulting either in a formal position from both BITS and The Financial Services Roundtable, or indirectly, through participation in national-level councils, working groups and task forces. Other examples of BITS' role in policy development are listed above in the categories of Comment Letters and Testimony.

- Joint BITS and Financial Services Roundtable Policy on Authentication Mandates
- Joint BITS and Financial Services Roundtable Policy on Spyware
- Joint BITS and Financial Services Roundtable Policy on Software Security
- Joint BITS and Financial Services Roundtable Policy on Internet Fraud and Phishing
- Support for President's National Infrastructure Advisory Council (NIAC)
- Participation in National Security Telecommunications Advisory Council (NSTAC) Financial Services Task Report
- Participation in Network Reliability and Interoperability Council (NRIC) VII
- Participation in Congressman Adam Putnam's Corporate Information Security Working Group (CISWG)
- Participation in the National Cyber Security Partnership

PILOTS AND PROJECTS

Financial Institutions Shared Assessments Project (FISAP)

- BITS has recently launched a new project aimed at improving efficiencies and achieving cost savings related to assessments of shared third party services providers. This Financial Institutions Shared Assessment Project (FISAP) is in pilot stage.
- Six institutions formed FISAP to leverage the *BITS Framework* and *BITS Expectations Matrix* and develop an industry solution for service provider assessments. Big Four firms are acting as Technical Advisors to the project. Critical success factors are to:
 - Develop reports that are comprehensive and suitable for multiple financial institutions;
 - Reduce the time and resources financial institutions and service providers spend responding to and executing one-off assessments to verify controls and security;
 - Create a process that is repeatable and consistent; and
 - Encourage support of regulators.
- The project is intended to result in significant cost savings and efficiency gains. These "shared assessments" are being developed to improve assessments based on consistent and objective information that is provided through a regularly-updated, standardized questionnaire as well as third-party testing and objective reporting on controls. It should be noted that FISAP is not a "100%" solution. The savings and efficiencies will fluctuate by risk, service and amount of dedicated vs. shared services. BITS expects to expand this project to additional participants in early 2006.

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 includes a searchable database of information from other financial institutions on their phishing incident and response experience, including contacts at law enforcement agencies, foreign governmental agencies, and ISP Web administrators. The Network also provides data on trends to help law enforcement build cases and shut down identity theft operations. The BITS Phishing Prevention and Investigation Network:

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

ChicagoFIRST

- With the encouragement of the US Treasury and support from BITS, Chicago's premier financial services institutions formed ChicagoFIRST in July 2003 as an industry coalition that addresses homeland security issues requiring a common response by Chicago's financial services sector. In 2005, ChicagoFIRST became a model for a similar regional coalition in Florida. These initiatives are prompted by a consensus that existing activities at the regional level do not adequately address the critical infrastructure protection concerns of Chicago's financial institutions. The mission of ChicagoFIRST is:
 - To increase the resilience of the Chicago financial services industry in the event of a regional disaster in collaboration with the city, state and federal agencies, including to:
 - protect the lives of the thousands of people that work in the industry;
 - protect the financial assets that have been entrusted for safe keeping and investment;
 - work directly with city and state authorities on emergency coordination and evacuation; and
 - implement the primary objectives in a rapid manner.

The "lessons learned" from ChicagoFIRST, as reported above and funded by the US Treasury, were published in December 2004, with the hope that additional coalitions will successfully establish similar organizations to strengthen critical infrastructures at a regional level. The Treasury supports the concept of regional coalitions of financial services firms and will work with interested parties to facilitate their formation. For more information, please contact the Office of Critical Infrastructure Protection and Compliance Policy at (202) 622-2602.

Identity Theft Assistance Center (ITAC)

- The Identity Theft Assistance Center (ITAC) was initiated as a one-year pilot program intended to help victims of identity theft by streamlining the recovery process and by enabling law enforcement to identify and prosecute perpetrators of this crime. The ITAC is now officially up and running as the pilot was a success. As of August 2005, more than 2500 victims of identity theft had received assistance from the ITAC. ITAC is an initiative of The Financial Services Roundtable and BITS, which represent 100 of the largest integrated financial services companies. The ITAC's services are free-of-

charge to customers and made available based on referrals to the ITAC by one of the ITAC's Members. For additional information, go to www.identitytheftassistance.org.

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. 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 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.

SURVEYS AND RESEARCH

Cybersecurity R&D Priorities.

- The results of a 2005 BITS survey on cybersecurity research and development are being used to advise the federal government (Congress, Treasury, the Department of Homeland Security) on its R&D priorities. The BITS survey coincides with the publication of a Cyber Security Industry Alliance (CSIA) paper urging the federal government to play a larger role in coordinating cybersecurity R&D funding. The CSIA paper notes that while the private sector contributes the majority of funds for R&D on cybersecurity, most of this money is for short-term solutions to existing problems. The CSIA and BITS are recommending the federal government organize long-term cybersecurity research to address problems before they emerge.

FOR ADDITIONAL INFORMATION, CONTACT:

Catherine A. Allen, CEO
John Carlson, Senior Director
BITS
1001 Pennsylvania Avenue NW
Suite 500 South
Washington DC 20004

(202) 289-4322
cathy@fsround.org
www.bitsinfo.org

ABOUT BITS

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. For more information, go to www.bitsinfo.org.