MAINE DATA BREACH STUDY
Pursuant to
Resolve 2007, Chapter 152

PREPARED BY THE STAFF OF THE
MAINE BUREAU OF FINANCIAL INSTITUTIONS

November 24, 2008

John Elias Baldacci
Governor

Anne L. Head
Commissioner

Lloyd P. LaFountain III
Superintendent

DATA BREACH STUDY

TABLE OF CONTENTS

INTRODUCTION

PART I: CURRENT LAWS AND REGULATIONS RELATING TO DATA PROTECTION AND RECOVERY

1) Disclosure of data breach 1
   a) Maine's Notice of Risk to Personal Data Act.....1
   b) Federal guidelines.....2
2) Protection of data.....3
   a) Federal guidelines for banks and credit unions 3
   b) Requirements of the Fair Credit Reporting Act.....4
   c) Responsibilities of non-financial institution entities 5
   d) The PCI Standard.....5
3) Recovery from data breach.....6
   a) State and federal laws protecting consumers from fraud loss 6
   b) Compensable damages under common law.....7
   c) Statutory liability for data breach losses: other States.....9
   d) Federal data breach legislation 10

PART II: STUDY FINDINGS

1) Responses by Maine financial institutions to incidents of data breach 11
   a) Introduction.....11
   b) Narrative questions and summary of responses 12
2) Costs Incurred by Maine financial institutions due to incidents of data breach.....18

Conclusion 24

APPENDIX A: Data Security Breach Questions.....25

APPENDIX B: Resolve 30

INTRODUCTION

The Bureau of Financial Institutions (the "Bureau") was required by Resolve 2007, chapter 152, to study the impact of data security breaches on Maine banks and credit unions, including financial institutions' response to data breaches and the actual costs and expenses incurred by financial institutions as a result of such breaches. The focus of the study is on those breaches that were reportable under Maine's new data breach law known as the Notice of Risk to Personal Data Act, 10 M.R.S.A. §1346 ("Maine's Data Breach Law"). As required by the Resolve, the Bureau prepared this study in consultation with the Maine Credit Union League, the Maine Association of Community Banks, the Maine Bankers Association, and the New England Financial Services Association.

Under Maine's Data Breach Law, which was passed by the Legislature in 2005, a security breach is defined as the unauthorized acquisition of an individual's unencrypted computerized data that compromises the security, confidentiality or integrity of the personal information. It requires that Maine residents receive notice when a security breach has occurred. For most entities, notice is required when, after investigation of the loss of personal information, misuse of the personal information has occurred or is reasonably possible to occur.

Various data breach notification laws have also been passed in other states in response to a growing national concern about identity theft in the wake of several large and well publicized data breaches. Over 44 other states have passed legislation with similar notice requirements for data breaches. The purpose of the notice requirement in these laws is to allow consumers the opportunity to take steps to protect themselves from financial harm. Notice encourages consumer vigilance in reviewing credit reports and account statements for unauthorized transactions. If unauthorized transactions are discovered, consumers may take advantage of other consumer protection laws to avoid having to pay for these unauthorized transactions.

Before discussing the impact of data breaches on Maine's financial institutions, Part I of this Report will review the various laws, guidelines and regulations that help prevent identity theft by requiring or encouraging safekeeping of personal information by financial institutions and other businesses. In addition, Part I will touch upon those laws that help individuals avoid liability for unauthorized charges and reclaim their identity. Part II of this Report will present the findings of the Bureau's study.

PART I: CURRENT LAWS AND REGULATIONS RELATING TO DATA PROTECTION AND RECOVERY

1) Disclosure of data breach

a) Maine's Notice of Risk to Personal Data Act

Maine's Data Breach Law requires disclosure to a Maine resident when a person or organization that maintains unencrypted computerized personal information becomes aware of a security breach and determines that misuse of the resident's personal information has occurred or is reasonably possible to occur. The rules are stricter for "information brokers," such as ChoicePoint and Reed Elsevier, the parent of LexisNexis, that collect information for the primary purpose of furnishing personal information to nonaffiliated third parties. Information brokers must provide notice whenever a breach occurs, whether or not harm is likely to occur. Thus, Maine's Data Breach Law has a tiered notice requirement depending upon whether or not the entity responsible for the information is an "information broker." Pursuant to Maine's Data Breach Law, notification requirements apply to all "persons" including colleges, universities and State Government.

Maine's Data Breach Law is typical of many other state laws in defining what type of lost "personal information" requires notification. "Personal information" is defined in 10 M.R.S.A. § 1347(6) to consist of a person's name, or their first initial and last name, in combination with any one or more of the following identifying data element(s): social security number, driver's license number or state identification card number; account number or credit card number or debit card number if circumstances exist whereby the number could be used without additional identifying information. "Personal information" also includes data elements when not used in connection with a name if this information would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the consumer whose information has been compromised. Importantly, Maine's Data Breach Law, like other state laws, does not require notification if the data that are lost, stolen, or accessed by an unauthorized person have been encrypted.

Maine's Data Breach Law requires that notice must be given to residents expediently and without delay, but consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the breach. When notice of breach is required, notification can be provided either in writing or electronically. In the case of very large breaches, Maine's law allows for substitute notice via email, conspicuous posting and statewide media, if: (a) providing normal written notice would cost over $5,000; (b) the number of affected persons exceeds 1,000; or (c) there is insufficient contact information. Notice must also be sent to the Department of Professional and Financial Regulation if the entity is regulated by the Department (*i.e.*, a Maine-chartered bank or credit union). If the entity is not regulated by the Department of Professional and Financial Regulation, notice must be sent to the Office of the Attorney General.

Similarly, the Office of the Attorney General is generally responsible for enforcing Maine's Data Breach Law. However, in cases where entities are regulated by the Department of Professional and Financial Regulation, such as financial institutions, the relevant Bureau within the Department is responsible for enforcement. In either case, if an entity fails to disclose a breach as required by the law, it may be fined up to $500 per violation, and up to $2,500 per day.

In addition to penalties for persons that fail to disclose a data breach, Maine recently passed a criminal law designed to deter and punish those who misuse identifying information like that obtained in a data breach (17-A M.R.S.A §905-A). A person is guilty of the class D crime of "Misuse of Identification" if they knowingly present a credit or debit card that is stolen, forged, canceled or obtained as a result of fraud or deception. Furthermore, law enforcement agencies are now required to make a police report and provide a copy of the police report to the consumer in the event that a consumer has reported the misuse of personal information (Title 10, §1350-B).

b) Federal guidelines

Pursuant to Maine's Data Breach Law, financial institutions that comply with the security breach notification requirements of rules, regulations, procedures or guidelines established pursuant to federal law are deemed to be in compliance with the requirements of Maine's Data Breach Law as long as the law to which the financial institution is subject is at least as protective

as Maine's Data Breach Law. Financial institutions are covered by the federal "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" or, in the case of credit unions, the "Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice" (collectively, the "Federal Guidelines") and are thus exempt from the notification requirements set forth in state law. The Federal Guidelines state that banks and credit unions should develop response programs that specify actions to be taken when they suspect or detect that an unauthorized individual has gained access to customer information systems. The Federal Guidelines formed the basis for Maine's Data Breach law, and are thus substantially similar.

2) Protection of data

a) *Federal guidelines for banks and credit unions*

In addition to the Federal Guidelines mentioned above, the Federal banking regulatory agencies issued two further Guidelines and updated another in 2005, all of which relate generally to the protection of personal information in light of electronic and Internet-based banking.

The "Interagency Guidelines Establishing Information Security Standards" and the "NCUA Guidelines for Safeguarding Member Information" (the "Security Guidelines") were first issued in 2005. The Security Guidelines established standards relating to administrative, technical and physical safeguards to ensure the security, confidentiality, integrity and proper disposal of customer information. The Security Guidelines were issued with a view toward preventing or responding to foreseeable threats to, or unauthorized access or use of, customer information.

In 2005, the Federal regulatory agencies also updated their Guidance entitled, "Authentication in an Electronic Banking Environment" (the "updated Authentication Guidance") originally issued in 2001. Pursuant to the updated Authentication Guidance, the Federal agencies state that "single-factor" authentication is inadequate for high-risk transactions involving access to customer information over the Internet or the movement of funds to other parties. The updated Authentication Guidance further states that financial institutions offering

Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services.

b) Requirements of the Fair Credit Reporting Act

The Fair Credit Reporting Act, later amended by the Fair and Accurate Credit Transaction Act, contains many consumer protection measures related to data collection and consumer reports. One provision requires credit card machines to truncate all credit and debit card numbers on non-manual receipts. The Fair Credit Reporting Act also requires each national credit bureau to provide a free credit report within 15 days of a consumer's request annually. Another new and important provision requires that the federal bank and credit union regulators issue guidelines requiring all financial institutions to actively seek out and prevent identity theft by looking for and responding to "red flags" that indicate potential problems. These federal guidelines require the establishment of an identity theft prevention program within every financial institution that is designed to detect, prevent and mitigate identity theft in connection with covered accounts, including personal debit and credit card accounts.

Financial institutions must have developed an identity theft prevention program that is appropriate to the size and complexity of each institution by November 1, 2008.[1] The elements of the program must include procedures to identify and detect patterns, practices, or activities considered to be red flags that indicate possible identity theft. Once identified, financial institutions may respond accordingly. Relevant red flags include alerts, notifications or other warnings from consumer reporting agencies or fraud detection services. These red flags may include notice of data breaches from credit card processors or third party retailers.

When a bank or credit union discovers a red flag, the guidelines suggest a number of responses. Appropriate responses may include monitoring the account; contacting customers; changing passwords; closing accounts; notifying law enforcement; or determining that no further response is warranted. These suggested responses are consistent with the actions described by

[1] On October 22, 2008, the FTC announced that it would suspend enforcement of the new "Red Flags Rule" until May 1, 2009, to give non-bank creditors and state-chartered financial institutions additional time in which to develop and implement written identity theft prevention programs. However, this announcement does not affect other federal agencies' enforcement of the original November 1, 2008 deadline for institutions subject to their oversight to be in compliance.

Maine's financial institutions, as set forth in Part II of this Report. These actions help prevent identity theft, defined in the guidelines as a fraud committed or attempted by using the identifying information of another person without authority.

c) Responsibilities of other non-financial institution entities

Although far less comprehensive, non-financial institutions are subject to some control over their use and storage of customer data. The Federal Trade Commission (the FTC) has adopted *de facto* national data security standards for non-bank creditors that are covered by the Federal Trade Commission Act. In 2005 and 2006, the FTC announced significant settlements with entities, including ChoicePoint, that have had personal information data under their control breached or compromised (FTC File No. 052-3069). Pursuant to a settlement with the FTC, ChoicePoint agreed to pay a $10 million civil penalty and another $5 million in consumer redress. The settlement also required ChoicePoint to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to submit to third-party audits for 20 years, and to establish and enforce a comprehensive information security program.

The FTC has also settled data breach actions against BJ's Wholesale Club, Inc. (In the Matter of BJ's Wholesale Club, Inc, FTC File No. 42-3160) and Discount Shoe Warehouse (In the matter of DSW Inc., FTC File No. 052-3096). Each of these settlements required these entities to establish and implement a comprehensive information security program and to submit to third party audits for 20 years.

In these cases, the FTC instituted the action, not as a "deceptive practice," but as an "unfair practice." The FTC did not charge these entities with having misstated their standard for data security; rather, the entities were charged because they did not adopt a minimal level of security for personal information data, thus leading to data breaches.

d) The PCI Standard

In addition to the laws that seek to prevent data breach and deter identity theft, the card industry itself has standards designed to prevent breach and deter fraud. These are known as the

Payment Card Industry Security Standard (the "PCI Standard"). The standard originally began as a number of individual programs established separately by each of the major credit card companies. The common goal of these programs was to create an additional level of protection for customers by ensuring that merchants met minimum levels of security when they stored, processed and transmitted cardholder data. Following the creation of the Payment Card Industry Security Standards Council, these credit card companies aligned their individual policies and, on December 15, 2004, released the PCI Standard.

Pursuant to the PCI Standard, an entity processing, storing, or transmitting payment card data must be PCI Standard compliant or risk losing its ability to process credit card payments and being audited and fined. All merchants and service providers who accept, capture, store, transmit or process credit and debit card data are subject to PCI compliance. PCI compliance includes 12 major requirements which emphasize the need for encryption, access controls and firewalls. A single violation of any of the requirements can trigger non-compliant status.

3) Recovery from data breach

a) State and federal laws protecting consumers from fraud loss

When a person's personal information is lost pursuant to a data breach, there are a number of laws that help to protect against identity theft and also permit them to recover any losses they may have suffered. Maine's Act Regarding Identity Theft Deterrence, 10 M.R.S.A. §1312, enables consumers to place a security freeze on their credit report so that an unauthorized third party may not apply for credit in that person's name. The federal Fair Credit Reporting Act also allows a fraud alert to be placed on a person's credit report to alert potential creditors of a problem. In addition, consumer reporting agencies must block reporting of information in a personal credit report file if it is related to identity theft, and furnishers of information are prohibited from "repolluting" an identity theft victim's credit report with erroneous credit information. Both State and federal law permit free copies of credit reports to allow individuals to review their reports for irregularities.

Once fraud has taken place, the Electronic Funds Transfer Act (implemented by federal Regulation E) protects consumers in the event of data breach occurrences. Pursuant to section

205.6(3) of Regulation E, as long as a consumer provides notice to their financial institution within 60 days from the date when the consumer's account statement containing an unauthorized transaction has been sent to the consumer, the consumer will not be liable for any amount of any unauthorized transactions on their account. However, if the consumer fails to give notice within this 60 day period, the consumer may be liable for any transactions occurring after the close of this 60 day period and before the consumer gives notice to the institution.

In the case of an unauthorized use of a credit card, under federal Regulation Z and Maine's Truth-in-Lending law, a consumer's liability is limited to $50 even when they have not notified the card issuer of the unauthorized use of their credit card. When the consumer has provided timely notice, they are not liable for any unauthorized transactions.

b) Compensable damages under common law

Recent cases have shown that, when determining whether or not financial institutions may obtain restitution for losses sustained as a result of third party data breaches, the law is still not settled. In 2006, suits brought by Sovereign Bank and BankNorth, N.A. against BJ's Wholesale Club Inc. were dismissed by a Pennsylvania Federal District Court. Both financial institutions reissued cards following a massive data breach at BJ's and, as a result, incurred significant expenses, including the costs of issuing new cards to replace those that had been compromised by the data breach.

Sovereign Bank and BankNorth claimed damages as a result of their costs incurred because of the third-party data breach, and framed their claims on several causes of action. On the financial institutions' claims for breach of contract against the retailer, the Pennsylvania Federal District Court held that the financial institutions were not intended third-party beneficiaries of the contracts between BJ's and the credit or debit card companies. Accordingly, it determined that the financial institutions could not succeed against BJ's for breach of contract, particularly in light of the fact that the contracts between BJ's and the credit and debit card companies specified that they were not for the benefit of, and not intended to be enforced by, any third party. Thus, the failure of BJ's to protect data was not a violation of any agreement with the banks.

Similarly, the Pennsylvania Federal District Court took a restrictive view of the types of losses that are compensable when the financial institutions' actions are framed in negligence. The Court applied the economic loss rule, adopted in many states, which bars recovery in a negligence claim for economic damages alone. The Court held that the economic loss rule barred the financial institutions' negligence claim because they claimed damages only for economic losses, not for damages to persons or property.

In July 2008, however, the 3rd U.S. Circuit Court of Appeals reversed the lower court's ruling on the issue of whether the financial institutions which issued the cards were third-party intended beneficiaries of the contracts between BJ's and the credit or debit card companies (3d Cir. 07/19/08). Specifically, and without actually deciding that the financial institutions were entitled to damages, the Court held that there was an issue of fact as to whether or not the financial institutions were third-party intended beneficiaries. Accordingly, the lower court's grant of summary judgment on this issue was reversed and the case has been remanded back to the District Court. If allowed to sue as third party beneficiaries, financial institutions may receive some compensation for breach of contract. (The court found that BJ's had breached its contract with VISA, more particularly, VISA's "operating regulations" which include the Cardholder Information Security Program, or CISP, providing for security requirements relating to the protection of cardholder information.)

In summary, the issue of whether or not financial institutions may obtain restitution at common law for losses sustained as a result of a third party data breach is still an open one, pending final determination by the courts.

c) Statutory liability for data breach: other States

Maine's law does not contain any specific provision for private causes of action[2] that may be brought by individuals subject to a breach or by third parties affected by a breach, or damages or remedies to which they may be entitled. Although several states have considered amending their data breach notification laws to include such a provision, only one state, Minnesota, has enacted a law providing for liability for costs incurred by affected third parties, such as financial institutions, as a result of data breaches. Minnesota's law was passed in August 2007, and the section in the law providing liability for costs became effective on August 1, 2008.[3]

Minnesota's law provides that, when a data breach has occurred due to an entity having retained personal information for longer than 48 hours after a transaction has been authorized, a violation under its law, the entity shall reimburse the financial institution that issued any access device affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach. Under Minnesota's law, these costs may include, but are not limited to: (1) the cancellation or reissuance of any access device affected by the breach; (2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts; (3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach; (4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and (5) the notification to cardholders affected by the breach. The financial institution is also entitled to recover costs for damages paid by the financial institution to cardholders injured by the data breach.

In 2007, California's House and Senate passed a similar bill that would have held entities in violation of its provisions liable to all owners and licensees of the information for the

[2] In the Report of the Department of Professional and Financial Regulation to the Joint Standing Committee on Insurance and Financial Services on Public Law 2005, Chapter 379, "An Act to Protect Maine Citizens from Identity Theft," the issue of whether or not to establish a private cause of action for consumers was raised and recommendations were made. The Department recommended the establishment of a private cause of action for actual damages suffered because a party subject to the proposed legislation failed to investigate a breach or failed to make timely notice. The Department, however, did not recommend permitting recovery for a technical violation if no actual damages occurred, and did not recommend recovery of double or treble damages, nor punitive or other exemplary damages.

[3] Minn. Stat. § 325E.64 (2007)

reimbursement of all reasonable and actual costs of providing notice to consumers pursuant to the breach and for the reasonable and actual cost of card replacement as a result of the data breach. However, this bill was vetoed by the Governor. The Governor, in vetoing the bill, claimed that the proposed law would be too onerous to businesses, especially small ones. The Governor also cited the PCI Standard that already established minimum data security standards for storing, processing, and transmitting credit card data, as another reason for vetoing the bill.

Several other state legislatures, including Illinois, Massachusetts, Texas and Connecticut have introduced bills providing for compensation to be paid to financial institutions for costs incurred as a result of a data breach. However, none of these bills has become law.

d) Federal data breach legislation

Because of the different approaches to data breach notification at the state level, there has been a strong push by the private sector for Congress to enact a federal data breach notification law. Numerous data security and data breach notification laws have been introduced in Congress but none has specifically provided for private parties to sue for damages as a result of third party data breaches.

There have been several differences between the House and Senate bills including, by way of example, their approach to preemption of state data breach notification laws, adoption of specific encryption standards, penalties for breach of the law, and what triggers notification requirements.

PART II: STUDY FINDINGS

1) Responses by Maine Financial Institutions to Incidents of Data Breach

a) Introduction

The Bureau surveyed state and federal financial institutions headquartered in Maine about their experiences responding to data breaches.[4] The Bureau received responses from both state and federal-chartered financial institutions, and from banks, thrifts and credit unions. In all, there were 50 credit unions and 25 banks that responded to the survey.

The Bureau's survey contained two parts. The first part was comprised of twelve questions to which financial institutions provided narrative responses. These questions focused on the responses of financial institutions to data breaches. To capture as much relevant information as possible without placing an onerous burden on the industry, the Bureau limited the questions and framed them in a generic fashion.

The responses to these questions were varied in detail and thoroughness. Nevertheless, the summaries of these narratives paint a useful broad brush picture of how Maine's financial institutions have been affected by data breaches and how they have responded to them.

Since January 1, 2007, there have been two major data breaches affecting Maine's financial institutions. These have been the TJX (a corporation that owns TJMaxx, Marshalls, HomeGoods, and other retailers) data breach which became known to financial institutions in January 2007, and the Hannaford Bros. Co. (Hannaford) data breach which became known to financial institutions in March 2008. Although there were occasional instances of other isolated data breaches, the survey results showed that they affected a small number of financial institutions and their affect on those financial institutions and customers was limited. The Bureau, in summarizing the responses, thus organized the data breaches as follows whenever possible: the TJX data breach, the Hannaford data breach, and "other" data breaches.

[4] See Appendix A: Data Security Breach Questions

Furthermore, the Bureau, in consultation with the Maine Credit Union League, the Maine Association of Community Banks, the Maine Bankers Association and the New England Financial Services Association, determined to limit the scope of the survey to those breaches affecting 25 or more Maine resident customers at each financial institution. Thus, not all data breaches have been captured by the survey.

Set forth below are the questions posed by the Bureau and the summaries of the responses to these questions.

b) Narrative questions and summary of responses

1. The Bureau asked each financial institution to identify each breach affecting that financial institution that involved 25 or more Maine customers and that occurred since January 1, 2007. The Bureau asked each financial institution to be as specific as possible in identifying each breach, e.g.*, entity name where the breach occurred (including the name of your financial institution, if applicable), or, if unavailable, the entity type, date or code number, as indicated on any CAMS (Compromised Account Management System) or similar fraud alerts.*

Responses

Financial institutions reported that it was not uncommon for them to receive several alerts for each data breach event. CAMs alerts were the only alert mentioned by name. These are electronics messages sent out by Visa after it has verified that a potential account compromise has occurred. Many of the financial institutions listed all of the CAMs alerts that they received. Although these CAMs alerts did not identify the source of the breach, the Bureau was able to identify and group these CAMs alerts by source, inferring from the proximity of the dates of the CAMs alerts and their code numbers. Because of the publicity surrounding the TJX and Hannaford data breaches, several financial institutions were able to identify the source of the breach without reference to any alert.

The Bureau's survey revealed that most of the responding financial institutions were affected by the TJX and Hannaford data breaches. Almost all reported being affected by the

Hannaford data breach. Only eighteen out of the responding financial institutions reported being affected by other data breaches captured by the survey.

2. The Bureau asked each financial institution to provide the date the breach was reported to regulators under 10 M.R.S.A. Chapter 210-B for each breach that occurred at the financial institution.

Responses

There was only one report of a data breach that occurred at a financial institution since January 1, 2007. Pursuant to 10 M.R.S.A. Chapter 210-B, this financial institution notified the Bureau of this breach shortly after the breach occurred.

3. For each breach that occurred at the financial institution, the Bureau asked the financial institution to describe how and when the breach was first detected within their financial institution.

Responses

In the case of the financial institution at which the breach occurred, the financial institution's risk management team was promptly notified by the employee responsible for the inadvertent breach.

4. For each breach that did not occur at the financial institution, the Bureau asked each financial institution how and when it first learned of the breach.

Responses

The majority of the financial institutions responded that they first learned of each breach through the CAMS alerts that they receive. As mentioned above, a CAMS alert is an email sent out by a card issuer (*i.e.*, Visa) after it has verified that an account compromise potentially has occurred. The CAMS alert notifies financial institutions of the accounts that may have been compromised. One financial institution responded that it first learned of a breach by a local

news report. Several other financial institutions reported that they first learned of data breaches directly from their card or data service processors (*e.g.*, Elan, Metavante and Fair Isaac), and one reported learning of the breach through the Maine Association of Community Banks (MACB). It was not clear in all cases whether the service providers or MACB were responsible for the initial reporting of the breach to these financial institutions.

*5. For each breach that occurred, the Bureau asked each financial institution to describe what personal information was breached, to the extent it is described in any breach notifications, such as CAMS alerts, received by the financial institution (*e.g.*, Track 1 or 2 data).*

Responses

Although the responses to these questions were not uniform, generally, the personal information that was breached with respect to the TJX data breach involved only Track 2 data. The term "Track 2 data" means that the information contained in the magnetic strips of credit and debit cards is less "dense," does not contain alphabetic text and, hence, does not contain the cardholder's name. Track 2 data include: the primary account number, the expiration date, the service code and certain discretionary data. The term "Track 1 data", on the other hand, means that the information contained in the magnetic strips of credit and debit cards is more "dense," does contain alphabetic text and, hence, contains the cardholder's name. Track 1 data include the following: the primary account number, the cardholder's name, the expiration date, the service code, and certain discretionary data. Although not all financial institutions reported the type of information that was breached by data breach occurrence, for those that did, it appears that only Track 2 data were compromised for the TJX and other smaller breaches but that Track 1 and 2 data were compromised for the Hannaford data breach. Some financial institutions made the distinction between Track 2 "full" data whereas others did not. However, this distinction was not explained. Generally, with respect to any small breaches, only Track 2 data were compromised. The only exception to this was an internal breach that included the names of bank customers.

6. For each breach, the Bureau asked each financial institution to identify/specify how many accounts at the financial institution were breached, and how many customers were affected by the breach.

The responses to this question were inconsistent, with some financial institutions reporting numbers of accounts affected, others reporting customers affected, and others reporting cards affected. Others did not specify, providing numbers only, which meant that the Bureau had no way of determining whether the financial institutions were referring to accounts, customers or cards. However, in all three cases, the numbers reported were generally of the same order. Of those financial institutions that reported the number of cards breached, many of the cards (as many as half in one case) were already no longer active and thus did not require deactivation (or "hot carding").

Responses

In general, the number of accounts, customers or cards affected at each financial institution was proportionate to the financial institution's total assets (*i.e.*, the smaller the financial institution's assets, the lower the number of accounts affected). With respect to the TJX breach, the lowest number of accounts affected at an individual financial institution was 26 and the highest number was 5,460. With respect to the Hannaford breach, the lowest number was 95 and the highest number was 11,793. Without exception, every financial institution that was affected by both the TJX breach and the Hannaford breach reported a greater number of accounts affected by the Hannaford breach. See Table 7 below for more details.

7. For each breach, the Bureau asked each financial institution to describe any audit(s) related to the breach that were conducted to determine what accounts were breached.

Responses

For many financial institutions, no audits were conducted. Rather, they decided to re-issue all customers' cards. For those financial institutions that did conduct audits, this process involved compiling card numbers from the CAMS alerts, and determining which of these card numbers were still active. These active cards were then blocked (or "hot carded") and new cards

were re-issued. In a minority of cases, financial institutions provided their customers with the option of having their cards replaced. Only after customers notified the financial institution that they wished to have their card replaced was the old card blocked (or "soft carded"). Otherwise, the decision to replace cards was made unilaterally by the financial institutions. Any reporting of unauthorized or fraudulent activity on accounts was followed up by manual reviews of those accounts to verify whether or not unauthorized or fraudulent activity took place.

8. For each breach, the Bureau asked each financial institution to describe the steps taken by the financial institution in response to the breach.

Responses

The purpose of this question was to capture any relevant activity conducted by financial institutions not covered elsewhere in the survey questions. The responses varied widely and thus it is difficult to summarize them. Some financial institutions either repeated or referred to their answers to other questions. In addition to this information, some financial institutions reported on the communication chains following discovery of a breach, starting with internal notifications to management and employees, followed by notification to customers, providing website "alerts," establishing "hotlines," "hot carding" or "soft carding" cards, reissuing new cards, and monitoring of unauthorized or fraudulent activities.

Prior to determining which customers needed to be notified, financial institutions conducted research to determine which accounts were (a) affected by the breach and (b) still active. This involved cross-checking account lists provided by the CAMS alerts and the financial institutions' own lists of accounts. Once a database of account numbers that (a) had been affected by the data breach and (b) were still active (or not already "hot carded") had been made, risk management teams next determined whether or not to "hot card" all of the affected accounts, "soft card" accounts of those customers wishing their existing accounts closed and new ones opened, or allow continued use of the compromised accounts. Once this was determined, a decision was made regarding how to notify customers. Generally, financial institutions decided to mail notifications to customers, informing them that their accounts would be "hot carded" and

that new cards would be issued together with pin numbers. Through the financial institutions' vendors, a new card and PIN number were produced and sent to customers.

9. For each breach, the Bureaus asked each financial institution to describe if, when and how it notified its customers of the breach.

Responses

As stated above, the majority of financial institutions notified their customers of the data breach by letter, indicating that notification by letter was the most efficient way to communicate the data breach, particularly with respect to the larger data breaches that occurred at TJX and Hannaford. In addition to sending letters, some smaller financial institutions notified their customers by telephone, some financial institutions posted website alerts, and at least one established a dedicated "hotline" for customers who had questions about the data breach.

10. For each breach, the Bureau asked each financial institution how many accounts, if any, were subject to unauthorized or fraudulent transfers and what amount from the financial institution was transferred fraudulently or without authorization.

Responses

Much of the "hard" data relating to this question may be found below in this Report. The majority of financial institutions reported no unauthorized or fraudulent transfers. Of the 71 affected financial institutions, 25 reported unauthorized or fraudulent transfers. In one case, the unauthorized activity involved only one account and, in most cases, fewer than 25 accounts. In another case, by contrast, the number of accounts which may have been subject to fraudulent transfers due to the breach was 265, and the amount subject to unauthorized or fraudulent transactions was reported to have been $75,000.

11. For each breach, the Bureau was asked to describe any media communications (oral, electronic and print) by the financial institution in relation to the breach.

Responses

Only two financial institutions reported any media communications. Two CEO's were interviewed on local news stations.

12. For each breach, the Bureau asked each financial institution to provide other relevant information, if any, in relation to the breach not described above.

Responses

No further relevant information was provided.

2) Costs Incurred by Maine Financial Institutions due to Incidents of Data Breach

As stated above, 75 financial institutions responded to the survey. Of the 75 respondents, 71 reported being affected by a data breach since January 1, 2007 and incurring expenses reported at $2.1 million. The Hannaford breach had the largest impact, affecting the most institutions (71), the highest number of affected account holders (243,599), and had the largest dollar cost ($1.6 million).

TABLE 1 – IMPACT SUMMARY

	TJX	Hannaford	Other	Total
Institutions Affected	52	71	18	71
Accounts Affected	64,825	243,599	8,008	316,432
Cards Reissued	54,737	186,885	4,857	246,479
Estimated Cost	$485,245	$1,595,444	$62,760	$2,143,450

The survey requested data on several categories of expenses, segregated by direct and indirect cost, as well as data on number of accounts affected and estimated hours. Because of the various degrees of completeness and inconsistencies in reporting the data, the aggregate data is imperfect. Further, detailed comparisons between the TJX breach and the Hannaford breach are limited, mostly because more and better records were generally maintained on the Hannaford breach based on the experience gained from the earlier TJX breach. Nevertheless, despite its weaknesses the aggregate data are considered representative of costs to Maine financial institutions in response to the subject data breaches.

As seen in Table 1, there is a fairly significant variance between the number of accounts affected and the number of cards reissued. The difference is attributable to two primary factors: (1) each account reported as affected in a CAMs alert is not an active account – the account may have been previously closed or is inactive; and (2) every institution did not automatically reissue all affected cards – in the TJX breach, two institutions reissued only at the customer's request and, in the Hannaford breach, four institutions reissued only at the customer's request.

The Survey identified 13 expense categories, but only three were utilized by a majority of the respondents and more than 95% of the expenses fell into four categories (net fraud losses being the fourth). (Table 2)

TABLE 2 – EXPENSE SUMMARY

	TJX		Hannaford		Other		Total	
	$	**%**	**$**	**%**	**$**	**%**	**$**	**%**
Investigation	71.6	14.8	184.9	11.6	13.4	21.3	269.9	12.6
Communication	72.6	15.0	218.6	13.7	13.2	21.1	304.5	14.2
Reissuance	285.1	58.8	859.5	53.9	19.5	31.1	1,164.2	54.3
Net Fraud	36.2	7.5	299.5	18.8	0.4	0.6	336.1	15.7
Other	19.6	4.0	32.9	2.1	16.2	25.9	68.8	3.2
TOTAL	485.2	100.0	1,595.4	100.0	62.8	100.0	2,143.5	100.0

$ in thousands.

For the TJX breach, 32 of the 52 affected institutions reported an Investigation Expense (Table 3), ranging from a low of $62 to a high of $21,000. The five largest accounted for 54% of total Investigation Expense. For the Hannaford breach, 47 of the 71 affected institutions reported an Investigation Expense, ranging from a low of $100 to a high of $29,983.

TABLE 3 – INVESTIGATION EXPENSE

	TJX	Hannaford
# Affected	52	71
# Report	32	47
Highest	$21,000	$29,983
Lowest	$62	$100
Highest Individual	29.3%	16.2%
Top 5	53.6%	46.4%

For the TJX breach, 42 of the 52 affected institutions reported a Communication Expense (Table 4), ranging from a low of $24 to a high of $23,895. For the Hannaford breach, 62 of the

71 affected institutions reported a Communication Expense, ranging from a low of $24 to a high of $27,809.

TABLE 4 – COMMUNICATION EXPENSE

	TJX	Hannaford
# Affected	52	71
# Report	42	62
Highest	$23,895	$27,809
Lowest	$24	$24
Highest Individual	16.2%	12.7%
Top 5	46.4%	38.7%

For the TJX breach, 49 of the 52 affected institutions reported a Reissuance Expense (Table 5), ranging from a low of $60 to a high of $32,146. For the Hannaford breach, 70 of the 71 affected institutions reported a Reissuance Expense, ranging from a low of $250 to a high of $58,278.

TABLE 5 – REISSUANCE EXPENSE

	TJX	Hannaford
# Affected	52	71
# Report	49	70
Highest	$32,146	$58,278
Lowest	$60	$250
Highest Individual	11.3%	6.8%
Top 5	42.9%	24.7%

For the TJX breach, gross fraud losses of $44,898 were reported by six institutions with one institution reporting a fraud recovery of $8,652. For the Hannaford breach, gross fraud losses of $318,213 were reported by 22 institutions with three institutions reporting fraud recoveries of $18,698. The Hannaford fraud losses occurred in more than 712 accounts (five of the 22 institutions that suffered a fraud loss did not report the number of accounts). Additionally, several respondents that did not report any fraud losses stated that fraud losses could not be tied to a specific event.

The non-fraud expenses were more concentrated in a few institutions in the TJX breach than in the Hannaford breach as five institutions accounted for 39% of total expenses (excluding fraud) in the former vs. 20% in the Hannaford breach.

TABLE 6 – NON-FRAUD EXPENSE CONCENTRATION

	TJX	**Hannaford**
Top 1	10.2%	5.0%
Top 5	39.1%	20.2%

The non-fraud expenses were also reviewed in relation to total assets and number of cards reissued by each of the responding institutions. As seen in Table 7 below, the total non-fraud expense is in all instances very proportionate to the cards reissued, for both the TJX breach and the Hannaford breach. For example, in response to the TJX breach nine institutions each reissued between 500 and 999 cards, which in the aggregate represented 11.3% of the total cards reissued and the total non-fraud cost to those nine institutions was 11.0% of the total non-fraud cost for the TJX breach.

TABLE 7 – DISTRIBUTION BY CARDS REISSUED

	TJX					**Hannaford**			
Cards Reissued	**# FI**	**% Cards**	**% Exp**	**% Fraud**		**# FI**	**% Cards**	**% Exp**	**% Fraud**
0 – 499	21	7.8	10.2	34.0		11	1.3	1.7	0.0
500 – 999	9	11.3	11.0	0.0		7	3.0	4.3	4.0
1,000 – 2,499	16	40.0	43.7	35.1		20	18.5	20.1	26.4
2,500 – 4,999	5	30.7	26.5	30.8		21	38.9	36.0	39.8
5,000 – 7,499	1	10.1	8.6	0.0		9	24.9	26.0	24.7
7,500+	0	0.0	0.0	0.0		3	13.3	11.9	5.0
TOTAL	**52**	**100.0**	**100.0**	**100.0**		**71**	**100.0**	**100.0**	**100.0**

While the correlation between percentage of cards reissued and percentage of non-fraud expenses is not as concentrated based on asset size as based on number of cards reissued, the variance is not considered significant. See Table 8. The 15 institutions with assets between $100 million and $249 million accounted for 32.3% of the cards reissued and 30.2% of the total non-fraud expenses related to the Hannaford breach.

TABLE 8 – DISTRIBUTION BY ASSET SIZE

	TJX					Hannaford			
Total Assets	**# FI**	**% Cards**	**% Exp**	**% Fraud**		**# FI**	**% Cards**	**% Exp**	**% Fraud**
0 – 99	22	22.1	15.8	2.3		38	34.9	31.5	35.4
100 – 249	14	33.1	37.0	1.8		15	32.3	30.2	13.8
250 – 499	5	7.0	4.8	0.0		6	7.6	5.9	3.1
500 – 749	4	5.3	7.2	39.4		4	5.7	9.7	23.3
750 – 999	5	16.9	23.8	56.5		6	13.5	18.8	16.9
1,000+	2	15.5	11.5	0.0		2	5.9	3.9	7.4
TOTAL	**52**	**100.0**	**100.0**	**100.0**		**71**	**100.0**	**100.0**	**100.0**

Assets are in millions of dollars.

Tables 7 and 8 also show that there is no correlation between cards reissued or total assets and net fraud losses in either the TJX breach or the Hannaford breach.

The survey also requested an estimate of the number of hours the institution spent in responding to the breach. Not all institutions that experienced a breach provided an estimated number of hours nor did all institutions provide an estimated number of hours for each expense category recognized. For example, an institution may have reported an investigation expense but not attributed any hours to that action. Nevertheless, most respondents provided some information regarding the estimated number of hours. Table 9 shows the average minutes and the range in minutes per reissued card, based on the number of cards reissued. For the nine institutions that reissued between 500 and 999 cards and that reported their estimated hours related to the TJX breach, the average time per reissued card was 13 minutes, with a low of 4 minutes and a high of 28 minutes.

TABLE 9 – TIME DISTRIBUTION BY CARDS REISSUED

	TJX				Hannaford		
Cards Reissued	**# FI**	**Ave**	**Range**		**# FI**	**Ave**	**Range**
0 – 499	15	25	4 – 206		11	14	4 – 49
500 – 999	9	13	4 – 28		6	25	1 – 73
1,000 – 2,499	14	16	5 – 53		18	9	2 – 25
2,500 – 4,999	3	4	2 – 5		20	7	1 – 21
5,000 – 7,499	1	5	5		8	6	2 – 15
7,500+	0	N/A			2	1	1 – 2
TOTAL	**42**	**12**	**2 - 206**		**65**	**7**	**1 – 73**

Table 10 provides the same data as Table 9, but is based on the asset size of the institutions. For the 34 institutions with assets less than $100 million, the average time per reissued card was 8 minutes, with a low of 1 minute and a high of 49 minutes, in addressing the Hannaford breach. Only three institutions, two for the TJX breach and one for the Hannaford breach, reported spending more than an average of 60 minutes per reissued card; only three other institutions reported spending between 30 minutes and 60 minutes, on average, per reissued card. That most institutions spent less time, per reissued card, on the Hannaford breach than on the TJX breach, is attributed to the timing of the breaches; *i.e.*, the TJX breach occurred first and therefore provided a roadmap for responding to the Hannaford breach.

TABLE 10 – TIME DISTRIBUTION BY ASSET SIZE

	TJX				Hannaford		
Total Assets	**# FI**	**Ave**	**Range**		**# FI**	**Ave**	**Range**
0 – 99	15	14	2 – 36		34	8	1 – 49
100 – 249	12	11	5 – 60		15	6	2 – 21
250 – 499	5	5	4 – 7		6	2	1 – 7
500 – 749	4	20	5 – 206		4	17	2 – 73
750 – 999	5	15	4 – 53		5	6	1 – 15
1,000+	1	5	5		1	8	8
TOTAL	**42**	**12**	**2 - 206**		**65**	**7**	**1 – 73**

Last, while 18 institutions reported a total of 36 data breaches occurring since January 1, 2007, the number of accounts affected was relatively small and the dollar cost comparatively minimal. Further, because of the manner of reporting, generally it was not possible to determine if a breach was common to more than one institution.

Conclusion

There is an ongoing debate as to whether current data breach notification laws are effective in providing consumer protection and whether they should specifically provide for liability in all circumstances. Although it is not the purpose of this Report to advocate a particular position in this debate, the Bureau hopes that the information provided in this Report will be useful to the Legislature in its deliberations.

APPENDIX A: Data Security Breach Questions

Data Security Breach Questions

Introduction

Pursuant to L.D. 2139, the Bureau of Financial Institutions, in consultation with the Maine Credit Union League, the Maine Association of Community Banks, the Maine Bankers Association and the New England Financial Services Association, was mandated to conduct a study of the impact of data security breaches on Maine banks and credit unions since January 1, 2007 that have or should have been reported under Maine's Notice of Risk to Personal Data Act. The Bureau was further mandated to submit its findings to the Insurance and Financial Services Joint Standing Committee by December 1, 2008.

"Data security breach" means the unauthorized acquisition of an individual's computerized data that compromises the security, confidentiality or integrity of personal information of the individual maintained by a person, including banks and credit unions.

"Personal information" means an individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

A. Social security number;
B. Driver's license number or state identification card number;
C. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords;
D. Account passwords or personal identification numbers or other access codes; or
E. Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

Good faith acquisition of personal information by an employee or agent of a person on behalf of the person is not a data security breach if the personal information is not used for or subject to further unauthorized disclosure.

Pursuant to Title 9-B, all submitted surveys will be treated as confidential by the Bureau. Information from the surveys will be aggregated and summarized, and the Bureau's findings will be submitted in a manner so that no individual financial institution will be identified.

Scope

Please provide information relating to data security breaches that have: (a) occurred since January 1, 2007; and (b) affected 25 or more customers at your financial institution who are Maine residents. Include those data security breaches that had an impact on your financial institution, whether or not the breach occurred at your financial institution.

Submission deadline

Complete and submit this survey to the Bureau by no later than August 15th, 2008.

General directions

There are two parts to the survey: Part I requires narrative responses to your institution's process in identifying and responding to breaches and Part II requests costs incurred in responding to the breaches. We understand that exact dollar amounts may not be known for all expenses incurred and therefore the use of estimated costs, if explained, is acceptable. Additional guidance for completing Part II is provided below:

Directions for completing Part II

1. All costs should be based upon information available to your financial institution. If precise figures are not available, please justify any estimated costs.
2. All costs are "per breach." Complete a separate spreadsheet for each breach identified in Part 1, Question 1.
3. Indirect costs are any costs that are not considered direct costs, such as lost productivity. Report only those indirect costs that are incurred as a result of the breach. Do not report indirect costs that would have been incurred in any event (*e.g.*, fraud department).
4. For all indirect costs, provide an accounting/explanation as to how such costs were calculated.
5. All categories of costs are mutually exclusive. Do not include a cost in one category if it has been included in another category.

Completed surveys should be sent to:

Bureau of Financial Institutions
Department of Professional and Financial Regulation
36 State House Station
Augusta, ME 04333-0036

Email: BFI.info@Maine.gov

To send a secure message, go to the following Zix site to set up an account and log in.
https://maine-securemail.net/s/login?b=stateofmaine

If you have any questions, contact Christian Van Dyck at (207) 624-8574.

SURVEY QUESTIONS

Name of Financial Institution:
Contact person:
Telephone number:
Email address:

Part I: General Questions (provide brief narrative responses)

1. Identify each breach affecting your financial institution and involving 25 or more Maine customers that occurred since January 1, 2007. Be as specific as possible, *e.g.*, entity name where the breach occurred (including the name of your financial institution, if applicable), or, if unavailable, the entity type, date or code number, as indicated on any CAMS (Compromised Account Management System) or similar fraud alerts.

2. For each breach that occurred at your financial institution, provide the date the breach was reported to regulators under 10 M.R.S.A. chapter 210-B.

3. For each breach that occurred at your financial institution, describe how and when the breach was first detected within your financial institution.

4. For each breach that did not occur at your financial institution, describe how and when your financial institution first learned of the breach.

5. For each breach, describe what personal information was breached, to the extent it is described in any breach notifications, such as CAMS alerts, received by your financial institution (*e.g.*, Track 1 or 2 data).

6. For each breach, identify/specify how many accounts at your financial institution were breached, and how many customers were affected by the breach.

7. For each breach, describe any audit(s) related to the breach that were conducted to determine what accounts were breached.

8. For each breach, describe the steps taken by your financial institution in response to the breach.

9. For each breach, describe if, when and how you notified your customers of the breach.

10. For each breach, how many accounts, if any, were subject to unauthorized or fraudulent transfers and what amount from your financial institution was transferred fraudulently or without authorization?

11. For each breach, describe any media communications (oral, electronic and print) by your financial institution in relation to the breach.

12. For each breach, provide other relevant information, if any, in relation to the breach that is not described above.

Part II: Costs (Complete the spreadsheet. Leave shaded cells blank.)

Identify breach and date of occurrence:

	Direct	Indirect	Affected Accounts	Estimated Hours
	$	$	#	#
1. Internal Investigation				
(a) Audit/research				
(b)Legal				
(c) Data Processing/IT				
(d) Other				
2. Customer Communications				
(a) initial notification				
(b) subsequent communications♦				
(c) public media♣				
3. Reissuance costs				
(a) credit card reissuance				
(b) debit card reissuance				
(c) other reissuance (*e.g.*, checks)				
4. External Legal				
(a) Investigation/consultation				
(b) Defendant/third party costs				
(c) Plaintiff costs				
5. External Audit				
6. External Consultant				
7. Fraud Losses•				
(a) Insurance Recovery	( )			
8. Judgment♥ in favor	( )			
9. Judgment♥ against				
(a) Insurance Recovery	( )			
10. Settlement paid out				
(a) Insurance Recovery	( )			
11. Settlement received	( )			
12. Free/Discounted Services to customers				
13. Other (Identify)				
TOTAL				

♦ Item 2(b). Includes all forms of internal and external communications, as well as call center costs.
♣ Item 2(c). Includes oral, electronic and print media.
• Item 7. Losses sustained as a result of actual fraudulent or unauthorized transfers from accounts.

♥ Items 8 and 9. Includes any final court order or arbitration award in favor of your financial institution or pursuant to which your financial institution has been ordered to pay any damages and/or costs.

Explanations/Justifications:

Resolve, Directing the Bureau of Financial Institutions To Study Data Security Breaches in the State

Sec. 1 Bureau of Financial Institutions directed to study the effect of security breaches in Maine. Resolved: That the Department of Professional and Financial Regulation, Bureau of Financial Institutions, in consultation with the Maine Credit Union League, the Maine Association of Community Banks, the Maine Bankers Association and the New England Financial Services Association, shall conduct a study of the impact of data security breaches since January 1, 2007 that have or should have been reported to state regulators under the Maine Revised Statutes, Title 10, chapter 210-B on Maine banks and credit unions, including the response of financial institutions to such breaches and the actual costs and expenses incurred as a result of such breaches, to the extent information is available; and be it further

Sec. 2 Reporting date. Resolved: That the Department of Professional and Financial Regulation, Bureau of Financial Institutions shall submit its findings under section 1 to the joint standing committee of the Legislature having jurisdiction over insurance and financial services matters by December 1, 2008.