



BITS/ABA

**KEY CONSIDERATIONS FOR
RESPONDING TO UNAUTHORIZED ACCESS TO
SENSITIVE CUSTOMER INFORMATION**

A PUBLICATION OF BITS
AND
THE AMERICAN BANKERS ASSOCIATION

DISCLAIMER

THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. Neither the individual members nor the member institutions of BITS, The Financial Services Roundtable, or the American Bankers Association, make any warranty or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of the information contained in this document, or represent that this document's use would not infringe privately-owned rights. Reference to any particular or special commercial products, processes, procedures, or services by trade name, trademark, service mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by BITS, The Financial Services Roundtable, the American Bankers Association, or any of their individual members.

ABOUT THE ABA AND BITS

The **American Bankers Association**, on behalf of the 2.2 million men and women who work in the nation's banks, brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership – which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks – makes ABA the largest banking trade association in the country.

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 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 three working groups that have a significant interest in responding to unauthorized access to sensitive customer information—the information security experts who are involved in the BITS Security and Risk Assessment Working Group, the fraud reduction experts who are involved in the BITS Fraud Reduction Steering Committee (FRSC), and the outsourcing risk managers who are involved in the BITS IT Service Provider Working Group.

BITS
1001 PENNSYLVANIA AVENUE, NW
SUITE 500 SOUTH
WASHINGTON DC 20004
(202) 289-4322
WWW.BITSINFO.ORG

AMERICAN BANKERS ASSOCIATION
1120 CONNECTICUT AVENUE, NW
WASHINGTON DC 20036
1-800-BANKERS
WWW.ABA.COM

BITS/ABA
KEY CONSIDERATIONS FOR
RESPONDING TO UNAUTHORIZED ACCESS TO SENSITIVE CUSTOMER
INFORMATION

TABLE OF CONTENTS

EXECUTIVE SUMMARY AND INTRODUCTION

LEGAL AND REGULATORY BACKGROUND

DIFFERENCES IN FEDERAL AND STATE CUSTOMER NOTIFICATION REQUIREMENTS

EXEMPTIONS FROM STATE LAW

DEFINITIONS OF COVERED INFORMATION

NOTIFICATION TRIGGERS AND TIMING

NOTIFICATION FORMAT AND CONTENTS

ELEMENTS OF A CUSTOMER RESPONSE PROGRAM

DEVELOPING AN INCIDENT RESPONSE TEAM

ASSESSING THE NATURE AND SCOPE OF AN INCIDENT

TAKING STEPS TO CONTAIN AND CONTROL THE INCIDENT

NOTIFYING THE INSTITUTION'S PRIMARY FEDERAL REGULATOR

WORKING WITH LAW ENFORCEMENT

NOTIFYING CUSTOMERS AND PROVIDING ASSISTANCE

THIRD PARTY SERVICE PROVIDER CONSIDERATIONS

APPENDICES

APPENDIX A: BITS AND ROUNDTABLE SECURITY BREACH CUSTOMER NOTICE POLICY STATEMENT

APPENDIX B: ABA AND BITS PROGRAMS, GUIDES AND TOOLS FOR DATA SECURITY, FRAUD REDUCTION, ID THEFT PREVENTION AND ASSISTANCE, AND THIRD PARTY OUTSOURCING

EXECUTIVE SUMMARY AND INTRODUCTION

Unauthorized access to sensitive customer information threatens to undermine customer confidence and the reputations of both individual financial institutions and the financial services industry. This threat is aggravated by the patchwork of state laws and federal regulations that govern unauthorized access or breach response incidents. Despite these challenges, financial institutions are strengthening data security programs and developing or improving customer notification programs. The “BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information” is a tool that may assist some financial institutions in developing and executing response programs when sensitive information is accessed and misused by unauthorized individuals.

The genesis of this paper dates to 2003 when several BITS working groups initiated discussions among information security experts within BITS/Financial Services Roundtable companies, the American Bankers Association, service providers, and regulators in response to emerging breach notification requirements. Since 2003, these experts have gained experience in mitigating the risks of unauthorized access while legal and regulatory standards have continued to evolve. In addition, the CEOs of BITS and The Financial Services Roundtable member companies adopted in March 2005 a policy statement on Security Breach Customer Notice which is found in Appendix A. Appendix B includes information on BITS and ABA programs, guides and tools that may be helpful resources for financial institutions in securing data.

The paper is divided into several sections that cover the following:

- **Evolving legal and regulatory requirements**, including differences in state and federal unauthorized access or breach response requirements. The focus points in this section are key areas where state laws most often diverge from each other and from federal regulation. Among these areas are notification triggers and timing, definitions of covered information, and notification method and content.
- **Potential elements of a response program**, including: a response team, coordination with various offices and lines of business, risk assessment processes for determining the risk of harm and potential impact, customer notification programs, oversight and coordination with third party service providers, and coordination with law enforcement, regulators, and other government officials. Not all of these elements will be included in every response program.
- **Considerations for managing third party service provider relationships** as they relate to data security programs and customer notification.

This document should not be construed as legal, regulatory or compliance advice. Because unauthorized access or breach response legislation and regulation are evolving at the state and federal levels, this paper should be viewed as a tool that may help some financial institutions develop and refine their own response program based on structure, risk, and the applicability of state and federal law and regulation.

LEGAL AND REGULATORY BACKGROUND

Public concern over the protection of sensitive information has increased in recent years. Media reports of potential unauthorized access to sensitive customer information have led state legislative and federal regulatory bodies to enact a variety of requirements mandating responses to such events, including customer notification.

California was the first state to enact regulations requiring responses to data breaches. As such, the California law has become the model for other states enacting customer notification legislation and it therefore serves as an example throughout this document. In March 2005, the federal financial regulatory agencies issued final guidance¹ entitled, “Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice” (“Guidance”).²

As of September 15, 2006, thirty-three states had adopted notification laws. As of that same date, eighteen bills failed to pass at the state level that either sought to require notification for the first time or to amend existing state notification requirements. Activity at the state level is likely to continue in 2007, with six bills from 2006 either requiring further study or scheduled to be carried over for consideration in 2007. In addition, the United States Congress is considering national standards that could potentially preempt state laws.

Compliance with state laws creates significant challenges for financial institutions given that the majority of financial institutions operate or have customers in multiple states. National uniformity, both geographically and across industries, is critical to preserving a fully functioning and efficient national marketplace. The differences in state laws create inconsistent standards that financial institutions must reconcile when undertaking notification following unauthorized access to sensitive customer information.

Enacting unauthorized access and breach response laws based on customers’ permanent residences is problematic for both large, international financial institutions and community-based financial institutions located in a single state. For example, community banks may have locations in only one state, but they almost always have customers who are residents of other states. This forces even community banks to reconcile inconsistent laws and regulations before they begin to notify customers.

Sensitive customer information is retained by many organizations and government agencies, not just financial institutions. The Identity Theft Resource Center reports that, in the first half of 2006, financial institutions accounted for only twelve percent of reported potential data compromise incidents (see chart below). The majority of incidents, seventy-eight percent, occurred at educational institutions, government agencies, retailers or others. Notwithstanding this, customers of financial institutions may perceive financial institutions as “guilty parties” even when a financial institution has no connection to a breach. This creates a significant risk of damage to a financial institution’s reputation, a vulnerability that is outside the control of the financial institution itself. In order to provide meaningful and consistent protection for consumers, all entities that handle sensitive customer information – not just financial institutions – should be subject to similar security standards.

¹ BITS and The Financial Services Roundtable submitted a comment letter on the proposed guidance. The comment letter is archived at: <http://www.bitsinfo.org/downloads/Comment%20letters/bitsbreachnotcloct03.pdf>

² 70 Fed. Reg. 15736-15754 (29 March 2005). Office of the Comptroller of the Currency. 12 CFR Part 30; Federal Reserve System. 12 CFR Parts 208 and 225; Federal Deposit Insurance Corporation. 12 CFR 364; Office of Thrift Supervision. 12 CFR Parts 568 and 570. “Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.”

RECENT PUBLICIZED INCIDENTS OF UNAUTHORIZED ACCESS TO SENSITIVE INFORMATION JANUARY – JUNE 2006		
Category	Number of Incidents	
	Number Reported	Percent of Total
Educational Institutions	39	30%
Governmental/Military Agencies	38	30%
General Business	23	18%
Banking/Credit/Financial Services	15	12%
Health Care Facilities/Companies	13	10%
Total	128	100%

Source: Identity Theft Resource Center, 2006

The federal Guidance that already applies to banking institutions offers federal and state policymakers both a model and a measure of experience to aid in establishing national umbrella consumer protections that could also extend to all industries that maintain sensitive consumer information. The Guidance outlines standards for safeguarding sensitive information and states that financial institutions should develop and implement a risk-based customer response program to address incidents of unauthorized access to or use of sensitive customer information that could result in substantial harm or inconvenience to a customer. The Guidance states that, at a minimum, the response program should contain procedures for:

- **Assessing the nature and scope of an incident** and identifying what customer information systems and types of customer information have been accessed or misused;
- **Notifying the institution’s primary federal regulator** as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;
- **Filing a timely Suspicious Activity Report (SAR)** in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, and promptly notifying appropriate law enforcement authorities;
- **Taking appropriate steps to contain and control the incident** to prevent further unauthorized access to or use of customer information; and,
- **Notifying customers** in a clear manner, if the financial institution becomes aware of an incident of unauthorized access to the customer’s information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or is reasonably possible to occur.

As more fully described in the next section of this paper, some states have attempted to use the Guidance in this fashion. Other states have developed unauthorized access or breach response requirements that are inconsistent with the Guidance. These inconsistencies perpetuate an environment that is confusing for consumers and inefficient and burdensome for financial institutions.

DIFFERENCES IN FEDERAL AND STATE CUSTOMER NOTIFICATION REQUIREMENTS

Exemptions from State Law

Twenty-two of the thirty-four states that recently enacted unauthorized access or breach response laws have instituted exemptions from their state law. In twenty-one of these states, a specific exemption exists for financial institutions that are subject to and in compliance with the federal Guidance. Where there is no exemption, or where more than one law may be applicable despite an exemption, financial institutions may find themselves facing conflicting state and federal standards.

Definitions of Covered Information

The states have enacted a number of definitions for “covered information.” Several of these definitions conflict with each other and with the definition in the Guidance. The first and most significant state breach notification law was enacted in 2002, and made effective July, 1 2003, by the state of California and codified in Section 1798 of the California Civil Code. The definition of covered information under Section 1798 (better known as Senate Bill 1386) is less encompassing than the standard put in place by the Guidance. Specifically, SB 1386 set a breach notification standard that pertained exclusively to unencrypted “computerized data.”³ The federal Guidance promulgated an expanded definition of “sensitive customer information” which covers information in all forms.⁴ There are also significant differences among states and between states and the federal Guidance as to the categories of information that can trigger notification.

Another difference in the scope of covered information stems from diverging use of terms. Some laws and regulations apply to customer information, others to consumer information, and still others to personal information. The precise scope of a given term is often governed by the definitions of the law or regulation, and a financial institution may find that the class of people to be notified in a situation differs according to these definitions.

California law and some state laws modeled on California law treat encryption differently from the federal Guidance. While encryption under the California law carries a blanket exemption, the federal Guidance does not.

Notification Triggers and Timing

Inconsistencies also exist between state law and the federal Guidance regarding notification timing and triggers. For example, the Guidance defines the standard for providing notice as follows:

“When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution

³ California Civil Code, Section 1798.82.

⁴ “Guidance.” p. 15751.

determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible.”⁵

Contrary to this approach taken in the federal Guidance, California’s law and some other state laws require notification to affected individuals without regard to the likelihood of misuse of the information.

For example, California’s law defines the notification trigger in the following manner:

“Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”⁶

In Congressional testimony, both the Federal Trade Commission (FTC) and the Federal Deposit Insurance Corporation (FDIC) have expressed concern that widespread notification as required by the California and other state laws could be counterproductive. The Federal Trade Commission expressed concern that customers may get so many notices that they will ignore them, while the Federal Deposit Insurance Corporation stressed the need to strike a balance and make sure that customers would not ultimately feel that notices were meaningless.⁷

These differences between state law and federal Guidance regarding when customer notice should be sent create uncertainty for customers and financial institutions. If an institution adopts a more conservative response to security breaches out of an abundance of caution, it may send customers notice even when notice is not required or warranted. Such unwarranted notification could ultimately result in the counterproductive customer response to notices that the FTC and FDIC have warned of.

With regard to notification, the Guidance provides a risk-based threshold. The standard for notification is based upon an institution’s belief that a security breach of sensitive customer information “could result in substantial harm or inconvenience to any customer.”⁸ This risk-sensitive approach to the actual threat of harm helps ensure that notification is limited to customers who may be at risk.

Both the federal Guidance and some state laws require notification within a specified time. These timing requirements vary. The Guidance requires financial institutions to notify affected customers as soon as possible after an investigation determines that misuse has occurred or is reasonably likely to occur. California law requires notification “in the most expedient time possible and without unreasonable delay.” Florida’s law requires that notice shall be made without unreasonable delay, and not later than 45 days after determination of a breach. These standards may not always conflict, but it is possible that financial institutions face difficulty reconciling different timing requirements in a given situation.

Both the Guidance and the California law allow delayed notification when law enforcement is pursuing a criminal investigation. When and how an institution may notify customers following a law enforcement-assisting delay may vary between the federal regulations and some state laws. Even a mandated delay may increase reputational risks if the details of a breach investigation are leaked to the media before an institution is able to notify customers.

⁵ Ibid. p. 15752.

⁶ California Civil Code, Section 1798.82.

⁷ “Enhancing Data Security: the Regulators’ Perspective,” Hearing before the Subcommittee on Financial Institutions and Consumer Credit of the Committee on Financial Services, U.S. house of Representatives, May 18, 2005. .

⁸ “Guidance.” p. 15752.

Notification Format and Contents

The federal Guidance provides a standard that suggests “clear and conspicuous” notification, but does not prescribe the medium or format. California’s law also set a precedent for the manner in which institutions must notify those individuals potentially affected by a security breach. Notice may be provided by one of the following methods:

“(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds \$500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media.”⁹

Unlike California law, the Guidance also provides some suggestions for the contents of a breach notification. The differences between these standards may cause some confusion for institutions.

⁹ California Civil Code, Section 1798.82.

ELEMENTS OF A CUSTOMER RESPONSE PROGRAM

The federal Guidance requires that each financial institution regulated by a federal banking agency have a risk-based customer response program as a component of the institution's overall information security program. This section reviews six potential elements of a customer response program:

- Developing an incident response team;
- Assessing the nature and scope of an incident;¹⁰
- Taking steps to contain and control the incident;¹¹
- Notifying the institution's primary federal regulator;¹²
- Working with law enforcement;¹³ and
- Notifying customers¹⁴ and providing assistance

Developing an Incident Response Team

A financial institution's incident response team should establish the procedures to follow and outline institutional responsibilities when responding to a possible instance of unauthorized access to sensitive customer information. An effective incident response team is an enterprise-wide effort that includes all affected lines of business.

Institutions also should be mindful of regulatory requirements regarding incident response teams. The Federal Financial Institutions Examination Council's Information Security Work Program Tier II examination guidelines require that examiners evaluate a financial institution to determine whether an incident response team:

- Contains appropriate membership;
- Is available at all times;
- Has appropriate training to investigate and report findings;
- Has access to back-up data and systems, an inventory of all approved hardware and software, and monitored access to systems (as appropriate), and;
- Has appropriate authority and timely access to decision makers for actions that require higher approvals.¹⁵

¹⁰ The Guidance identifies procedures for "[a]ssessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused" as a required element of a response program. "Guidance." p. 15752.

¹¹ The Guidance identifies procedures for "[t]aking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence" as a required element of a response program. Ibid.

¹² The Guidance identifies procedures for "[n]otifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of *sensitive* customer information, as defined below" as a required element of a response program. Ibid.

¹³ The Guidance identifies procedures "[c]onsistent with the Agencies' Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing" as a required element of a response program. Ibid.

¹⁴ The Guidance identifies procedures for "[n]otifying customers when warranted" as a required element of a response program. Ibid.

¹⁵ FFIEC IT Examination Handbook – July 2006. pp.48-9.

The Federal Deposit Insurance Corporation (FDIC) also has specific examination guidelines for FDIC supervised institutions regarding such teams, instructing examiners to evaluate the effectiveness of incident response practices by considering the following:

- Establishment of appropriate escalation procedures to address varying alerts or incidents;
- Establishment of an incident response team to address incidents;
- Procedures governing actions to be taken based on incident reports received from outsource providers (e.g., Internet service providers, web hosting companies, application processors);
- Procedures for reporting suspected crimes to local authorities and violations of federal law on Suspicious Activity Reports (SARs).¹⁶

An incident response team has many of the same characteristics of other financial institution recovery teams. The incident response group may be closely aligned with the business continuity and disaster recovery teams. Just like other recoveries, the team can vary depending upon the incident's circumstances. Representatives from legal, compliance, risk, communications, privacy, information security and the relevant business units may be among the "first responders" to an incident or may be brought in following an initial assessment.

Assessing the Nature and Scope of an Incident

All institution employees, groups, and support areas should report incidents and allegations of possible unauthorized acquisition of individual customer information to a contact designated by the financial institution. All parties should be encouraged to make such reports as quickly as possible following the discovery or awareness of the incident or allegation to optimize fraud control.

In the event of a breach of customer information, the institution's corporate security or information security department should first conduct a preliminary assessment. Based on this assessment, the incident response team will support relevant departments, and may determine the source of the compromise, the scope of impact, as well as recovery strategies and notification, if any.

Corporate security or information security should, when appropriate, work with the proper authorities to trace and retrieve the source (e.g., laptop, computer file, paper documentation) of the unauthorized access. Once the source is identified, corporate security or information security should determine the scope of the impact. The scope assessment should include the number of customers potentially impacted and the classification of information compromised.

Taking Steps to Contain and Control the Incident

Based on the nature and scope of the incident, an institution may take one or more of the following steps to contain and control the incident and prevent further unauthorized access to or use of customer information: monitoring, freezing, or closing affected customer accounts; or modifying computer access codes or physical access controls.

¹⁶ FDIC FIL-118-2002. (http://www.fdic.gov/news/news/financial/2002/FIL11802a.html#2_1).

Notifying the Institution's Primary Federal Regulator

The federal Guidance and a number of state laws require institutions to notify the institution's primary federal regulator, the appropriate state Attorney General, or other state official. Examples of the different parties that may need to be notified include:

- Hawaii's law requires notification to Hawaii's Office of Consumer Protection of the timing, distribution, and content of notices when notice is provided to more than 1,000 persons at one time.¹⁷
- Louisiana's law requires that written notice detailing the breach of security be provided to the Consumer Protection Section of the Attorney General's office within 10 days of distribution of notices to Louisiana citizens.¹⁸
- Maine's law requires notice to the appropriate state regulators within the Department of Professional and Financial Regulation or, if not regulated by the department, to the Attorney General.¹⁹
- New Jersey's law requires that, prior to notifying the customer, the business must report the breach of security to the Division of the State Police.²⁰
- New York state law requires notification to the State Attorney General, Consumer Protection Board and State Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content, and distribution of notices and the approximate number of affected persons on a prescribed reporting form.²¹
- North Carolina requires notice to the Consumer Protection Division of the state Attorney General's Office if notice is provided to more than 1,000 persons at one time.²²

The federal Guidance requires that an institution's breach response program specify notification of the institution's primary federal regulator as soon as possible, notification of appropriate law enforcement officials, and filing of a Suspicious Activity Report (SAR) when appropriate.

In addition, several states require institutions to advise the Credit Reporting Agencies (CRAs) if a particular incident will require notification of a material number of consumers. For example, Hawaii requires nationwide CRA notification, in writing and without undue delay, when a business provides notice to more than one thousand consumers at a time; some other states exempt from CRA notice requirements those entities that are subject to Title V of the GLBA.

Working with Law Enforcement

The Guidance states that an institution's procedures should be "consistent with the Agencies' Suspicious Activity Report (SAR) regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing."²³

Law enforcement involvement in a breach of customer information may result in requests for customer notification delays so that law enforcement investigations may be conducted. If legal counsel has not been

¹⁷ S.B. 2290 §2(f) (signed into law May 25, 2006, Act 135). To be codified at Haw. Rev. Stat. Tit. 26. Effective January 1, 2007.

¹⁸ Louisiana Administrative Code Title 16, Part III, §701.

¹⁹ Maine Revised Statutes Title 10, Part 3, Chapter 210-B §1348 (5). Effective January 31, 2007.

²⁰ New Jersey Permanent Statutes Title 56:8-163 12(c)(1).

²¹ New York Consolidated Laws GBS Article 39F, §899-aa. 8(a).

²² North Carolina General Statutes § 75-65(f) (2005).

²³ "Guidance." p. 15752.

involved in the earlier stages of the breach response, it may be advisable to involve legal counsel in any decision to contact investigative agencies.

Notifying Customers and Providing Assistance

An institution's customer notification program should be designed to ensure that all employees understand their roles in a potential instance of unauthorized access to sensitive customer information.

Institutions may benefit from customer notification processes that are carefully defined. Institutions may consider having available sample drafts of customer notification letters, sample scripts for telephone inquiries from customers, and using appropriate media across the institution's various delivery channels. Internal communication channels should be readily available. In addition, institutions may consider creating a dedicated customer inquiry line. In some cases, institutions may wish to offer credit monitoring services to some or all of the affected individuals.

The financial services industry's proactive approach to assisting victims of identity theft is best demonstrated in the creation and success of the Identity Theft Assistance Center (ITAC). As of October 2006, ITAC has assisted over ten thousand consumers by walking them through their credit reports, identifying suspicious activity, and notifying the relevant creditors. ITAC also places fraud alerts with the credit bureaus and shares information with the FTC and law enforcement. ITAC is a free service to the customers of its member companies.²⁴

²⁴ See <http://www.identitytheftassistance.org> for more information on ITAC.

THIRD PARTY SERVICE PROVIDER CONSIDERATIONS

Under existing information security requirements, financial institutions are responsible for ensuring that third party service providers take appropriate measures designed to meet the objectives of the guidelines and comply with section 501(b) of GLBA.²⁵ According to the FFIEC, those measures should result from the institution's security processes, and must be included or referenced in the contract between the institution and the third party service provider.²⁶

According to the Guidelines, the institution is responsible for notifying customers, but may authorize or contract with its third party service provider to notify the institution's customers on its behalf. The institution may consider specifying that a third party service provider promptly notify the institution of suspected or actual unauthorized access to sensitive customer information. An institution may also consider addressing which party is responsible for notifying customers.

BITS has issued several guides on third party service provider relationships. Among these are the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships*, the *BITS IT Service Provider Expectations Matrix*, the *BITS Key Considerations for Global Background Screening Practices*, and *Key Contractual Considerations for Developing an Exit Strategy*.²⁷

²⁵ 15 U.S.C. 6801.

²⁶ FFIEC Information Security Examination Handbook – Outsourcing of Technology Services (http://www.ffiec.gov/ffiecinfobase/booklets/outsourcing/Outsourcing_Booklet.pdf).

²⁷ These documents and other BITS work on Outsourcing is accessible at http://bitsinfo.org/p_publications.html#ITSP.

APPENDIX A: SECURITY BREACH CUSTOMER NOTICE POLICY STATEMENT

The following is a policy statement on security breach customer notification that the CEOs of BITS and Roundtable member companies approved initially in March 2005 and updated in March 2006.

SECURITY BREACH CUSTOMER NOTICE POLICY STATEMENT

Legislatures and regulatory agencies have enacted or proposed laws and regulations mandating that financial institutions notify customers in response to security breaches.

The members of BITS and The Financial Services Roundtable believe:

- Financial institutions have a strong track record in protecting customer information and in communicating with customers when security concerns arise.
- Protecting customer information is of paramount concern and our member institutions have taken a proactive approach in this regard. Examples of these efforts include the creation of the Identity Theft Assistance Center (ITAC) as well as guidelines and best practices for reducing fraud, managing third party providers, engaging law enforcement agencies, and communicating with customers.
- Financial institutions should have the flexibility to develop their own risk-based approaches toward dealing with unauthorized access to customer information, whether at their own operations or with a third party service provider, within the current regulations set forth in section 501b of GLBA. For example, financial institutions should be given flexibility in determining a course of action when they “flag” and secure accounts that have been threatened.
- Notifying customers is a complicated and complex process and can, if poorly done, undermine confidence in the financial services industry. Care must be exercised in alerting consumers to steps they can take to protect themselves from ID theft and other forms of fraud while averting needless alarm.
- Efforts by various states and regulatory agencies raise significant implementation problems for financial institutions. In a transient society, notification should occur uniformly regardless of which state the consumer may live in. Moreover, inconsistent application of inconsistent state law inevitably creates a compliance nightmare for institutions with a multistate presence.

The members of BITS and The Financial Services Roundtable further resolve to:

- Urge legislators and regulators to support risk-based approaches for determining when and how to notify customers.
- Urge legislators and regulators to adopt uniform national standards to avoid serious implementation problems and inconsistent applications.
- Urge legislators and regulators to mandate notification only when there is some indication that the breach actually has the potential to cause harm or injury. If harm is demonstrably contained, for example, and no risk really exists, there should not be any reason to notify and scare people.
- Urge legislators and regulators to require companies that discover breaches in security to immediately notify law enforcement authorities, as well as consumer reporting agencies, so that law enforcement authority can get a jump on any existing criminality and Credit Reporting Agencies may be better prepared for the potential volume of consumer inquiries about the impact of any breach on consumer credit history.
- Support measures to impose caps on damages. Any allowable damages should have firm caps and there should be no damages absent a showing of intent or actual harm. Absent negligence, an affirmative defense should be available if the company can demonstrate that it is a victim of fraud.

- Support measures that provide “safe harbors” from lawsuits. Companies should be afforded some form of safe harbor from lawsuits if they have instituted reasonable internal notification procedures.
- Continue to work with service providers, law enforcement agencies, and regulatory agencies to develop efficient and effective means of notifying customers while ensuring that appropriate steps are taken to investigate crimes.
- Continue to respond aggressively to the escalation in identity theft and online fraud through the BITS Fraud Reduction Program and the Identity Theft Assistance Center (ITAC).

The members of BITS and The Financial Services Roundtable are encouraged to:

- Implement tools to prevent additional regulation and legislation by demonstrating effective self-regulation, such as implementing the BITS Voluntary Guidelines for Consumer Confidence in Online Financial Services. Guidelines include establishing a single point of contact for serving customers with fraud, security or identity theft issues and joining the Identity Theft Assistance Center.

APPENDIX B: ABA, BITS AND ROUNDTABLE PROGRAMS, GUIDES AND TOOLS FOR DATA SECURITY, FRAUD REDUCTION, ID THEFT PREVENTION AND ASSISTANCE, AND THIRD PARTY OUTSOURCING

The following is a list and brief description of ABA, BITS and Financial Services Roundtable Programs, Guides and Tools for data security, fraud reduction, ID theft prevention and assistance, and third party outsourcing. These are listed first as ongoing programs or in chronological order based on publication dates. Most publications are publicly available, but a few are not publicly available and only provided to member companies of either the ABA or BITS.

ABA PROGRAMS, GUIDES AND TOOLS

ABA Works on Fraud: Phishing Prevention & Resolution. The ABA distributed a members-only resource, ABA Works on Fraud, Phishing Prevention & Resolution, which is designed to help bank management information system (MIS), compliance, marketing, legal and communications staff raise customer and employee awareness and reduce the risks of phishing. The ABA is also a research partner of the Anti-Phishing Working Group, in a joint effort to help deter identity theft and fraud, working with the APWG and voluntary and commercial groups that offer takedown services to assist ABA members in shutting down fraudulent phishing and spoofing Web sites. See http://www.aba.com/Members+Only/ABAWorks_phish.htm

ABA Peer Group Benchmarking Programs. The following peer group programs are designed to help ABA members benchmark operational efficiencies and fraud detection mechanisms.

Check Fraud and ACH Loss Reporting. This reporting group tracks quarterly check-related losses from forgeries, counterfeits, alterations, kiting, and seven types of return reasons. Also reported are new account losses, identity fraud losses, and ACH losses. Losses are reported by region and scaled by the number of transaction accounts.

Loss Avoidance Reporting. This reporting group tracks loss avoided due to banks' prevention procedures. Loss avoidance is reported at the bank level and by the source of fraud attempts: ATM fraud; debit card fraud; Reg. E claims; check fraud back office, check fraud claims, customer file maintenance, deposit fraud, new account fraud, pre-charge-off collection, teller phone center support, and transactions cancelled at the teller window. The loss avoidance amount is scaled by the number of transaction accounts.

Debit Card Loss Reporting. This reporting group tracks offline debit card losses from compromised cards; cards not received; counterfeit cards; lost or stolen cards; account takeover; duplicate transactions; merchant disputes; misposted, unposted/nonposted or recurring payment transactions. Losses are reported at the bank level and scaled by sales volume and the number of cards.

National Best Practices Discussion Group. This reporting group examines fraud prevention systems and techniques used by the participating banks.

ABA Deposit Account Fraud Survey Report (November 2004). This report concentrates on collecting baseline information on check and electronic payment fraud losses, and the actions taken or planned by banks to reduce these losses. The survey examines the leading threats against deposit accounts, current and projected check fraud losses and other fraud-related topics both by overall industry trends and by bank asset size. See http://www.aba.com/Surveys+and+Statistics/SS_Depositfraud.htm

ABA Identity Theft Communications Kit. This toolkit is designed to help educate customers on identity theft and how they can protect themselves. See http://www.aba.com/Members+Only/Legislative/gr_idtheftkit_home.htm

BITS AND THE FINANCIAL SERVICES ROUNDTABLE PROGRAMS, GUIDES AND TOOLS

Identity Theft Assistance Center (ITAC). ITAC is a cooperative initiative founded by the financial services industry that now welcomes companies in other industries targeted by identity thieves. Since it was established in August 2004, ITAC has helped thousands of consumers restore their financial identities. Part of the ongoing industry focus on combating fraud and identity theft, ITAC is run by the Identity Theft Assistance Corporation, a not-for-profit membership corporation sponsored by The Financial Services Roundtable and BITS. (September 2004-ongoing) See www.identitytheftassistance.org.

Financial Institution Shared Assessment Program. The Shared Assessments Program was created by BITS member institutions in response to member and service provider needs for a more robust and efficient third party service provider assessment process. Through a comprehensive questionnaire, the Standardized Information Gathering (SIG), and objective and consistent assessment process, Agreed Upon Procedures (AUPs), the process creates major efficiencies and cost savings while raising the bar on security in the financial services industry. (January 2006-ongoing). For additional information, see <http://www.bitsinfo.org/FISAP>

Early Warning® Internal Fraud Prevention Service. This service was developed through the BITS Fraud Reduction Steering Committee. The project took more than four years from idea to implementation, largely because of the need to address human resources and legal issues. After resolving these issues and after an extensive request for proposal process, Primary Payments Systems, Inc. (PPS), an affiliate of First Data Corporation, was chosen to develop and manage this new insider fraud prevention service. The Service is now provided through Early Warning Services LLC, a division of PPS that is owned by financial institutions. The Service protects financial institutions from hiring employees who have been fired from other financial institutions for compromising consumer information and/or knowingly committing fraud. The service began on August 1, 2006 and is ongoing. For more information, visit www.early-warning.com/internalfraud/ or contact [Tony Selway](mailto:Tony.Selway@primarypayments.com) at tselway@primarypayments.com.

BITS Phishing Prevention and Investigation Network. 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. 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; and facilitates communication among fraud specialists at financial institutions, service providers and law enforcement agencies.

BITS Remote Deposit Image Capture: The Processes, Risks and Strategies Used to Mitigate Them (September 2006). See <http://www.bitsinfo.org/downloads/Publications%20Page/BITSRDICFINALSept06.pdf>

BITS Authentication Initiative. BITS has convened numerous calls and hosted two forums to discuss regulatory requirements for stronger authentication as outlined in the FFIEC’s “Authentication in an Internet

Banking Environment”. BITS has summarized some of these calls as a members-only reference guides. Members only documents.

BITS Key Considerations for Securing Data in Storage and Transport: Securing Physical Media in Storage, Transport, and for Data Erasure and Destruction (April 2006). See <http://www.bitsinfo.org/downloads/Publications%20Page/bitsdatatrans.pdf>

BITS Fraud Prevention Toolkit: Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation provides information to support the implementation or improvement of a financial institution internal program for education and awareness about abuse of, and exploitation against, the elderly and vulnerable adults (February 2006). See <http://www.bitsinfo.org/downloads/Publications%20Page/bitstoolfeb06.pdf>

BITS Consumer Confidence Toolkit: Data Security and Financial Services (October 2006). See <http://www.bitsinfo.org/downloads/Publications%20Page/BITSConsumerConfidenceToolkitPublicOCTOBER2006FINAL.pdf>

BITS Voluntary Guidelines for Consumer Confidence in Online Financial Services (September 2005). See <http://www.bitsinfo.org/downloads/Publications%20Page/bitsconscon.pdf>

BITS Critical Success Factors for Security Awareness and Training Programs (September 2005). See <http://www.bitsinfo.org/downloads/Publications%20Page/bitssecaware.pdf>

BITS Key Considerations for Global Background Screening Practices (June 2005). See <http://www.bitsinfo.org/downloads/Publications%20Page/bitsbcheck.pdf>

Key Contractual Considerations for Developing an Exit Strategy (May 2005). See <http://www.bitsinfo.org/downloads/Publications%20Page/bitsexitstrategy.pdf>

BITS Guide to Verification, Authentication and Financial Experience Information Technology for Online New Account Openings (January 2005). 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.

BITS Fraud Prevention Strategies for Consumer, Commercial and Mortgage Loan Departments (January 2005). 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 Strategies for Mitigating Fraud Risks Associated with the Check Clearing for the 21st Century Act (October 2004). See <http://www.bitsinfo.org/downloads/Publications%20Page/check21oct04.pdf>

BITS Developing a Key Risk Indicator Program: Guidance for Operational Risk Managers (September 2004). See <http://www.bitsinfo.org/downloads/Publications%20Page/bitskriprog.doc>

BITS Best Practices for Software Patch Management (July 2004). See <http://www.bitsinfo.org/downloads/Publications%20Page/bitssecaware.pdf>

BITS Calculator: Key Risk Measurement Tool for Information Security Operational Risks (June 2004). 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 *Kalculator* 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. See

<http://www.bitsinfo.org/downloads/Publications%20Page/BITS%20Kalculator/bitskalcnarrative.pdf>

BITS Voluntary Guidelines for Collections in the Financial Services Industry

(March 2004). See <http://www.bitsinfo.org/downloads/Publications%20Page/bitscollectionsmar04.pdf>

BITS Software Security Initiative. Beginning in 2003, Members of BITS and The Financial Services Roundtable outlined business requirements for software vendors in light of significant software security costs and risks facing the financial services industry. BITS convened a CEO-level forum to discuss these concerns with leaders of the software industry and government officials. See

<http://www.bitsinfo.org/downloads/Publications%20Page/bitssummittoolkit.pdf> for BITS/FSR CEO Software Security Toolkit (February 2004).

BITS Voluntary Guidelines for Aggregation Services (January 2004). See

<http://www.bitsinfo.org/downloads/Publications%20Page/bitsaggguide2004.pdf>

BITS Framework for Managing Technology Risk for IT Service Provider Relationships (November 2003). See <http://www.bitsinfo.org/downloads/Publications%20Page/bits2003framework.pdf>

BITS Fraud Reduction Guidelines: Strategies for Identity Theft Prevention (July 2003). See

<http://www.bitsinfo.org/downloads/Publications%20Page/bitsfraudguidelinesJULY03.pdf>

Financial Identity Theft: Prevention and Consumer Assistance (June 2003). See

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

BITS Fraud Prevention Strategies for Internet Banking (April 2003). See

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

BITS Mobile Financial Services Recommendations for Business Requirements and Technical Requirements (April 2002). See

<http://www.bitsinfo.org/downloads/Publications%20Page/BITSMob1.pdf>

BITS Evolution of Fraud Prevention Technologies in a Truncation Environment (Members only document).

BITS: A Financial Institution's Guide to Account, People and Transaction Databases (Members only document).

BITS Preventing E-Scams White Paper (Members only document).