

ADDITIONAL INFORMATION FROM

ERIK STEIN

EXECUTIVE VICE PRESIDENT & DIRECTOR,
FRAUD RISK MANAGEMENT
COUNTRYWIDE FINANCIAL CORPORATION

SUBMITTED ON BEHALF OF BITS

FOLLOWING TESTIMONY BEFORE THE

UNITED STATES CONGRESS
HOUSE COMMITTEE ON WAYS & MEANS
SUBCOMMITTEE ON SOCIAL SECURITY

HEARING ON
THE ROLE OF SOCIAL SECURITY NUMBERS (SSNs)
IN IDENTITY THEFT AND
ISSUES RELATED TO ENHANCING PRIVACY

ORIGINAL TESTIMONY WAS DELIVERED
MARCH 30, 2006

BITS

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

Submitted May 8, 2006

NOTE:

The following is additional information provided by BITS at the request of Rep. Xavier Becerra following the testimony of Erik Stein, Executive Vice President & Director, Fraud Risk Management, Countrywide Financial Corporation. Mr. Stein testified on BITS' behalf on March 30, 2006.

ADDITIONAL INFORMATION

BITS would like to again thank Chairman McCrery and the Subcommittee on Social Security of the Ways & Means Committee for the opportunity to present testimony on March 30, 2006 on the role of Social Security Numbers in Identity Theft and enhancing SSN privacy. During the hearing, Mr. Becerra¹ requested that Erik Stein, on BITS' behalf, provide the committee with additional information on industry practices to safeguard the consumer information of account holders and/or borrowers at financial institutions that have closed these accounts. The following is a general overview of the information security practices of financial institutions and general business practices for securing information and protecting customer information after account or loan closure.

The financial services industry makes security and privacy protection a first priority by virtue of its fiduciary responsibilities to customers and stockholders, maintenance of public confidence (and therefore the health of the economy) and regulatory requirements for maintaining safety and soundness in the financial system.

Five agencies—the Federal Reserve Board, Office of the Comptroller of the Currency, Office of Thrift Supervision, Federal Deposit Insurance Corporation and the U.S. Securities and Exchange Commission—share responsibility for the oversight and supervision of financial services at the federal level. While specific approaches vary among institutions within the financial services sector, the industry uses as a guide the risk management framework developed by the federal financial regulators through the Federal Financial Institutions Examination Council (FFIEC).² The FFIEC framework is risk-based and robust and serves as the *de facto* industry standard. All financial institutions are required to comply with a rigorous set of regulations and guidelines. In addition, examiners from the federal

¹ This request was made following the testimony provided by witnesses of third panel which included Erik Stein, Countrywide Financial Corporation, who represented BITS.

² The Federal Financial Institutions Examination Council (FFIEC) is a regulatory consortium comprised of experts from the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration. Visit <http://www.ffiec.gov/ffiecinfobase/index.html>.

financial regulators routinely assess the adequacy of security programs to ensure that financial institutions operate in a safe and sound manner.

Member agencies of the FFIEC defined such a process-based approach to security in the “Guidelines Establishing Standards to Safeguard Customer Information” to implement section 501(b) of the Gramm–Leach–Bliley Act of 1999 (GLBA). The guidelines afford powerful and prompt enforcement options to the FFIEC agencies if financial institutions do not establish and maintain adequate information security programs. The FFIEC Information Security booklet follows the same process-based approach, applies it to various aspects of the financial institution’s operations, and serves as a supplement to agency GLBA 501(b) expectations. The framework takes into account other regulatory requirements, such as those in the Sarbanes-Oxley Act, Basel II and the Federal Deposit Insurance Corporation Improvement Act (FDICIA).

The FFIEC framework provides an approach for implementing an enterprise-wide security program. The framework includes oversight of third party service providers. Regulators examine financial institutions and hundreds of third party service providers on a regular basis. According to the FFIEC, financial institutions are required to implement an ongoing security process, and assign clear and appropriate roles and responsibilities to the board of directors, management and employees. Senior management must provide management with expectations and requirements for:

- Central oversight and coordination;
- Areas of responsibility;
- Risk measurement;
- Monitoring and testing;
- Reporting; and
- Acceptable residual risk.

Building a framework requires financial institutions to complete an Information Security Risk Assessment. According to the FFIEC, financial institutions must maintain an ongoing Information Security Risk Assessment program that effectively:

- Gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements;
- Analyzes the probability and impact associated with the known threats and vulnerabilities to its assets; and
- Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and testing necessary for effective mitigation.

It is important to note that financial institutions have established document retention periods associated with their account records. These retention periods are based on a number of considerations, not the least of which is regulatory compliance obligations. In the case of loans, even once closed, information remains in the consumer’s credit report for seven years after closure. During this period consumers may have questions regarding information (derogatory or otherwise) that may require a review of the loan documents to respond appropriately to the consumer’s question. The credit grantor, in the absence of

supporting documentation, may have an obligation to remove information³ that is reported to the bureaus, thereby obligating the lender to retain those records for a period commensurate with the information contained in the credit report.

It is important to yet again acknowledge that the business practices and approaches listed below may vary among institutions. In addition, many of following practices are not exclusive to the protection of consumer information solely after account or loan closure. They may also be applied to open/existing relationships.

ROLE-BASED ACCESS - Many financial institutions have implemented, or are in the process of implementing, role-based access. Role-based access uses the theory of “least privilege” to ensure that employees receive, at a maximum, the minimum level of access to sensitive information required to perform their job functions. (See next paragraph for more information regarding least privilege.) These access levels are modified based on changes in the employee’s job functions or changes in the consumer’s circumstances. For example, if an account or loan is closed, employees who once required access to sensitive customer data while the relationship was open⁴ may no longer have a business need for such information. Thus, their access to this information is then terminated.

LEAST PRIVILEGE - Least privilege ensures that employees don’t have access to information that exceeds their need to know to perform their job. Many financial institutions apply the theory of least privilege to restrict access to sensitive information (e.g. Social Security Numbers) by employees. Employees can be segmented into three broad groups:

- (1) Those who have no need to view, confirm or edit consumer SSNs and therefore do not have access to SSNs at all (e.g., accountants, facilities managers);
- (2) Those who have a need to verify consumers using their SSN (e.g., customer service agents, tellers) who see only a redacted version of the SSN (i.e., last 4 digits); and
- (3) Those who have a need to view, confirm or edit the full SSN (e.g., investigators, tax-reporting employees) who are allowed specialized access sufficient to appropriately perform their job.

DATA COLLECTION - The industry has undertaken, and continues to undertake, thorough evaluation of the data it collects from consumers during account opening, loan origination and other transactions to determine the need and use of the data collected. Financial institutions have a vested interest in ensuring that they only collect information that is necessary and subsequently retain only that for which there is a continuing business need or statutory or regulatory obligation.

DATA DISCLOSURE - Financial institutions review data that they provide both internally and externally to employees, consumers and others. This ensures that wherever customer-specific information is displayed, it is either mandated by law or regulation or required to meet a specific business purpose and is not inconsistent with applicable law or regulation. Specific examples of this type of review includes: the removal or truncation of SSNs when

³ This can include derogatory information.

⁴ (e.g. tellers, customer service agents, etc.)

the entire number is not required; and the removal or truncation of the account number or credit card number where the full number is not essential.

AUDIT LOGS - Many financial institution applications maintain audit logs which record activities conducted through or within the application. These audit logs can provide the records of employees, contractors and others who have accessed consumer information. The knowledge of the logs' existence serves as a deterrent to unauthorized access, allows detection of access attempts and provides evidence of unauthorized activity.

ANOMALOUS BEHAVIOR MONITORING - Audit logs can also facilitate anomalous behavior detection (i.e. activity that is inconsistent with expected behavior or outside the scope or realm of anticipated norms), thereby providing an early indicator of potentially fraudulent activity.

ENCRYPTION - Based on the specifics of each circumstance, financial institutions may encrypt sensitive consumer information including both data in transit and data at rest. Varying encryption types may be used again based on the facts and circumstances of the need and the sensitivity of the data. This encryption ensures that unauthorized access does not result in the compromise of the encrypted data.

RETENTION PERIODS - Information retention periods are established by financial institutions in conformance with legal, regulatory and contractual obligations. These retention periods ensure that information, including consumer information, no longer required is destroyed.

SECURE DESTRUCTION - When records are available for destruction, based on financial institutions' document retention schedules, destruction is accomplished securely, typically through third-party secure document destruction services. The documents, tapes, and other media are completely destroyed so as not to be retrievable.

NETWORK PROTECTION - Financial institutions have some of the most rigorous intrusion detection, malware⁵ detection and cleaning, traffic monitoring, firewall routing technology available to protect their network infrastructure, consumer information and proprietary secrets.

Thank you again for the opportunity to provide additional information. Please contact us with any questions or additional requests.

BITS
The Financial Services Roundtable
1001 Pennsylvania Avenue NW
Suite 500 South
Washington DC 20004
(202) 289-4322
Attention: Heather Wyson, BITS Director

⁵ Includes viruses, Trojans, worms, etc.