MAINE DEPARTMENT OF

Professional & Financial Regulation

Report of the Department of Professional & 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"

February 1, 2006

Christine A. Bruenn
Commissioner
Professional & Financial Regulation

William N. Lund
Director
Office of Consumer Credit Regulation

Bureau of Financial Institutions

Bureau of Insurance

Office of Licensing and Registration

Office of Securities

Contents

Appendices

I. Introduction and Background

In 2005, the Maine Legislature was presented with information regarding the growing problem of the loss or theft of computerized data containing consumers' personal information. Lawmakers also became concerned about the rising incidence of identity theft. They learned that more than 250 Maine consumers were among the 145,000 US citizens whose personal data may have been stolen from ChoicePoint, a data collection and sales company, and that information stolen from ChoicePoint was used to commit identity theft affecting consumers in other states. They were made aware that the ChoicePoint breach became public knowledge primarily because of a newly-enacted California law requiring notification of consumers whose computerized personal data had been lost or stolen.

The Legislature also learned that the ChoicePoint incident was not an isolated occurrence. For example, the Privacy Rights Clearinghouse (www.privacyrights.org), a respected nonprofit information source, reports that in 2005 approximately 80 such large-scale data breaches occurred, potentially involving the loss of data from as many as 51 million individual consumer accounts across the United States (*see* "A Chronology of Data Breaches Reported Since the ChoicePoint Incident", updated as of January 9, 2006, attached as Exhibit #1).

Finally, Maine lawmakers were told that more than 20 other states have enacted, or are considering, comprehensive data breach laws. In addition, 15 bills have been introduced in the US Congress to address the issues of data breach, identity theft, and the collection and sales of personal financial information (*see e.g.*, the "Financial Data Protection Act of 2005", sponsored by Rep. LaTourette, and the "Notification of Risk to Personal Data Act", sponsored by Sen. Feinstein).

In response to these concerns, the Maine Legislature adopted a number of consumer privacy measures, including Public Law 2005, Chapter 379, entitled "An Act to Protect Maine Citizens from Identity Theft" (attached as Exhibit #2 to this report). This statute requires that information brokers such as ChoicePoint notify consumers if unauthorized persons acquire personal data that could result in identity theft. The law does not require notification to consumers by other types of businesses (such as banks, merchants, credit reporting agencies, securities broker-dealers or insurance companies) if those businesses experience security breaches that could lead to misuse of consumers' personal data.

Section 2 of the public law requires the Department of Professional & Financial Regulation (hereinafter "Department") to complete a study on businesses' data security and security breach requirements, and to deliver that study, and any suggested legislation, to the Insurance & Financial Services Committee by February 1, 2006. [1]

[1] This report was drafted by William N. Lund, Director of the Office of Consumer Credit Regulation with assistance from Christine A. Bruenn, Commissioner, Department of Professional and Financial Regulation; Lloyd P. LaFountain, III, Superintendent, Bureau of Financial Institutions; John Barr, Attorney, Bureau of Financial Institutions; Alessandro A. Iuppa, Superintendent, Bureau of Insurance; Judith M. Shaw, Deputy Superintendent, Bureau of Insurance; Benjamin Yardley, Staff Attorney, Bureau of Insurance; and Michael J. Colleran, Securities Administrator, Office of Securities.

The law requires the Department to develop the report in consultation with the Attorney General's Office, state financial regulatory agencies, business representatives, companies that store electronic consumer data, and consumer advocates.

The statute establishes specific issues to be addressed:

1) *Current electronic data security plans used by businesses;*
2) *The value, practicality and costs of imposing additional requirements, including notification requirements, on businesses;*
3) *An evaluation of the existing California breach notification law; and*
4) *Whether to establish a private cause of action for consumers injured by a violation of the law.*

The Department held an opportunity for public comment at its Gardiner Annex offices on Tuesday, October 4, 2005. Notice was sent to more than 40 individuals and organizations that had participated in deliberations on PL 2005, c. 379 (*see* Interested Parties List, attached as Exhibit #3). In addition, notice of the meeting was included in the September/October, 2005 issue of *Maine Creditor Update*, the newsletter of the Office of Consumer Credit Regulation that is mailed to nearly 2000 individuals and entities regulated by that agency.

Participants were requested to provide written materials prior to the meeting. They were also given an opportunity to present written and verbal testimony at the meeting, and in addition were given approximately two weeks after the meeting to supply follow-up written materials.

Approximately 15 individuals participated in the October 4 meeting, and the participants represented a wide range of interests: legislators; the banking and credit union industries; the Attorney General's Office; the non-bank lending and consumer credit industries; the insurance industry; state financial services regulators; merchants; the food services industry; and the state's information technology office (*see* Attendance List, attached as Exhibit #4). A summary of verbal comments received at the meeting is attached as Exhibit #5.

Many of the parties submitted written materials prior to, during or after the public comment meeting. A list of those who submitted materials is attached as Exhibit #6; complete copies of comments are available from the Department, upon written request.

II. Analysis of the Questions Posed in PL 2005, c. 379

1. Current electronic data security plans used by businesses

Companies utilize a wide range of electronic data security plans. The scope and breadth of these plans appear to be determined by several major factors, including 1) the level of national and/or state government oversight focused on the industry; 2) the type, amount and sensitivity of the information maintained; and 3) the size and sophistication of the business itself.

The broad categories of businesses that collect, store and utilize consumers' personal information can be delineated as follows:

A. Information brokers. These companies, including such entities as LexisNexis and ChoicePoint, are subject to the security requirements and notification standards found in Maine's PL 2005, c. 379. In addition, they are subject to most or all of the data security and notification laws of approximately 22 other states. Unlike depository institutions and many other types of historically-regulated financial service providers, information brokers operated with relative anonymity until they were thrust into the public spotlight by the converging events of 1) large-scale data breaches in 2004 and 2005; and 2) the State of California's mandatory notification requirement (discussed in greater detail in Subsection 3, page 9). They are not required to be licensed or examined by any state regulator unless they also engage in another business that brings them into the Department of Professional and Financial Regulation's jurisdiction; *e.g.*, ChoicePoint conducts certain credit reporting functions and is registered with the Office of Consumer Credit Regulation as a credit reporting agency, since that state office is responsible for enforcement of Maine's Fair Credit Reporting Act.

B. Banks and credit unions. These depository institutions are subject to the safeguarding privacy provisions of the federal Gramm-Leach-Bliley Act (GLBA). In addition, they maintain some of the most comprehensive data security plans of any business sector, primarily because their state and federal regulators have successfully administered binding "guidance," instructing the institutions on appropriate handling of personal information, and on determining those instances in which notification of consumers is warranted; *see "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice"*, 12 CFR Part 30, Appendix B.

The federal guidance requires depository institutions to ensure that their third party service providers also meet security objectives. Where an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers, it is the responsibility of the institution to notify customers of a breach. Experience in other states demonstrates the importance of clarifying notification responsibilities in any data breach law, in order to avoid disputes between parties as to which party is responsible for the potentially-expensive remediation measures.

C. Insurance companies. The insurance industry in Maine offers a wide range of products, from health and life insurance to property and casualty coverage; it includes international, national and local companies of varying sizes. A variety of sales and claims practices affects applicants and policyholders, and includes such parties as insurers, producers, third-party administrators and other contractors, and adjusters. As of January 2006, over 21,000 such entities and individuals (not including nonresident producers) are actively licensed with the Bureau of Insurance to carry on various aspects of the insurance business in Maine. These parties handle confidential consumer information, such as credit card numbers and health information, to varying degrees. The industry's inherent complexity and size increase the risk of its being involved in a data security breach.

The industry is traditionally regulated at the state level, but federal law, which in some instances preempts state law, greatly affects the industry. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes national standards covering electronic health care transactions. HIPAA's purpose is to protect the confidentiality and security of individually-identifiable health information. The standards generally require a covered entity, such as an insurer, to protect such information. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule adopted pursuant to HIPAA. HIPAA leaves the mitigation steps to the entity's judgment and does not specifically require notification to the affected consumer.

GLBA requires insurance companies, among other financial institutions, to adopt measures to protect the security of customer information and to prevent unauthorized access to or use of such records. GLBA also requires state insurance regulators to establish appropriate standards relating to administrative, technical, and physical safeguards to ensure the security and confidentiality of such information. GLBA does not address data security breaches. The Bureau of Insurance promulgated Rule Chapter 980 in response to GLBA. Chapter 980 requires each regulated insurance entity to "implement a written, comprehensive information security program that includes administrative, technical, and physical safeguards for the protection of customer information." Like HIPAA and GLBA, however, Chapter 980 does not require that an insurance company notify any customer should there be a breach of private customer information.

D. Brokerage firms and investment advisers. Firms that offer and sell securities or provide investment advice range in size from small, local companies to huge, multi-state operations, and they are subject to a stringent system of concurrent regulation at both the federal and state level. Among other requirements, they are subject to the general safeguarding security standards imposed by the federal Gramm-Leach-Bliley Act (GLBA) and the implementing Regulation S-P, adopted by the United States Securities and Exchange Commission. Maine securities law, enforced by the state's Office of Securities, makes compliance with these federal provisions a condition of licensure for these firms. Firms that offer and sell securities or provide investment

advice generally have possession of specific and comprehensive financial information about their clients. As with insurance companies, the securities industry has a complex sales and servicing model increases the risk of data breaches. However, currently applicable federal provisions do not specifically require the firms to provide notification to customers of data breaches.

E. Nonbank lenders, loan brokers, creditors and other consumer financial service providers. Generally operating under state, rather than federal, oversight, these lenders, loan brokers, creditors and other consumer financial service providers are subject to the general safeguarding security standards imposed by GLBA, as well as to individual state's file breach notification requirements in those states that apply such mandates broadly. This industry segment ranges from very large entities (*e.g.*, mortgage companies operating in many states) that could likely absorb the costs of notification, to very small business (*e.g.*, auto dealers, rent-to-own companies), for which notification could prove relatively costly. The Office of Consumer Credit Regulation serves as the primary regulator for the majority of these businesses that operate in Maine.

F. Merchants, restaurants, health care providers, private schools and other professional and retail entities. As in the case of non-bank lenders and creditors, this "professional and retail" category includes a wide range of businesses, from large mega-stores (Wal-Mart) to tiny retailers (neighborhood convenience stores), from local eateries to large chain restaurants, and from hospitals to country doctors. At the public meeting held as part of this study, testimony relative to this large business segment focused on two issues: first, the potentially-burdensome cost involved if a small business were required to determine the extent of a data loss and notify affected consumers; and second, the fact that many small businesses lack resources to stay informed of regulatory responsibilities, while at the same time being involved in highly complex monetary systems (such as the credit card authorization and payment process).

Health care providers and their staffs are generally regulated by HIPAA. As previously discussed in this report, although this federal law contains many substantive requirements for the safeguarding of patient medical information, HIPAA does not specifically require notification of those patients if their personal or financial information is compromised.

Retail merchants are not generally regulated by any financial services agency within the Department of Professional and Financial Regulation. Rather, their activities are governed by the Attorney General's Office pursuant to the provisions of the Unfair Trade Practices Act.

Unlike each of the other types of entities listed in subsections A through E, above, retail creditors and many other members of this "retail and professional" category are not subject to the provisions of the GLBA. That is because most small businesses do not fall into the broad federal definition of "financial institution" found in GLBA and its implementing regulations.

2. The value, practicality and costs of imposing additional requirements, including notification requirements, on businesses.

This issue and its discussion are central to this report, and for that reason it is important to preface this section by setting forth a core conclusion reached by the Department. After considering the pros and cons, after hearing from different industry segments, and after factoring in the legislative sentiment that led to the enactment of PL 2005, c. 379, the Department concludes that under certain circumstances, any and all businesses should be required to notify consumers of an electronic data security breach.

The notice triggering standard that the Department urges the Legislature to apply is best described as the "financial institution standard", because it is the triggering standard that federal regulators have applied to financial institutions under their jurisdiction; namely, that any business that maintains computerized data that includes personal or financial information must give notice of a breach of the security of the system following discovery or notification of the breach to a resident of this state if a reasonable investigation reveals that the resident's personal information has been misused, or if it is reasonably possible that the data will be misused.

The following two factors are important to consider when evaluating this proposal:

1. This "financial institution standard" is the core requirement applied to state-chartered and federally-chartered banks and credit unions, so its imposition should not raise issues of inconsistency or incompatibility with regulatory "guidance" governing those institutions.

2. Imposition of this standard would not prevent bank regulators, or other financial regulators (insurance, securities, consumer credit), from adopting stricter or ancillary requirements (*e.g.*, the duty to adopt reasonable standards to safeguard personal electronic data, or the duty to utilize specific language in the notices to consumers).

Despite the potential cost implications of establishing a single, uniform standard for both large and small, sophisticated and unsophisticated businesses, overwhelming consumer sentiment has developed around this issue during the last 12 to 18 months, and consumers now have an expectation of being notified if their personal information is stolen or lost. The fact that more than 20 different states, including some of the most populated states, have considered or enacted notification requirements means that Maine should act in order to prevent a situation in which its citizens are less protected than the population of much of the rest of the country.

It is important to remain mindful of the value of such notification to affected consumers. Notifying consumers does not "fix" the problem. However, such notification does provide a warning to consumers that they should take preliminary steps (*e.g.*, checking their credit reports for evidence of unauthorized activity; placing fraud alerts on their credit reports; and/or "freezing" access to those credit reports) to reduce the risks associated with undetected identity theft.

Therefore, the Department recommends application of a core notification requirement to all businesses: if a business knows of a breach of data security, and a reasonable investigation

reveals that the data has been misused or that it is reasonably possible that the data will be misused, the business must notify affected consumers of the breach.

Once this core principle or standard is established, then the issue of whether or not to impose appropriate ancillary, supplemental or stricter requirements, can be made dependent on the specific industry involved and upon the judgment of the Legislature or each industry's respective regulator. For example:

A. Information brokers. The Department recommends leaving undisturbed the more protective standard established by the Legislature in PL 2005, c. 379. That law does not permit a great deal of discretion on the part of the information broker concerning the risk posed by a breach: notice to consumers is required upon discovery that an unauthorized person has acquired the data. The Department feels that this standard, which is more protective than the "financial institution standard", is warranted, because of 1) the lack of pre-existing, general regulation at the state or national level with respect to the activities of information brokers; and 2) the absence of specific state or federal regulators to whom oversight of this industry is currently assigned.

B. Banks and credit unions. Federal regulatory guidance has currently imposed near-uniform standards on depository institutions. In summary, those standards are:

    a. Institutions must adopt reasonable standards to safeguard personal electronic data.

    b. Institutions must conduct an investigation if they suspect a file breach.

    c. They must notify their primary regulators of the breach.

    d. If the institution's investigation reveals that misuse of the data has occurred, or that it is reasonably possible that misuse will occur, then consumers must be notified.

    e. Notification must be clear, conspicuous and sufficiently detailed to provide meaningful information to affected consumers.

    As discussed above, the Department recommends that the Legislature specifically require compliance with the core triggering standard (misuse of data or the reasonable possibility of misuse), but then defer to the Bureau of Financial Institutions or federal bank regulators to develop ancillary or supplemental requirements. Thus, state law would establish a base level of parity among all types of businesses, without interfering with the abilities of the institutions' functional regulators to establish more protective or detailed standards.

C. Insurance companies. The Department recommends that insurance companies be subject to the core standard currently applicable to depository financial institutions. As mentioned above, this standard requires notice to consumers following a breach if misuse of electronic data is discovered or if it is reasonably possible. Several reasons support this recommendation. First, the insurance industry handles large amounts of confidential information. Second, insurance companies are forms of "financial institutions" to which it is reasonable to apply this standard. Third, Maine has a

comprehensive system of state insurance laws, administered by a specific state agency. The Bureau of Insurance is in the most appropriate position to evaluate such issues as how best to assign responsibility for responding to data security breaches among the various entities regulated by the Bureau, and the extent to which such parties should establish preventive programs, investigate breaches and notify regulators and policy- or certificate-holders.

D. Brokerage firms and investment advisors. The Department recommends that the "financial institutions" standard also be made applicable to broker-dealers and investment advisers. This proposal reflects the relatively high level of sophistication of the securities industry, even among small firms; the highly sensitive nature of the data held by the industry; and the reasonableness of the standard. As in the cases above, the Department recommends permitting the Securities Administrator to make such detailed, supplemental or ancillary requirements as the Securities Administrator deems appropriate for the industry.

E. Non-bank lenders, loan brokers and creditors. The Department again recommends imposition of the aforementioned core "financial institution" standard to consumer credit and loan companies. Although the non-bank lender, loan broker and creditor industries are not as large or sophisticated as banks, credit unions or insurers, the number and size of these consumer finance businesses have grown dramatically in recent decades. The risks to consumers upon breach are similar, and in the Department's opinion the identical core standard should apply.

G. Merchants, restaurants, health care providers, private schools and other professional and retail entities. This "retail and professional" category is varied and diverse in terms of size, sophistication, and data collection processes. In comments provided to the Department at the public meeting, representatives of merchants, especially small retail merchants, provided compelling evidence concerning the practical difficulties and possible costs associated with being required to develop complex file breach-prevention plans and other comprehensive approaches to the file breach issue. For example, the restaurant industry indicated that it is required to collect certain minimum data to process credit cards, not because it intends to store that information and use it for future marketing or sales, but merely to ensure that the restaurant will be compensated for the meals it provides. Further, retailers testified that many of their establishments are at the mercy of credit card companies and other large-scale payment processors, and that not only is their customer base transitory, but the retailers usually have no reason or justification to collect customer addresses, making subsequent notification extremely difficult.

While mindful of these issues, the Department recommends that businesses in the "retail and professional" category be subject to the same core triggering standard proposed to apply to other businesses addressed in this report. Whether financially sophisticated or not, these retailers, healthcare providers, private schools and professions are now part of a system that collects and stores consumers' personal information. To the extent that such entities maintain such computerized data, the Department recommends that the Legislature require such businesses to conduct a reasonable investigation if they are notified of a breach, and to notify consumers if

they discover that misuse has occurred or if such misuse is reasonably possible. The underlying premise for the Department's recommendation is that the potential level of harm that occurs to a consumer following a file breach is not dependent on the source of that breach.

Although the Department recommends imposition of the "core" requirement to merchants (loss of electronic data plus misuse or reasonable possibility of misuse must result in notification to consumers), the Department does not recommend that the Legislature mandate further requirements at this time, such as requiring comprehensive data loss prevention programs, because of the potential expense involved and because many retailers and professionals do not have functional financial regulators. The Department also recommends that the Legislature retain the "substitute notification" option included in current law, for those instances in which individual notice is not practicable or is prohibitively expensive.

3. An evaluation of the existing California breach notification law

California's statute, found in Sections 1798.29, 1798.82, and 1798.84 of its Civil Code (copy attached as Exhibit #7 to this report) pioneered states' efforts in the area of file breach notification. Not only was it the first such law, but it was, and remains, one of the most consumer-protective measures of any state in its requirements and coverage.

Its two primary characteristics can be summarized as follows:

A. **Coverage**: The California statute's requirements encompass "[a]ny agency that owns or licenses computerized data that includes personal information", as well as "[a]ny person or business that conducts business in California, and that owns or licenses computerized data that includes personal data" and "[a]ny person or business that maintains computerized data." In short, any in-state company is covered by the law, as are out-of-state companies that conduct business in the state and agencies of the government.

B. **Triggering event**: The consumer notification requirement is triggered by a breach of the security of an electronic system if unencrypted information is, or is reasonably believed to have been, acquired by an unauthorized person. No harm, actual or potential, is required before the notification mandate arises.

Although federal bank regulators had not issued binding guidance at the time of the enactment of the California law, the state law does arguably accommodate such guidance when it states that an entity that "maintains its own notification procedures as part of an information security policy . . . and is otherwise consistent with the timing requirements" of the law, shall be deemed in compliance with the statute. It is unclear, however, how the law would be administered in the case of an entity that maintained a policy establishing a less protective triggering threshold before notification was required.

Nor does the California statute answer all the possible conflicts that can arise as a result of a major file breach. For example, following a recent massive credit card-related breach, VISA

and MasterCard were involved in litigation against banks in California in a dispute over which entities were legally responsible for conducting the actual consumer notifications. The court agreed with the large credit card issuers, and ruled that the local banks were required to provide the notices to their customers.

Comparing the California statute to Maine's 2005 "information broker" file breach notification law, it becomes clear that one major component of California's law was incorporated into our state's law (the low triggering threshold that requires notification upon a breach and unauthorized acquisition of data, without a specific finding of probable or actual harm), while a second major component (the broad coverage to all companies and to government agencies) was not adopted in Maine. One sub-component (expansion of coverage to businesses other than data brokers) is the subject of this report, while another sub-component (application of the requirement to government agencies) is the subject of a separate report being prepared by Maine's Chief Information Officer.

Comparing California law to the recommendations of this report reveals that the Department is borrowing an important concept from the approach adopted by the California Assembly; namely, imposition of a uniform minimum triggering standard for all types of companies. Consumer advocates could argue that California's standard (acquisition of information by an unauthorized person, with no showing of harm or reasonably possible harm required) is more protective than the "financial institution standard" proposed by this report. While that is true, it is important to remember that federal regulators had not issued their "guidance" prior to the California law's enactment. For Maine to adopt the California standard now would immediately put the state's policy at odds with federal regulators of banks and credit unions, which in turn would raise issues of federal preemption, uneven treatment of state-chartered banks versus their federally-chartered competitors, and other issues. In the Department's opinion it is more important to enact a uniform minimum standard across all businesses and establish the tools to enforce that standard at a state level, than it is to recommend adoption of the strictest standard in the country without a specific showing that the "misuse or reasonably possible misuse" standard will leave consumers materially unprotected.

4. Whether to establish a private cause of action for consumers injured by a violation of the law.

The issue of whether or not to provide a private cause of action for violations of the law, is a controversial topic. Consumer advocates point out that nearly all of Maine's statutes that contain consumer-protection elements (including the Consumer Credit Code, the Fair Debt Collection Practices Act, the Fair Credit Reporting Act, the Unfair Trade Practices Act, the Maine Uniform Securities Act, and the Maine Insurance Code) permit private rights of action under certain circumstances. They argue that the threat of private civil liability would serve as a powerful incentive for companies to comply with provisions of a breach notification law. In addition, the advocates argue that individuals protecting their own rights could effectively supplement the limited resources of the Attorney General's Office. Finally, they point to the precedent established by California law, which provides a private cause of action for damages and injunctive relief (CA Civil Code § 1798.84).

Businesses, on the other hand, are strongly opposed to establishment of a private cause of action. They fear that a technical violation of strict standards could subject them to class action suits, exemplary damages and attorneys' fees. During the opportunity for public comment held as part of the preparation of this report, they testified that A) businesses, especially small businesses, may have very little sophistication regarding security; B) they are heavily reliant on the expertise of their computer software providers, their seasonal employees and their outsourced service providers (such as credit card banks and processors); and C) private civil liability, therefore, would be difficult to avoid and potentially hugely expensive.

The Department agrees in part with the businesspersons who say that any legislation resulting from this study should not simply provide an opportunity for litigious individuals to exploit technical violations of the law. However, the Department also agrees with the consumer advocates who say that, at least with respect to compliance with the basic elements of the investigation and notice requirement, private civil liability is appropriate.

For these reasons, the Department recommends 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 does not recommend permitting recovery for a technical violation if no actual damages occur, and does not recommend recovery of double or treble damages (as are called for under some states' statutes), nor punitive or other exemplary damages. In addition, if the committee in its consideration of this legislation supplements the bill by including additional, detailed requirements not in the attached draft (such as, for example, requiring that all businesses adopt comprehensive prevention policies and practices, or by requiring certain standards or language in the notices), the Department urges the committee to make violation of those additional standards subject to regulatory correction but not to private causes of action. The Department is of the opinion that violations of technical standards are best handled by the businesses' functional regulators (if the businesses have specific regulators), or by the Attorney General's office (for general retailers or other entities without a functional financial regulator). Regulators may be in the best positions to work with the businesses for which they are responsible, to develop consistent, effective plans and to administratively require corrections as necessary.

III. Recommendations

The Department recommends that the committee approve legislation containing the following elements:

1. The current strict standards for "information brokers" should be retained (notice must follow discovery that personal information has been acquired by an unauthorized person), and a requirement to investigate breaches, as well as a private cause of action for actual damages, should be added to the statute.

2. All other businesses operating in this state should be subject to the core "financial institution" notice triggering standard; namely, notification of consumers is required if a breach occurs and if a reasonable investigation reveals that personal information has been misused, or if there is a reasonable possibility that such information will be misused. These minimum core standards can be supplemented or enhanced by the businesses' primary functional regulators. A limited private cause of action should be established, limiting recovery to actual damages suffered as a result of failure to comply with the duty to investigate a breach, or to notify affected consumers in a timely manner.

As comprehensive as the Department has attempted to make this report and legislative recommendations, it is important to recognize that even if the recommendations are adopted, not all conflicts relating to data security file breach notifications will be resolved. The experience in other states, as well as the complex sales, marketing, servicing and outsourcing business models that are common today, all mean that disputes as to what party bears responsibility for investigating suspected breaches and notifying consumers are certain to arise. However, by placing legal responsibility on the party that "maintains computerized data that includes personal information", the Department feels that the parties can then allocate responsibility among themselves through contractual and other business-to-business agreements. In addition, the attached draft does not attempt to dictate the specific or exact content of the notices to consumers, leaving such details to the judgment and discretion of businesses and their respective regulators. However, in the Department's opinion the attached draft legislation establishes a reasonable minimum framework within which the investigation and notification process can occur.

IV. Proposed Legislation

122nd MAINE LEGISLATURE

SECOND REGULAR SESSION - 2005

Legislative Document **No. ___**

An Act to Amend the Risk to Personal Data Laws

Be it enacted by the People of the State of Maine as follows:

Sec. 1. 10 MRSA sec. 1347, sub-§1 is amended to read:

1. Breach of the security of the system. "Breach of the security of the system" or "security breach" means unauthorized acquisition of an individual's computerized data that compromises the security, confidentiality or integrity of personal information of the individual maintained by ~~an information broker~~ a person. Good faith acquisition of personal information by an employee or agent of ~~an information broker for the purposes of the information broker~~ a person on behalf of the person is not a breach of the security of the system if the personal information is not used for or subject to further unauthorized disclosure.

Sec. 2. 10 MRSA sec. 1347, sub-§4 is amended to read:

4. Notice. "Notice" means:

A. Written notice;

B. Electronic notice, if the notice provide is consistent with the provisions regarding electronic records and signatures set forth in 15 United States Code, Section 7001; or

C. Substitute notice, if the ~~information broker~~ person maintaining personal information demonstrates that the cost of providing notice would exceed $5,000, that the affected class of individuals to be notified exceeds 1,000 or that the ~~information broker~~ person maintaining personal information does not have sufficient contact information to provide written or electronic notice to those individuals. Substitute notice must consist of all of the following:

(1) E-mail notice, if the ~~information broker~~ person has e-mail addresses for the individuals to be notified;

(2) Conspicuous posting of the notice on the ~~information broker~~ person's publicly accessible website, if the ~~information broker~~ person maintains one; and

(3) Notification to major statewide media.

Sec. 3. 10 MRSA sec. 1347, sub-§5 is amended to read:

5. Person. "Person" means an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity. "Person" as used in this chapter may not be construed to require duplicative notice by more than one individual, corporation, trust, estate, cooperative, association or other entity involved in the same transaction. For purposes of this chapter, "person" does not include a government agency. *

**Note: This section may be modified depending on the committee's determinations following presentation of a separate report from the state's Chief Information Officer on the subject of privacy and security of electronic personal information maintained by state government, pursuant to PL2005, c. 379, sec. 3.*

Sec. 4. 10 MRSA sec. 1347, sub-§8 is amended to read:

8. Unauthorized person. "Unauthorized person" means a person who does not have authority or permission of ~~an information broker~~ the person maintaining personal information to access personal information maintained by the ~~information broker~~ person or who obtains access to such information by fraud, misrepresentation, subterfuge or similar deceptive practices.

Sec. 5. 10 MRSA sec. 1348, sub-§1 and 2 is amended to read:

§1348. Security breach notice requirements

1. Notification to residents.

A. Information Broker. If an ~~An~~ information broker that maintains computerized data that includes personal information becomes aware of a breach of security of the system, it must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused, and ~~shall~~ must give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

B. Other Persons. If any other person who maintains computerized data that includes personal information becomes aware of a breach of security of the system, the person must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused, and must give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State if misuse of the personal information has occurred, or if it is reasonably possible that misuse will occur.

C. The notice required under paragraphs A and B must be made as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement pursuant to subsection 3 or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data in the system.

2. Notification to ~~information broker~~ person maintaining personal data. A ~~person~~ third-party entity that maintains, on behalf of ~~an information broker~~ a person, computerized data that includes personal information that the ~~person~~ third-party entity does not own shall notify the ~~information broker~~ person maintaining personal data of a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Sec. 6. 10 MRSA sec. 1348, sub-§§ 4 and 5 is amended to read:

4. Notification to consumer reporting agencies. If ~~an information broker~~ a person discovers a breach of the security of the system that requires notification to more than 1,000 persons at a single time, the ~~information broker~~ person shall also notify, without unreasonable delay, consumer reporting agencies that compile and

maintain files on consumers on a nationwide basis, as defined in 15 United States Code, Section 1681a (p).

5. Notification to state regulators. When notice of a breach of the security of the system is required under subsection 1, the ~~information broker~~ person shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the ~~information broker~~ person is not regulated by the Department, the Attorney General.

Sec. 7. 10 MRSA § 1349, sub-§§ 1 and 2 are amended to read:

§1349. Enforcement; penalties

1. Enforcement. The appropriate state regulators within the Department of Professional and Financial Regulation shall enforce this chapter for any ~~information broker~~ person that is licensed or regulated by those regulators. The Attorney General shall enforce this chapter for all other ~~information broker~~ persons.

2. Civil violation. ~~An information broker~~ A person that violates this chapter commits a civil violation and is subject to one or more of the following:

A. A fine of not more than $500 per violation, up to a maximum of $2,500 for each day the ~~information broker~~ person is in violation of this chapter;

B. Equitable relief; or

C. Enjoinment from further violations of this chapter.

Sec. 8. 10 MRSA § 1350 is enacted as follows:

§1350. Private remedy.

A person injured by any of the following actions taken by a person subject to the provisions of this chapter may bring a civil action and recover actual damages together with costs and reasonable attorney's fees:

1. After becoming aware of a security breach, a person subject to the provisions of this chapter fails to conduct in good faith a reasonable and prompt investigation as required by this chapter; or

2. After becoming aware of a security breach, a person subject to the provisions of this chapter fails to provide the notification as required by this chapter.

Sec. 9. 10 MRSA § 1351 is enacted to read as follows:

§1351. Rulemaking

The appropriate financial services regulators within the Department of Professional and Financial Regulation may adopt reasonable rules for the administration and implementation of this chapter. Rules adopted pursuant to this chapter are routine technical rules as defined in Title 5, chapter 375, subchapter II-A.

SUMMARY

This bill expands to other types of persons and businesses the current requirement that information brokers notify consumers upon a security breach of consumers' personal information. The bill also establishes a private cause of action for certain violations of the obligation to notify consumers.

Appendices

Exhibit #1	A Chronology of Data Breaches Reported Since the ChoicePoint Incident
Exhibit #2	Public Law 2005, Chapter 379, "An Act to Protect Maine Citizens from Identity Theft"
Exhibit #3	Interested parties list for advance notice of opportunity for public comment
Exhibit #4	Attendance list, opportunity for public comment (October 4, 2005)
Exhibit #5	Summaries of verbal public comments received
Exhibit #6	Index of written comments received
Exhibit #7	California's file breach statute; Civil Code sections 1798.29, 1798.82 and 1798.84
Exhibit #8	Title 10 MRSA Chapter 210-B in its entirety, showing proposed amendments

Exhibit #1

A Chronology of Data Breaches Reported Since the ChoicePoint Incident

DATE MADE PUBLIC	COMPANY	TYPE OF BREACH	NUMBER
Feb. 15, 2005	ChoicePoint	Bogus accounts established by ID thieves	145,000
Feb. 25 , 2005	Bank of America	Lost backup tape	1,200,000
Feb. 25, 2005	PayMaxx	Exposed online	25,000
March 8, 2005	DSW/Retail Ventures	Hacking	100,000
March 10, 2005	LexisNexis	Passwords compromised	32,000
March 11, 2005	Univ. of CA, Berkeley	Stolen laptop	98,400
March 11, 2005	Boston College	Hacking	120,000
March 12, 2005	NV Dept. of Motor Vehicle	Stolen computer	8,900
March 20, 2005	Northwestern Univ.	Hacking	21,000
March 20, 2005	Univ. of NV., Las Vegas	Hacking	5,000
March 22, 2005	Calif. State Univ., Chico	Hacking	59,000
March 23, 2005	Univ. of CA, San Francisco	Hacking	7,000
March 28, 2005	Univ. of Chicago Hospital	Dishonest insider	unknown
April ?, 2005	Georgia DMV	Dishonest insider	465,000
April 5, 2005	MCI	Stolen laptop	16,500
April 8, 2005	Eastern National	Hacker	15,000
April 8, 2005	San Jose Med. Group	Stolen computer	185,000
April 11, 2005	Tufts University	Hacking	106,000
April 12, 2005	LexisNexis	Passwords compromised	Additional 280,000
April 14, 2005	Polo Ralph Lauren/HSBC	Hacking	180,000
April 14, 2005	Calif. Fastrack	Dishonest Insider	4,500
April 15, 2005	CA Dept. of Health Services	Stolen laptop	21,600
April 18, 2005	DSW/ Retail Ventures	Hacking	Additional 1,300,000
April 20, 2005	Ameritrade	Lost backup tape	200,000
April 21, 2005	Carnegie Mellon Univ.	Hacking	19,000
April 26, 2005	Mich. State Univ's Wharton Center	Hacking	40,000
April 26, 2005	Christus St. Joseph's Hospital	Stolen computer	19,000
April 28, 2005	Georgia Southern Univ.	Hacking	"tens of thousands"
April 28, 2005	Wachovia, Bank of America, PNC Financial Services Group and Commerce Bancorp	Dishonest insiders	676,000
April 29, 2005	Oklahoma State Univ.	Missing laptop	37,000
May 2, 2005	Time Warner	Lost backup tapes	600,000
May 4, 2005	CO. Health Dept.	Stolen laptop	1,600 (families)
May 5, 2005	Purdue Univ.	Hacking	11,360

DATE MADE PUBLIC	COMPANY	TYPE OF BREACH	NUMBER
May 7, 2005	Dept. of Justice	Stolen laptop	80,000
May 11, 2005	Stanford Univ.	Hacking	9,900
May 12, 2005	Hinsdale Central High School	Hacking	2,400
May 16, 2005	Westborough Bank	Dishonest insider	750
May 18, 2005	Jackson Comm. College, Michigan	Hacking	8,000
May 18, 2005	Univ. of Iowa	Hacking	30,000
May 19, 2005	Valdosta State Univ., GA	Hacking	40,000
May 20, 2005	Purdue Univ.	Hacking	11,000
May 26, 2005	Duke Univ.	Hacking	5,500
May 27, 2005	Cleveland State Univ.	Stolen laptop Update 12/24: CSU found the stolen laptop	[44,420] Not included in total below
May 28, 2005	Merlin Data Services	Bogus acct. set up	9,000
May 30, 2005	Motorola	Computers stolen	unknown
June 6, 2005	CitiFinancial	Lost backup tapes	3,900,000
June 10, 2005	Fed. Deposit Insurance Corp. (FDIC)	Not disclosed	6,000
June 16, 2005	CardSystems	Hacking	40,000,000
June 17, 2005	Kent State Univ.	Stolen laptop	1,400
June 18, 2005	Univ. of Hawaii	Dishonest Insider	150,000
June 22, 2005	Eastman Kodak	Stolen laptop	5,800
June 22, 2005	East Carolina Univ.	Hacking	250
June 25, 2005	Univ. of CT (UCONN)	Hacking	72,000
June 28, 2005	Lucas Cty. Children Services (OH)	Exposed by email	900
June 29, 2005	Bank of America	Stolen laptop	18,000
June 30, 2005	Ohio State Univ. Med. Ctr.	Stolen laptop	15,000
July 1, 2005	Univ. of CA, San Diego	Hacking	3,300
July 6, 2005	City National Bank	Lost backup tapes	unknown
July 7, 2005	Mich. State Univ.	Hacking	27,000
July 19, 2005	Univ. of Southern Calif. (USC)	Hacking	270,000 possibly accessed; "dozens"exposed
July 21, 2005	Univ. of Colorado-Boulder	Hacking	42,000
July 30, 2005	San Diego Co. Employees Retirement Assoc.	Hacking	33,000
July 30, 2005	Calif. State Univ., Dominguez Hills	Hacking	9,613
July 31, 2005	Cal Poly-Pomona	Hacking	31,077
Aug. 2, 2005	Univ. of Colorado	Hacking	36,000
Aug. 9, 2005	Sonoma State Univ.	Hacking	61,709
Aug. 9, 2005	Univ. of Utah	Hacking	100,000
Aug. 10, 2005	Univ. of North Texas	Hacking	39,000
Aug. 17, 2005	Calif. State University, Stanislaus	Hacking	900
Aug. 19, 2005	Univ. of Colorado	Hacking	49,000
Aug. 22, 2005	Air Force	Hacking	33,300

DATE MADE PUBLIC	COMPANY	TYPE OF BREACH	NUMBER
Aug. 27, 2005	Univ. of Florida, Health Sciences Center/ChartOne	Stolen Laptop	3,851
Aug. 30, 2005	J.P. Morgan, Dallas	Stolen Laptop	Unknown
Aug. 30, 2005	Calif. State University, Chancellor's Office	Hacking	154
Sept. 10, 2005	Kent State Univ.	Stolen Computers	100,000
Sept. 15, 2005	Miami Univ.	Exposed Online	21,762
Sept. 16, 2005	ChoicePoint (2nd notice, see 2/15/05 for 145,000)	ID thieves accessed; also misuse of IDs & passwords.	9,903
Sept. 17, 2005	North Fork Bank, NY	Stolen laptop (7/24/05) with mortgage data	9,000
Sept. 19, 2005	Children's Health Council, San Jose CA	Stolen backup tape	5,000 - 6,000
Sept. 22, 2005	City University of New York	Exposed online	350
Sept. 23, 2005	Bank of America	Stolen laptop with info of Visa Buxx users (debit cards)	Not disclosed
Sept. 28, 2005	RBC Dain Rauscher	Illegitimate access to customer data by former employee	100+ customers' records compromised out of 300,000
Sept. 29, 2005	Univ. of Georgia	Hacking	At least 1,600
Oct. 15, 2005	Montclair State Univ.	Exposed online	9,100
Oct. 21, 2005	Wilcox Memorial Hospital, Hawaii	Lost backup tape	130,000
Nov. 1, 2005	Univ. of Tenn. Medical Center	Stolen laptop	3,800
Nov. 4, 2005	Keck School of Medicine, USC	Stolen computer	50,000
Nov. 5, 2005	Safeway, Hawaii	Stolen laptop	1,400 in Hawaii, perhaps more elsewhere
Nov. 8, 2005	ChoicePoint	Bogus accounts established by ID thieves Total affected now reaches 162,000 (See Feb. 15 & Sept. 16)	17,000 more
Nov. 9, 2005	TransUnion	Stolen computer	3,623
Nov. 11, 2005	Georgia Tech Ofc. of Enrollment Services	Stolen computer, Theft 10/16/05	13,000
Nov. 11, 2005	Scottrade Troy Group	Hacking	Unknown
Nov. 19, 2005	Boeing	Stolen laptop with HR data incl. SSNs and bank account info.	161,000
Dec. 1, 2005	Firstrust Bank	Stolen laptop	100,000
Dec. 1, 2005	Univ. of San Diego	Hacking. Faculty, students and employee tax forms containing SSNs	7,800
Dec. 2, 2005	Cornell Univ.	Hacking. Names, addresses, SSNs, bank names and acct. numbers.	900
Dec. 6, 2005	WA Employment Security Dept.	Stolen laptop. Names, SSNs and earnings of former employees.	530
Dec. 12, 2005	Sam's Club/Wal-Mart	Unknown. Exposed credit card data at gas stations.	Unknown
Dec. 16, 2005	La Salle Bank, ABN AMRO Mortgage Group	Backup tape with residential mortgage customers lost in shipment by DHL, containing SSNs and account information. Update 12/20: DHL found the lost tape	[2,000,000] Not included in total below
Dec. 16, 2005	Colorado Tech. Univ.	Email erroneously sent containing names, phone numbers, email addresses, Social	1,200

DATE MADE PUBLIC	COMPANY	TYPE OF BREACH	NUMBER
		Security numbers and class schedules.	
Dec. 20, 2005	Guidance Software, Inc.	Hacking. Customer credit card numbers	3,800
Dec. 22, 2005	Ford Motor Co.	Stolen computer. Names and SSNs of current and former employees.	70,000
Dec. 25, 2005	Iowa State Univ.	Hacking. Credit card information and Social Security numbers.	5,500
Dec. 28, 2005	Marriot International	Lost backup tape. SSNs, credit card data of time-share owners	206,000
Jan. 1, 2006	University of Pittsburgh Medical Center, Squirrel Hill Family Medicine	6 Stolen computers. Names, Social Security numbers, birthdates	700
Jan. 2, 2006	H&R Block	SSNs exposed in 40-digit number string on mailing label	Unknown
Jan. 9, 2006	Atlantis Hotel - Kerzner Int'l	Dishonest insider or hacking. Names, addresses, credit card details, Social Security numbers, driver's license numbers and/or bank account data.	55,000
TOTAL			52,075,632

Exhibit #2

PUBLIC LAWS
First Special Session of the 122nd

CHAPTER 379
H.P. 1180 - L.D. 1671

An Act To Protect Maine Citizens from Identity Theft

Be it enacted by the People of the State of Maine as follows:

Sec. 1. 10 MRSA c. 210-B is enacted to read:

CHAPTER 210-B
NOTICE OF RISK TO PERSONAL DATA

§1346. Short title

This chapter may be known and cited as "the Notice of Risk to Personal Data Act."

§1347. Definitions

As used in this chapter, unless the context otherwise indicates, the following terms have the following meanings.

1. Breach of the security of the system. "Breach of the security of the system" or "security breach" means unauthorized acquisition of an individual's computerized data that compromises the security, confidentiality or integrity of personal information of the individual maintained by an information broker. Good faith acquisition of personal information by an employee or agent of an information broker for the purposes of the information broker is not a breach of the security of the system if the personal information is not used for or subject to further unauthorized disclosure.

2. Encryption. "Encryption" means the disguising of data using generally accepted practices.

3. Information broker. "Information broker" means a person who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated 3rd parties. "Information

broker" does not include a governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes.

4. Notice. "Notice" means:

A. Written notice;
B. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 United States Code, Section 7001; or
C. Substitute notice, if the information broker demonstrates that the cost of providing notice would exceed $5,000, that the affected class of individuals to be notified exceeds 1,000 or that the information broker does not have sufficient contact information to provide written or electronic notice to those individuals. Substitute notice must consist of all of the following:

(1) E-mail notice, if the information broker has e-mail addresses for the individuals to be notified;
(2) Conspicuous posting of the notice on the information broker's publicly accessible website, if the information broker maintains one; and
(3) Notification to major statewide media.

5. Person. "Person" means an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity. "Person" as used in this chapter may not be construed to require duplicative notice by more than one individual, corporation, trust, estate, cooperative, association or other entity involved in the same transaction.

6. Personal information. "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.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

7. System. "System" means a computerized data storage system containing personal information.

8. Unauthorized person. "Unauthorized person" means a person who does not have authority or permission of an information broker to access personal information maintained by the information broker or who obtains access to such information by fraud, misrepresentation, subterfuge or similar deceptive practices.

§1348. Security breach notice requirements

1. Notification to residents. An information broker that maintains computerized data that includes personal information shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice must be made as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement pursuant to subsection 3 or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data in the system.

2. Notification to information broker. A person that maintains, on behalf of an information broker, computerized data that includes personal information that the person does not own shall notify the information broker of a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

3. Delay of notification for law enforcement purposes. The notification required by this section may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation; the notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.

4. Notification to consumer reporting agencies. If an information broker discovers a breach of the security of the system that requires notification to more than 1,000 persons at a single time, the information broker shall also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 United States Code, Section 1681a(p).

5. Notification to state regulators. When notice of a breach of the security of the system is required under subsection 1, the information broker shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the information broker is not regulated by the department, the Attorney General.

§1349. Enforcement; penalties

1. Enforcement. The appropriate state regulators within the Department of Professional and Financial Regulation shall enforce this chapter for any information broker that is licensed or regulated by those regulators. The Attorney General shall enforce this chapter for all other information brokers.

2. Civil violation. An information broker that violates this chapter commits a civil violation and is subject to one or more of the following:

A. A fine of not more than $500 per violation, up to a maximum of $2,500 for each day the information broker is in violation of this chapter;
B. Equitable relief; or
C. Enjoinment from further violations of this chapter.

3. Cumulative effect. The rights and remedies available under this section are cumulative and do not affect or prevent rights and remedies available under federal or state law.

Sec. 2. Data security and security breach study; report. The Department of Professional and Financial Regulation, in conjunction with the Attorney General, other financial regulatory agencies, business representatives, other interested parties that store electronic consumer data and consumer representatives, shall conduct a study regarding data security and security breach requirements. The study must include, but is not limited to, current electronic data security plans used by businesses; the value, practicality and costs of imposing additional requirements, including notification requirements, on businesses; California law governing security breach and notification requirements; and the right to private cause of action for a person injured by a violation of security breach notification law. The Department of Professional and Financial Regulation shall report its findings, including any proposed legislation, to the Joint Standing Committee on Insurance and Financial Services, by February 1, 2006. Following receipt and review of the report required under this section and the report required under section 3, the Joint Standing Committee on Insurance and Financial Services may report out a bill related to the reports to the Second Regular Session of the 122nd Legislature.

Sec. 3. Security of information maintained by State Government; report. No later than February 1, 2006, the Chief Information Officer within the Department of Administrative and Financial Services shall report to the Joint Standing Committee on Insurance and Financial Services regarding the State's current and planned-for policies, strategies and systems to protect the privacy and security of electronic personal information maintained by State Government.

Sec. 4. Effective date. That section of this Act that enacts the Maine Revised Statutes, Title 10, chapter 210-B takes effect January 31, 2006.

See title page for effective date, unless otherwise indicted.

Exhibit #3

2005 Breach Notification Study Interested Party List

FIRST NAME	LAST NAME	TITLE	COMPANY	ADDRESS 1	TELEPHONE
BRUCE C	GERRITY		PRETI FLAHERTY BELIVEAU PACHIOS & HALEY LLC	45 MEMORIAL CIRCLE PO BOX 1058 AUGUSTA ME 04332-1058	623-5300
REP DEBORAH	PELLETIER-SIMPSON		MAINE HOUSE OF REPRESENTATIVES	38 BROADVIEW AVENUE AUBURN ME 04210	777-1379
SEN NANCY	SULLIVAN		MAINE STATE SENATE	20 WESTWOOD DRIVE BIDDEFORD ME 04005	282-5594(H)
SEN BARRY	HOBBINS		MAINE STATE SENATE	22 GLENHAVEN CIRCLE SACO ME 04072	282-7101
REP JOHN	BRAUTIGAM		MAINE HOUSE OF REPRESENTATIVES	1 KNIGHT HILL ROAD FALMOUTH ME 04105	797-7131(H)
REP SEAN	FAIRCLOTH		MAINE HOUSE OF REPRESENTATIVES	PO BOX 1574 BANGOR ME 04401	941-8339(H)
REP MARILYN	CANAVAN		MAINE HOUSE OF REPRESENTATIVES	28 MAY STREET WATERVILLE ME 04901	872-6221
NANCY	KELLEHER		AARP	1685 CONGRESS STREET PORTLAND ME 04102	791-3904
MARK	WALKER	VP & COUNSEL	MAINE BANKERS ASSOCIATION	132 MAIN STREET PO BOX 735 AUGUSTA ME 04332-0745	622-6131
JOE	PIETROSKI JR	PRESIDENT	MAINE BANKERS ASSOCIATION	132 MAIN STREET PO BOX 735 AUGUSTA ME 04332-0745	622-6131
CHRIS	PINKHAM	PRESIDENT	MAINE ASSOCIATION OF COMMUNITY BANKS	489 CONGRESS STREET PORTLAND ME 04101-3430	791-8400
QUINCEY H	HENTZEL	DIRECTOR OF GOVERNMENT AFFAIRS	MAINE CREDIT UNION LEAGUE	2 LEDGEWOOD DRIVE WESTBROOK ME 04092	773-5671 ext. 265
NORM	FERGUSON	EXECUTIVE COMMITTEE	AARP	1685 CONGRESS STREET PORTLAND ME 04102	364-7641
CHRISTINE A	BRUENN	COMMISSIONER	DEPARTMENT OF PROFESSIONAL & FINANCIAL REGULATION	35 STATE HOUSE STATION AUGUSTA ME 04333-0035	624-8510
LLOYD P	LAFOUNTAIN III	SUPERINTENDENT	BUREAU OF FINANCIAL INSTITUTIONS	36 STATE HOUSE STATION AUGUSTA ME 04333-0036	624-8575
COLETTE M	MOONEY	DEPUTY SUPERINTENDENT	BUREAU OF FINANCIAL INSTITUTIONS	36 STATE HOUSE STATION AUGUSTA ME 04333-0036	624-8574
JOHN A	BARR	ATTORNEY	BUREAU OF FINANCIAL INSTITUTIONS	36 STATE HOUSE STATION AUGUSTA ME 04333-0036	624-8561
DAVID	BRAGDON	ASSISTANT TO THE COMMISSIONER	DEPARTMENT OF PROFESSIONAL & FINANCIAL REGULATION	35 STATE HOUSE STATION AUGUSTA ME 04333-0035	624-8545
MICHAEL	COLLERAN	SECURITIES ADMINISTRATOR	OFFICE OF SECURITIES	122 NORTHERN AVENUE GARDINER ME 04345	624-8551
ALESSANDRO	IUPPA	SUPERINTENDENT	BUREAU OF INSURANCE	124 NORTHERN AVE GARDINER ME 04345	624-8401
JUDITH	SHAW	DEPUTY SUPERINTENDENT	BUREAU OF INSURANCE	124 NORTHERN AVE GARDINER ME 04345	624-8403
LINDA	CONTI	ASST ATTORNEY GENERAL	OFFICE OF THE ATTORNEY GENERAL	6 STATE HOUSE STATION AUGUSTA ME 04333-0006	626-8591
STEVEN	ROWE	ATTORNEY GENERAL	OFFICE OF THE ATTORNEY GENERAL	6 STATE HOUSE STATION AUGUSTA ME 04333-0006	626-8599
KRISTINE	OSSENFORT	SENIOR GOVERNMENTAL AFFAIRS SPECIALIST	MAINE CHAMBER OF COMMERCE	7 UNIVERSITY DRIVE AUGUSTA ME 04330	623-4568 EXT 21
WILLIAM	LUND	DIRECTOR	OFFICE OF CONSUMER CREDIT REG	35 STATE HOUSE STATION AUGUSTA ME 04333-0035	624-8527

FIRST NAME	LAST NAME	TITLE	COMPANY	ADDRESS 1	TELEPHONE
MARY	YOUNG	EXAMINER-IN-CHARGE	OFFICE OF CONSUMER CREDIT REG	35 STATE HOUSE STATION AUGUSTA ME 04333-0035	624-8527
CHARLES	SOLTAN		LAW OFFICES OF CHARLES C SOLTAN LLC	45 MEMORIAL CIRCLE AUGUSTA ME 04332-0188	621-6300
JIM	MCGREGOR		MAINE MERCHANTS ASSOCIATION INC	PO BOX 5060 AUGUSTA ME 04332-5060	623-1149
DAVID	BRENERMAN	GOVERNMENT & PUBLIC AFFAIRS	UNUM PROVIDENT	2211 CONGRESS STREET PORTLAND ME 04122	575-4311
JOHN	DELAHANTY		PIERCE ATWOOD LLP	ONE MONUMENT SQUARE PORTLAND ME 04101-1110	791-1100
PATTY	AHO		MAINE OIL DEALERS ASSOCIATION	25 GREENWOOD ROAD PO BOX 249 BRUNSWICK ME 04011-0249	729-5298
JAMIE	PYE		MAINE OIL DEALERS ASSOCIATION	25 GREENWOOD ROAD PO BOX 249 BRUNSWICK ME 04011-0249	729-5298
KATHY	KENEBORUS		MAINE ASSOCIATION OF COMMUNITY BANKS	489 CONGRESS STREET PORTLAND ME 04101-3430	791-8400
RICHARD	GROTTON		MAINE RESTAURANT ASSOCIATION	5 WADE STREET PO BOX 5060 AUGUSTA ME 04332-5060	623-2178
PAM	CAHILL		HOWE & COMPANY	11 COLUMBIA STREET AUGUSTA ME 04330	622-4466
CHRISTOPHER	O'NEIL		DRUMMOND WOODSUM & MACMAHON	245 COMMERCIAL STREET PORTLAND ME 04101-4084	774-0317
JOE	MACKEY		PUBLIC AFFAIRS GROUP	185 STATE STREET AUGUSTA ME 04330-6407	626-3052
ALLAN	MUIR		PIERCE ATWOOD LLP	ONE MONUMENT SQUARE PORTLAND ME 04101-1110	791-1100
DAN	BERNIER		PHILLIPS & BERNIER LLC	179 MAIN STREET SUITE 307 WATERVILLE ME 04901	877-8970
LUCIA	NIXON	LEGAL ANALYST	MAINE STATE LEGISLATURE	OFFICE OF POLICY AND LEGAL ANALYSIS 13 STATE HOUSE STATION AUGUSTA ME 04333-0013	287-1670
TOM	BROWN	EXECUTIVE DIRECTOR	MAINE AUTO DEALERS	180 CIVIC CENTER DRIVE PO BOX 2667 AUGUSTA ME 04338-0013	623-3882
COLLEEN	MCCARTHY REID	LEGAL ANALYST	MAINE STATE LEGISLATURE	POLICY & LEGAL ANALYSIS 13 STATE HOUSE STATION AUGUSTA ME 04333-0013	287-1670
DAVID	CLOUGH		NFIB	PO BOX 796 SOUTH FREEPORT ME 04078-0796	846-5776

Exhibit #4*

PLEASE SIGN IN

SECURITY BREACH NOTIFICATION COMMENT MEETING

Tuesday, October 4, 2005; 10 AM

NAME, ADDRESS AND COMPANY
Robert L. Witham, Jr. Office of Info. Tech. State of Maine
Bruce Gerrity, Esq. Preti Flaherty 45 Memorial Circle Augusta, ME 04330
Representative John Brautigam 1 Knight Hill Road Falmouth, ME 04105
Linda Conti, Assistant Attorney General Office of the Attorney General State House Station 6
Chris Pinkham Maine Assoc. of Community Banks 489 Congress Street Portland, ME 04101
Will Lund Office of Consumer Credit Regulation State of Maine
Mary Young Office of Consumer Credit Regulation State of Maine
Michael Atleson Office of Securities State of Maine
Dan Bernier, Esq. NAIFA – ME (National Association of Insurance and Financial Advisors) & MIAA (Maine Insurance Agents Association)

**Note: This document was typed using information from the sign-in sheet of attendees at the October 4, 2005, comment meeting. A copy of the original is available upon request at 624-8527.*

Exhibit #4*

PLEASE SIGN IN

SECURITY BREACH NOTIFICATION COMMENT MEETING

Tuesday, October 4, 2005; 10 AM

NAME, ADDRESS AND COMPANY
Jim MacGregor Maine Merchants P.O. Box 5060 Augusta, ME 04332
Chalie Soltan, MAIC (Maine Association of Insurance Companies) P.O. Box 188 Augusta, ME 04332-0188
Dick Grotton Maine Restaurant Association P.O. Box 5060 Augusta, ME 04332-5060
Kristine Ossenfort Maine State Chamber 7 University Drive Augusta, ME 04330
Kathy Keneborus Maine Association of Community Banks 489 Congress Street Portland, Maine 04101
Quincy Hentzel Maine CU League 2 Ledgewood Dr. Westbrook, ME 04092

**Note: This document was typed using information from the sign-in sheet of attendees at the October 4, 2005, comment meeting. A copy of the original is available upon request at 624-8527.*

.

Exhibit #5

Summaries of verbal public comments received

Commenter: Linda Conti (Attorney General's office)

Summary: Recommends that the requirement to notify affected consumers be extended to businesses that handle consumers' personal data, and that a low triggering threshold be adopted. Recommend that a private cause of action accrue for instances in which failure to notify consumers results in actual harm.

_____

Commenter: Bruce Gerrity (Maine Auto Dealers Association; American Insurance Association; Property and Casualty Insurance Association of America; New England Financial Services Association

Summary: Recommends a high triggering standard (only after "material" breach), because if consumers receive too many notices, the notices will lose their impact (*i.e*., they will become "white noise"). Recommends looking to the Delaware law for model language. The notification requirement should be extended to loss of data maintained by the State of Maine. Opposes private cause of action, because that will serve as a "haven for lawyers" and an incentive not to investigate suspected leaks.

_____

Commenter: Jim MacGregor (Maine Merchants Association)

Summary: Opposes private cause of action. Recommends application of a single, federal standard. Would narrow the definition of "breach", and require notices only for certain breaches. Urges Department to "keep it simple" for ease of compliance by merchants.

_____

Commenter: Dan Bernier (Maine Insurance Agents Association; National Association of Insurance and Financial Advisors)

Summary: Opposes "one size fits all" approach; recommends different standards for different industries. Hopes that the NAIC will develop a single, uniform standard. Is concerned about which party in the insurance process will be required to send the notice (*e.g*.; the individual agent; the insurance agency; or the underwriter).

_____

Commenter: Chris Pinkham (Maine Association of Community Banks)

Summary: Expressed concern about the definition of "breach". Stated that banks are already tightly regulated, and are in fact the "victims" of identity theft, in that they often end up responsible for reimbursing customers for losses. Hopes that Maine regulators will coordinate Information Technology exams with federal regulators.

_____

Commenter: Charles Sultan (Maine Association of Insurance Companies)

Summary: The law should set a higher standard than just unauthorized access to information before the notification requirement is triggered. Notice requirement should apply only in cases in which a material economic impact results. No need exists to create a private cause of action; existing remedies are sufficient. Offered to research whether HIPAA requires notification upon breach (*note*: the Department subsequently determined that HIPAA does not contain a specific notice requirement following file breach).

_____

Commenter: Dick Grotton (Maine Restaurant Association)

Summary: Feels that the term "identity theft" has been overly broadened, and now is incorrectly viewed as encompassing "unauthorized charges" as well as the true definition of the term, which involves assumption of another's identity I order to apply for credit. Asks why a customer's name appears on the customer's copy of a credit card receipt. Wonders how a restaurant could comply with a notification requirement, since it does not have the addresses of customers who charge meals on credit cards, pointing out that some customers are tourists from foreign countries.

_____

Commenter: Kristine Ossenfort (Maine Chamber of Commerce)

Summary: The law's reference to conducting a study of "businesses" creates a very broad mandate. Many business types may not be aware of this study, including health care providers. The Chamber recognizes the need for some regulation in this area. Expresses concern about the cost and burden of creation of a private cause of action. Stresses consumer education, saying that notices will do no good if consumers do not understand their significance.

_____

Exhibit #6

BREACH NOTIFICATION COMMENTS RECEIVED
Meeting of October 4, 2005 at 10:00 AM

Name and Address	**Date Received**
Daniel J. Bernier, Esq. Phillips & Bernier, LLC 179 Main Street, Suite 307 Waterville, ME 04901 On behalf of the Maine Insurance Agents Association and National Association of Insurance and Financial Advisors-Maine	09/29/05 and supplemental comments received on 10/12/05
Christopher Pinkham, President Maine Association of Community Banks 489 Congress Street Portland, ME 04101-3430	9/30/05
Linda Conti, Assistant Attorney General Office of the Attorney General 6 State House Station Augusta, ME 04333-0006	9/30/05 and supplemental comments received on 10/12/05
David H. Brenerman, Assistant Vice President Government & Public Affairs UNUM Provident 2211 Congress Street Portland, ME 04122	9/30/05
Chantele L. Mack Manager, Government Relations Consumer Data Industry Association – CDIA 1090 Vermont Avenue, NW, Suite 200 Washington, DC 20005	9/30/05
Quincy H. Hentzel Director of Governmental Affairs Maine Credit Union League 2 Ledgeview Drive Westbrook, Maine 04092	9/30/05
Alessandro A. Iuppa, Superintendent Bureau of Insurance 34 State House Station Augusta, ME 04333-0034	10/11/05

Exhibit #7

CALIFORNIA CIVIL CODE

Sections 1798.29, 1798.82, 1798.84
Effective July 1, 2003

1798.29. (a) Any agency 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. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, ‘‘breach of the security of the system’’ means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, ‘‘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:

(1) Social security number.

(2) Driver’s license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

(f) For purposes of this section, ‘‘personal information’’ does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, ‘‘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 agency 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.

(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.82. (a) 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. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, ''breach of the security of the system'' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, ''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:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, ‘‘personal information’’ does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
(g) For purposes of this section, ‘‘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 person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:
(A) E-mail notice when the person or business has an e-mail address for the subject persons.
(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.
(C) Notification to major statewide media.
(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.84. (a) Any customer injured by a violation of this title may institute a civil action to recover damages.
(b) Any business that violates, proposes to violate, or has violated this title may be enjoined.
(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

Exhibit #8

Title 10 MRSA Chapter 210-B: NOTICE OF RISK TO PERSONAL DATA

(in entirety, showing proposed amendments)

§1346. Short title

This chapter may be known and cited as "the Notice of Risk to Personal Data Act."

§1347. Definitions

As used in this chapter, unless the context otherwise indicates, the following terms have the following meanings.

1. Breach of the security of the system. "Breach of the security of the system" or "security breach" means unauthorized acquisition of an individual's computerized data that compromises the security, confidentiality or integrity of personal information of the individual maintained by ~~an information broker~~ a person. Good faith acquisition of personal information by an employee or agent of ~~an information broker for the purposes of the information broker~~ a person on behalf of the person is not a breach of the security of the system if the personal information is not used for or subject to further unauthorized disclosure.

2. Encryption. "Encryption" means the disguising of data using generally accepted practices.

3. Information broker. "Information broker" means a person who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated 3rd parties. "Information broker" does not include a governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes.

4. Notice. "Notice" means:

A. Written notice;

B. Electronic notice, if the notice provide is consistent with the provisions regarding electronic records and signatures set forth in 15 United States Code, Section 7001; or

C. Substitute notice, if the ~~information broker~~ person maintaining personal information demonstrates that the cost of providing notice would exceed $5,000, that the affected class of individuals to be notified exceeds 1,000 or that the ~~information broker~~ person maintaining personal information does not have sufficient contact information to provide written or electronic notice to those individuals. Substitute notice must consist of all of the following:

(1) E-mail notice, if the ~~information broker~~ person has e-mail addresses for the individuals to be notified;

(2) Conspicuous posting of the notice on the ~~information broker~~ person's publicly accessible website, if the ~~information broker~~ person maintains one; and

(3) Notification to major statewide media.

5. Person. "Person" means an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity. "Person" as used in this chapter may not be construed to require duplicative notice by more than one individual, corporation, trust, estate, cooperative, association or other entity involved in the same transaction. For purposes of this chapter, "person" does not include a government agency.*

** Note: This section may be modified depending on the committee's determinations following presentation of a separate report from the state's Chief Information Officer on the subject of privacy and security of electronic personal information maintained by state government, pursuant to PL2005, c. 379, sec. 3.*

6. Personal information. "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.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

7. System. "System" means a computerized data storage system containing personal information.

8. Unauthorized person. "Unauthorized person" means a person who does not have authority or permission of ~~an information broker~~ the person maintaining personal information to access personal information maintained by the ~~information broker~~ person or who obtains access to such information by fraud, misrepresentation, subterfuge or similar deceptive practices.

§1348. Security breach notice requirements

1. Notification to residents.

A. Information Broker. If an ~~An~~ information broker that maintains computerized data that includes personal information becomes aware of a breach of security of the system, it must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused, and ~~shall~~ must give notice of a breach of the

security of the system following discovery or notification of the security breach to a resident of this State whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

B. Other Persons. If any other person who maintains computerized data that includes personal information becomes aware of a breach of security of the system, the person must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused, and must give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State if misuse of the personal information has occurred, or if it is reasonably possible that misuse will occur.

C. The notice required under paragraphs A and B must be made as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement pursuant to subsection 3 or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data in the system.

2. Notification to ~~information broker~~ person maintaining personal data. A ~~person~~ third-party entity that maintains, on behalf of ~~an information broker~~ a person, computerized data that includes personal information that the ~~person~~ third-party entity does not own shall notify the ~~information broker~~ person maintaining personal data of a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

3. Delay of notification for law enforcement purposes. The notification required by this section may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation; the notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.

4. Notification to consumer reporting agencies. If ~~an information broker~~ a person discovers a breach of the security of the system that requires notification to more than 1,000 persons at a single time, the ~~information broker~~ person shall also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 United States Code, Section 1681a (p).

5. Notification to state regulators. When notice of a breach of the security of the system is required under subsection 1, the ~~information broker~~ person shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the ~~information broker~~ person is not regulated by the department, the Attorney General.

§1349. Enforcement; penalties

1. Enforcement. The appropriate state regulators within the Department of Professional and Financial Regulation shall enforce this chapter for any ~~information broker~~ person that is licensed or regulated by those regulators. The Attorney General shall enforce this chapter for all other ~~information broker~~ persons.

2. Civil violation. ~~An information broker~~ A person that violates this chapter commits a civil violation and is subject to one or more of the following:

A. A fine of not more than $500 per violation, up to a maximum of $2,500 for each day the ~~information broker~~ person is in violation of this chapter;

B. Equitable relief; or

C. Enjoinment from further violations of this chapter.

3. Cumulative effect. The rights and remedies available under this section are cumulative and do not affect or prevent rights and remedies available under federal or state law.

§1350. Private remedy.

A person injured by any of the following actions taken by a person subject to the provisions of this chapter may bring a civil action and recover actual damages together with costs and reasonable attorney's fees:

1. After becoming aware of a security breach, a person subject to the provisions of this chapter fails to conduct in good faith a reasonable and prompt investigation as required by this chapter; or

2. After becoming aware of a security breach, a person subject to the provisions of this chapter fails to provide the notification as required by this chapter.

§1351. Rulemaking

The appropriate financial services regulators within the Department of Professional and Financial Regulation may adopt reasonable rules for the administration and implementation of this chapter. Rules adopted pursuant to this chapter are routine technical rules as defined in Title 5, chapter 375, subchapter II-A.