

BITS

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

BITS Fraud Steering Committee and BITS Fraud Program 2007 Accomplishments

BITS Fraud Steering Committee

In addition to providing oversight and guidance to the various working groups and projects under the BITS Fraud Program, the BITS Fraud Steering Committee (FSC) provided input and/or review to the following forums, papers, and/or projects:

Comment Letters

- **President's ID Theft Task Force.** (January 2007) The letter provided recommendations to improve the effectiveness and efficiency of the U.S. federal government's efforts to reduce identity theft. The letter is available at <http://www.bitsinfo.org/downloads/Comment%20letters/BITSRoundtableIDTaskForceLetterFINAL.pdf>.
- **ICANN/WHOIS Database.** (January 2007) The letter reinforced the industry's position and concerns about continued access to the WHOIS database by supporting the "special circumstances model." The letter is available at <http://www.bitsinfo.org/downloads/Comment%20letters/BITSFSRWHOISCommentLetterJan122007.pdf>.
- **DHS NPRM for Minimum Standards for State-issued Driver's Licenses and ID Cards in Compliance with the REAL ID Act of 2005.** (May 2007) This letter commented on the following five areas of concerns identified by members of the BITS FSC, Security Working Group, and former Identity Theft Working Group: the importance of secure government-issued credentials and a secure enrollment process; the operation of the "federated query service" and its protection of sensitive personal information; the use and challenges associated with card encryption; the security and protection of data and databases that house the personal information of consumers; and the use of background checks on DMV employees. The letter is available at <http://www.bitsinfo.org/downloads/Comment%20letters/RoundtableCommentLetterREALID NPRMMay07.pdf>.
- **Social Security Administration's CBSV Process.** (September 2007) The letter recommends flexibility for obtaining individual consent and alternatives to a stand-alone Form SSA-89. The letter is available at http://www.fsround.org/policy/regulatory/pdfs/Roundtable_CBSVcomments_091207.pdf.
- **SSNs in the Private Sector.** (September 2007) The comment letter outlined current laws and regulations relating to the required uses and protection of SSNs as well as financial services industry leadership in protecting SSNs and reducing their use, particularly in the authentication process. The letter is available at http://www.fsround.org/policy/regulatory/pdfs/FSRoundtablecomments_SSNs_090507.pdf.
- **Unlawful Internet Gambling Rule.** (December 2007) Submitted in response to the U.S. Department of the Treasury and Federal Reserve Board's proposed rule on "Prohibition on

Funding of Unlawful Internet Gambling” that implements provisions of the Unlawful Internet Gambling Enforcement Act of 2006, the letter provided specific comments on provisions and requests clarifications on issues such as definitions, terms, and monitoring requirements; the expectations of financial institutions to maintain a list of illegal gambling entities; and how regulators will enforce the rule. In addition, the comment letter recommends that Safe Harbor provisions be strengthened and that the deadline for implementation be extended to account for the time it will take financial institutions, payments organizations and others to develop rules and modify systems that will be necessary to comply with final requirements. The letter is available at http://www.fsround.org/policy/regulatory/pdfs/FSRUnlawfulInternetGamblingLetter_final.pdf.

Formal Surveys

- **Federal Reserve Survey on Retail Payments Fraud.** (January 2007) Provided responses to the survey, which gathered information from the industry regarding current trends in payments fraud, key issues/concerns, mitigation methods, structural barriers to detection/mitigation and industry initiatives to reduce fraud.

Forums

- **BITS Forum, “A Strategic Look at Mitigating Internal Fraud.”** (March 2007) More than 130 representatives from 85 companies attended the forum. Attendees heard from a distinguished group of speakers and panelists from financial institutions, regulatory and law enforcement agencies, and the vendor and consulting community who spoke to the key elements needed to mitigate the risk of internal fraud.

Support of Federal Law Enforcement Efforts

- The BITS FSC provided support to USPIS regarding their National Internet Fraud Consumer Awareness Campaign and Global Counterfeit Strategy Initiative by promoting and encouraging member involvement in these efforts. Members attended calls and meetings as needed, promoted efforts internally and via the BITS Weekly Fraud Update and website; and encouraged member attendance at industry briefings.

BITS Fraud Program: Working Groups and Projects

BITS ACH Risk Project Group, led by Shirley Inscoc, Wachovia Corporation

- ***BITS ACH Check Conversion Risk Management Toolkit.*** (March 2007) This document addresses the risks and liabilities associated with check conversion from the both the Originating Depository Financial Institution (ODFI) and Receiving Depository Financial Institution (RDFI) perspective.

BITS Debit Card/ATM Fraud Working Group, led by Linda Chumley and Kevin Hale, Wells Fargo & Company

- This group met quarterly to share information and mitigation strategies in response to fraud losses due to several merchant compromises. The group also discussed ATM fraud loss trends and shared a member case study regarding their experience and the strategies implemented to prevent and detect skimming incidents on their ATM estate.

BITS Mortgage Fraud Reduction Project Group, led by Susan Dailey, JPMorgan Chase & Co.

- **BITS/MBA Quarterly Meeting with Federal Law Enforcement.** (February 2007) BITS and MBA representatives from mortgage lending companies met with representatives from the FBI, DOJ and FinCEN to discuss issues such as SAR filings and guidelines, local task forces, and law enforcement and consumer education. During this meeting, BITS was tasked with developing a “Marketing 101” document to provide information to financial institutions on how to package cases to enhance investigation/prosecution.
- **Mortgage Fraud: Processes and Procedures Matrix.** (July 2007) This informal project resulted from members’ expressed interest in sharing information about how their peers’ mortgage fraud departments are structured and how they identify and track mortgage fraud. A matrix was released on July 2 to members only for completion by July 27. Anonymized and compiled responses were circulated only to those who participated. Generalized answers were shared with the group during the September conference call.

BITS Remote Channel Fraud Working Group, led by Stan Szwalbenest, JPMorgan Chase & Co.

- **Remote Channel Fraud: Achieving the Ideal Risk Environment Matrix.** A subgroup developed and circulated a matrix for completion by members to identify the current risks to the various remote banking channels and products, and to identify effective control strategies that have been implemented by institutions to mitigate these risks.
- **Information Sharing Calls.** This group met via conference call on a monthly basis to share information on various issues including:
 - Members’ experiences and efforts to address VoIP fraud;
 - High velocity fraudulent credit applications from the Internet channel;
 - Measuring online fraud losses;
 - Interbank transfers via the online channel and customer authentication across the enterprise;
 - Telephone banking authentication;
 - Taxonomy of phishing frauds; and
 - Fraud trends in vishing; pharming, Trojan horse bots, etc.

BITS Rising Fraud Risk Discussion Forum, led by Dorothy Steffens, Credit Union National Association (CUNA) and Scott Grizzle, Sovereign Bancorp

- **New Relationship Fraud.** (January 2007) Participants identified the need for an additional call to revise the definitional timeframe of new account fraud; share confirmed, known bad addresses and telephone numbers; and share risk mitigation strategies that financial institutions have employed.
- **Impact of TJX Compromise on DDAs.** (February 2007) Participants identified the need to engage in discussions with the National Retail Foundation (NRF) to discuss how merchants/retailers establish a hub/network for information sharing.
- **Increase in Fraud via WesternUnion.com.** (February 2007) Participants discussed trends and losses associated with this fraud and shared mitigation strategies. Information was shared with Western Union representatives, establishing a collaborative partnership to address this issue. Subsequently Western Union representatives joined the BITS FSC and Debit Card/ATM Fraud Working Group calls to discuss the issue.

- **New Account Fraud.** (March 2007) A continuation of the January call that focused on new account fraud, this discussion focused on the timeline for “new account fraud” and if/how members may share confirmed bad addresses and telephone numbers associated with this fraud, and share risk mitigation strategies.
- **Increases in Fraud due to Compromised Customer Information on the Deposit Accounts.** (June 2007) A member reported on a recent investigation into a case where a high value customer experienced identity theft and account compromise, which uncovered the potential for a huge loss to the financial institution and highlighted the need for enterprise fraud management and file sharing among all lines of business. This incident was not a data breach or privacy event, but an attack on a full banking relationship where information on a customer has been culled including DOBs, PINs, etc., a profile built, and accounts were taken over or established to commit fraud. The fraudsters have a high amount of customer information, including dates of birth, PIN numbers, and other authentication data.
- **Reverse Phishing.** (July 2007) The call discussed trends and distributed a NACHA advisory to BITS membership to raise awareness of the increase in ACH phishing attacks targeted against treasury management services. A follow up call was held in August to discuss and identify what, if any, ramifications exist, should financial institutions share payee information in an attempt to combat this fraud.
- **Diagnosing Infected Computers and Educating Consumers.** (October 2007) This call focused on if/how financial institutions diagnose customers’ computers that have been infected with malware, software and other incendiary information gathering devices. Financial institutions were also asked to share what programs/efforts they had in place to increase consumer education on how to protect their computers.
- **Increase in Counterfeit Travelers Checks.** (November 2007) Carol Christensen, American Express, discussed trends seen regarding counterfeit Travelers and Gift Cheques. While the vast majority of American Express cheques presented to financial institutions are authentic, there have been reports of altered and counterfeit paper, and it is believed there may be an increase around the holiday shopping season. Subsequent advisories have been distributed to members and posted on the BITS website to increase awareness.
- **Fraud Considerations for Mobile Banking.** (December 2007) Javelin Strategy & Research representatives presented on security considerations and implementation concerns related to the implementation of mobile banking. Much of the information provided was gathered from their April 2007 report, “The Call for Technology Standards and Proactive Security Messaging.” This study focused mainly on consumers’ perception of, and interest in, mobile banking.

For additional information, contact:

Heather Wyson
 Director
 BITS
 202.289.4322
 heather@fsround.org
 www.bitsinfo.org

Appendix A: 2007 Fraud Steering Committee Participating Institutions

Chair: Kim Duncan, SunTrust Banks, Inc.

Vice Chair: William “Tom” French, Bank of America Corporation

Bank of America Corporation
The Bank of New York Mellon Corporation
BB&T Corporation
Capital One Financial Corporation
Citigroup Inc.
Citizens Financial Group
Comerica Incorporated
Countrywide Financial Corporation
Credit Union National Association (CUNA)
Federal Reserve Bank of Philadelphia
Federal Reserve Board
Fifth Third Bancorp
JPMorgan Chase & Co.
Sovereign Bancorp
SunTrust Banks, Inc.
U.S. Bancorp
Wachovia Corporation
Washington Mutual, Inc.
Wells Fargo & Company