JONES DAY®

JANUARY 2007

AN OVERVIEW OF U.S. SECURITY BREACH STATUTES

AN OVERVIEW OF U.S. SECURITY BREACH STATUTES

Jeffrey M. Rawitz and Ryan E. Brown[1]

This Jones Day *White Paper* summarizes what is generally entailed in the security breach statutes of specific states in the U.S. and provides a quick reference for state-specific qualifications and nuances. It is not intended, however, to be a substitute for reference to the laws of a particular state. Immediately following this overview are the relevant sections of each state's respective statute.

There are presently 33 states with statutes requiring the public disclosure of a security breach when the unencrypted personal information of an individual may have been compromised. Several federal bills are currently being considered, but as of yet, there is no federal law addressing the topic.

GENERAL REQUIREMENTS OF SECURITY BREACH LAWS

Application. Although each state varies, the laws typically apply to any person or entity doing business in a particular state where the person or entity owns, licenses, or maintains computerized data that includes personal information.

Security Breach. A "breach of the security of the system" is generally defined by the statutes as being the unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.

Personal Information. "Personal information" is generally defined as 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 state identification card number; (3) account number or 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. For data element (3), some of the states require only a password, unaccompanied by the account number, or an account number that does not require a password. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Notification Obligations. A person or entity that has been affected by a security breach generally must make the disclosure in the most expedient time possible and without unreasonable delay. Notice may be delayed when a law enforcement agency determines that the notification will impede a criminal investigation. Notification to affected consumers may be provided in writing or electronically if the electronic notice complies with the federal Electronic Signature Act. If a company can demonstrate that the cost of providing notice would exceed $250,000, that the affected class of subject persons to be notified exceeds 500,000, or that the company does not have sufficient contact information, then the company can rely on "substitute notice" to comply with its notification requirements. Substitute notice involves all of the following three actions: (1) e-mail notice when the company has e-mail addresses for the subject persons; (2) conspicuous posting of the notice on the company's web page, if it maintains one; and (3) notification in a major statewide medium.

State-Specific Qualifications and Nuances

This section highlights notable state-specific departures from the general requirements discussed above.

---

1 Jeffrey M. Rawitz (1.213.243.2537; jrawitz@jonesday.com) is a partner in the Los Angeles Office.
Ryan E. Brown (1.213.243.2214; rebrown@jonesday.com) is an associate in the Los Angeles Office.

Arizona

1) Allows for telephonic notice.
2) "Substitute notice" is allowed where the cost of providing notice will exceed $50,000 or the affected class of individuals to be notified exceeds 100,000.
3) Notice can also be effected where a database owner maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are consistent with the applicable statute.
4) Notice is not required if the unauthorized access is not reasonably likely to cause substantial economic loss to an individual.

Arkansas

1) Adds "medical information" to the list of "data elements" in the definition of "personal information."
2) Notice is not required if, after a reasonable investigation, the entity determines that there is no reasonable likelihood of harm to an individual.
3) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.

California

Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.

Colorado

1) Allows for telephonic notice.
2) Substitute notice is allowed where the affected class of persons to be notified exceeds 250,000.
3) Notice is not required where the entity establishes that misuse of the information is not reasonably likely.
4) If an entity discovers circumstances requiring notification to more than 1,000 persons, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
5) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.

Connecticut

1) Notice is not required where after an appropriate investigation and consultation with relevant federal, state, and local agencies responsible for law enforcement, the entity reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired.
2) Allows for telephonic notice.
3) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.

Delaware

1) Allows for telephonic notice.
2) "Substitute notice" is allowed where the cost of providing notice will exceed $75,000 or the affected class of Delaware residents to be notified exceeds 100,000 residents.
3) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.
4) Notice is not required where after an appropriate investigation the entity reasonably determines that the breach will not likely result in the misuse of personal information.

Florida

1) Unless otherwise provided in the statute (*e.g.*, request by law enforcement), notification must be made no later than 45 days following the determination of the breach. Failure to procure notification within 45 days can amount to fines not to exceed $500,000.
2) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.
3) Notice is not required where after an appropriate investigation and consultation with relevant federal, state, and local agencies responsible for law enforcement, the entity reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired.
4) If an entity discovers circumstances requiring notification to more than 1,000 persons, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

Georgia

1) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.
2) Qualifies the definition of "personal information" by noting that any of the data elements alone are sufficient, without the individual's name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.
3) If an entity discovers circumstances requiring notification to more than 10,000 persons, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

Hawaii

1) Notice is not required where the entity establishes that illegal use of the personal information is not reasonably likely to occur or create a risk of harm to a person.
2) An entity must provide notice of the breach if encrypted information is accessed in conjunction with the encryption key.
3) Allows telephonic notice.
4) "Substitute notice" is allowed where the cost of providing notice will exceed $100,000 or the affected class of individuals to be notified exceeds 200,000.
5) If a database owner is required to make a disclosure to more than 1,000 consumers, the database owner shall also notify all consumer reporting agencies as defined in 15 U.S.C. §1681a(p).

Idaho

1) Allows for telephonic notice.
2) "Substitute notice" is allowed where the cost of providing notice will exceed $25,000 or the affected class of individuals to be notified exceeds $50,000.
3) Notice is not required where the entity establishes that misuse of the information is not reasonably likely to occur.
4) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.

Illinois

Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.

Indiana

1) "Breach of the security of a system" includes the unauthorized acquisition of computerized data that has been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data is no longer in a computerized format.
2) A Social Security number alone is sufficient for being considered "personal information."
3) Notice is required if the database owner knows or should know that the unauthorized acquisition constituting the breach has resulted in or could result in identity theft or fraud affecting an Indiana resident.
4) If a database owner is required to make a disclosure to more than 1,000 consumers, the database owner shall also notify all consumer reporting agencies as defined in 15 U.S.C. §1681a(p).
5) Allows telephonic, facsimile, and e-mail notification.
6) Notice can also be effected where a database owner maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are as stringent as the applicable statute.

Kansas

1) "Substitute notice" is allowed where the cost of providing notice will exceed $100,000 or the affected class of individuals to be notified exceeds 5,000.
2) Notice is not required if the entity does not reasonably believe the breach will result in identity theft to any consumer.
3) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.
4) If a database owner is required to make a disclosure to more than 1,000 consumers, the database owner shall also notify all consumer reporting agencies as defined in 15 U.S.C. §1681a(p).

Louisiana

1) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.
2) Notice is not required where after an appropriate investigation the entity reasonably determines that the breach will not likely result in the misuse of personal information.

3) If an entity discovers circumstances requiring notification to more than 1,000 persons, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

Maine

1) "Substitute notice" is allowed where the cost of providing notice will exceed $5,000 or the affected class of individuals to be notified exceeds 1,000.
2) Qualifies the definition of "personal information" by noting that any of the data elements alone are sufficient, without the individual's name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.
3) If an entity discovers circumstances requiring notification to more than 1,000 persons, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

Minnesota

1) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.
2) If an entity discovers circumstances requiring notification to more than 500 persons, the entity shall notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

Montana

1) Allows for telephonic notice.
2) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed without unreasonable delay.

Nebraska

1) Allows for telephonic notice.
2) "Substitute notice" is allowed where the cost of providing notice will exceed $75,000 or the affected class of individuals to be notified exceeds 100,000. A less stringent form of substitute notice is also allowed for small businesses.
3) Adds "unique electronic identification number" and "unique biometric data" to the list of data elements in the definition of "personal information."
4) Notice is not required where the entity establishes that misuse of the information is not reasonably likely to occur.
5) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.

Nevada

1) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.

2) If an entity discovers circumstances requiring notification to more than 1,000 persons, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

New Hampshire

1) Notice is not required where the entity establishes that misuse of the information is not reasonably likely to occur.
2) Allows telephonic notice.
3) "Substitute notice" is allowed where the cost of providing notice will exceed $5,000 or the affected class of individuals to be notified exceeds 1,000.
4) Notice can also be effected pursuant to an entity's internal notification procedures maintained as part of an information security policy for the treatment of personal information.
5) If an entity discovers circumstances requiring notification to more than 1,000 persons, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

New Jersey

1) Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.
2) Notice is not required where the entity establishes that misuse of the information is not reasonably possible. Any such determination shall be documented in writing and retained for five years.
3) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.
4) If an entity discovers circumstances requiring notification to more than 1,000 persons, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

New York

1) Allows for telephonic notice.
2) If an entity discovers circumstances requiring notification to more than 5,000 persons, the entity shall notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
3) If any NY residents are notified, notification must also be made to the state Attorney General, the Consumer Protection Board, and the state Office of Cyber Security and Critical Infrastructure Coordination.

North Carolina

1) Allows for telephonic notice.
2) If an entity discovers circumstances requiring notification to more than 1,000 persons, the entity shall notify the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
3) Notification is not required where there is not a material risk of harm to the consumer.
4) Biometric data, fingerprints, and digital signatures are added to the list of "data elements" in the definition of "personal information."

North Dakota

1) Birth date, mother's maiden name, employer identification, and electronic signature are added to the list of "data elements" in the definition of "personal information."

2) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.

Ohio

1) Notice is not required where it is not reasonably believed that a material risk of identity theft exists.
2) Unless otherwise provided in the statute (*e.g.*, request by law enforcement), notification must be made no later than 45 days following the determination of the breach.
3) Allows for telephonic notice.
4) A less stringent form of "substitute notice" is also allowed for small businesses.
5) If an entity discovers circumstances requiring notification to more than 1,000 residents, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

Pennsylvania

1) Notice is not required where the entity does not reasonably believe that the unauthorized access has caused or will cause loss or injury to any resident of the Commonwealth.
2) Allows for telephonic and e-mail notice.
3) "Substitute notice" is allowed where the cost of providing notice will exceed $100,000 or the affected class of subject persons exceeds 175,000.
4) A resident of the Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data, is in the Commonwealth.
5) An entity must provide notice of the breach of encrypted information if it can be linked to a security breach of the encryption key.

Rhode Island

1) Notice is not required where a determination is made that the breach will not likely result in a significant risk of identity theft to the individuals whose personal information has been acquired.
2) "Substitute notice" is allowed where the cost of providing notice will exceed $25,000 or the affected class of subject persons exceeds 50,000.
3) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.

Tennessee

1) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.
2) If an entity discovers circumstances requiring notification to more than 1,000 residents, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

Texas

1) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.

2) If an entity discovers circumstances requiring notification to more than 10,000 residents, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

Utah

1) Notice is not required where the entity establishes that misuse of the information is not reasonably likely to occur.
2) Allows for telephonic notice and notice by publication in a newspaper of general circulation.
3) Does not provide for "substitute notice."
4) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.

Vermont

1) Allows for telephonic notice.
2) "Substitute notice" is allowed where the cost of providing notice will exceed $5,000 or the affected class of individuals to be notified exceeds 5,000.
3) If an entity discovers circumstances requiring notification to more than 1,000 residents, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
4) Notice is not required where the entity establishes that misuse of the information is not reasonably possible. Notice of such determination must be provided to the Attorney General or the Department of Banking, Insurance, Securities, and Health Care Administration.

Washington

1) Notice can also be effected where a person or entity maintains its own notice procedures as part of an information security policy for the treatment of personal information, and such procedures are followed in a manner consistent with the timing requirements of the statute.
2) Notification is not required if the security breach does not seem reasonably likely to subject customers to a risk of criminal activity.

Wisconsin

1) The statute addresses all forms of the impermissible acquisition of personal information and is not limited to the security breach of a computer.
2) The individual's deoxyribonucleic acid profile and unique biometric data are added to the list of "data elements" in the definition of "personal information."
3) If an entity discovers circumstances requiring notification to more than 1,000 residents, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
4) Notice is not required if the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.
5) Notice shall occur within 45 days after the entity learns of the acquisition of personal information.
6) Notice shall be by mail or a method that the entity has previously employed to communicate with the subject of the personal information. Otherwise, the entity shall provide notice by a method reasonably calculated to provide actual notice to the subject of the personal information.

ARIZONA

44-7501. NOTIFICATION OF BREACH OF SECURITY SYSTEM; ENFORCEMENT; CIVIL PENALTY; PREEMPTION; EXCEPTIONS; DEFINITIONS

(Conditionally Rpld.)

A. When a person that conducts business in this state and that owns or licenses unencrypted computerized data that includes personal information becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's personal information, the person shall conduct a reasonable investigation to promptly determine if there has been a breach of the security system. If the investigation results in a determination that there has been a breach in the security system, the person shall notify the individuals affected. The notice shall be made in the most expedient manner possible and without unreasonable delay subject to the needs of law enforcement as provided in subsection C of this section and any measures necessary to determine the nature and scope of the breach, to identify the individuals affected or to restore the reasonable integrity of the data system.

B. A person that maintains unencrypted computerized data that includes personal information that the person does not own shall notify and cooperate with the owner or the licensee of the information of any breach of the security of the system following discovery of the breach without unreasonable delay. Cooperation shall include sharing information relevant to the breach of the security of the system with the owner or licensee. The person that owns or licenses the computerized data shall provide notice to the individual pursuant to this section. The person that maintained the data under an agreement with the owner or licensee is not required to provide notice to the individual pursuant to this section unless the agreement stipulates otherwise.

C. The notification required by subsection A of this section may be delayed if a law enforcement agency advises the person that the notification will impede a criminal investigation. The person shall make the notification after the law enforcement agency determines that it will not compromise the investigation.

D. The disclosure required by subsection A of this section shall be provided by one of the following methods:

   1. Written notice.
   2. Electronic notice if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in the electronic signatures in global and national commerce act (P.L. 106-229; 114 Stat. 464; 15 United States Code section 7001).
   3. Telephonic notice.
   4. Substitute notice if the person demonstrates that the cost of providing notice pursuant to paragraph 1, 2 or 3 of this subsection would exceed fifty thousand dollars or that the affected class of subject individuals to be notified exceeds one hundred thousand persons, or the person does not have sufficient contact information. Substitute notice shall consist of all of the following:
      (a) Electronic mail notice if the person has electronic mail addresses for the individuals subject to the notice.
      (b) Conspicuous posting of the notice on the web site of the person if the person maintains one.
      (c) Notification to major statewide media.

E. A person who maintains the person's own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the person notifies subject individuals in accordance with the person's policies if a breach of the security system occurs.

F. A person that complies with the notification requirements or security breach procedures pursuant to the rules, regulations, procedures, guidance or guidelines established by the person's primary or functional federal regulator is deemed to be in compliance with this section.

G. A person is not required to disclose a breach of the security of the system if the person or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur.

H. This section may only be enforced by the attorney general. The attorney general may bring an action to obtain actual damages for a wilful and knowing violation of this section and a civil penalty not to exceed ten thousand dollars per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

I. The state legislature determines that security system breach notification is a matter of statewide concern. The power to regulate security breach notification is preempted by this state and this section shall supersede and preempt all municipal and county laws, charters, ordinances and rules relating to issues regulated by this chapter.

J. This section does not apply to either of the following:

1. A person subject to title V of the Gramm-Leach-Bliley act of 1999 (P.L. 106-102; 113 Stat. 1338; 15 United States Code sections 6801 through 6809).
2. Covered entities as defined under regulations implementing the health insurance portability and accountability act, 45 Code of Federal Regulations section 160.103 (1996).

K. A law enforcement agency, a prosecution agency and a court shall create and maintain an information security policy that includes notification procedures for a breach of the security system of the law enforcement agency, the prosecuting agency or the court.

L. For the purposes of this section:

1. "Breach", "breach of the security of the system", "breach of the security system" or "security breach" means an unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information maintained by a person as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual. Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security system if the personal information is not used for a purpose unrelated to the person or subject to further wilful unauthorized disclosure.
2. "Court" means the supreme court, court of appeals, superior court, courts inferior to the superior court and justice courts.
3. "Encrypted" means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.
4. "Individual" means a person that is a resident of this state as determined by a principal mailing address in this state as reflected in the records of the person conducting business in this state at the time of the breach.
5. "Law enforcement agency" means the department of public safety, county sheriff departments or municipal police departments.
6. "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency or any other legal or commercial entity. Person does not include a law enforcement agency, a prosecution agency or a court.
7. "Personal information":
   (a) 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 the data element is not encrypted, redacted or secured by any other method rendering the element unreadable or unusable:
      (i) The individual's social security number.
      (ii) The individual's number on a driver license issued pursuant to section 28-3166 or number on a nonoperating identification license issued pursuant to section 28-3165.

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

(b) 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.

8. "Prosecution agency" means the attorney general, any county attorney or any municipal prosecutor.

9. "Redact" means alter or truncate data such that no more than the last four digits of a social security number, driver license number, nonoperating identification license number, financial account number or credit or debit card number is accessible as part of the personal information.

ARKANSAS

4-110-101. SHORT TITLE.

This chapter shall be known and cited as the "Personal Information Protection Act".

History. Acts 2005, No. 1526, § 1.

4-110-102. FINDINGS AND PURPOSE.

(a) It is the intent of the General Assembly to ensure that sensitive personal information about Arkansas residents is protected.

(b) To that end, the purpose of this chapter is to encourage individuals, businesses, and state agencies that acquire, own, or license personal information about the citizens of the State of Arkansas to provide reasonable security for the information.

History. Acts 2005, No. 1526, § 1.

4-110-103. DEFINITIONS.

As used in this chapter:

(1) (A) "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 a person or business.

(B) "Breach of the security of the system" does not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure;

(2) (A) "Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country or the parent or the subsidiary of a financial institution.

(B) "Business" includes:

(i) An entity that destroys records; and

(ii) A state agency;

(3) "Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business;

(4) "Individual" means a natural person;

(5) "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional;

(6) "Owns or licenses" includes, but is not limited to, personal information that a business retains as part of the internal customer account of the business or for the purpose of using the information in transactions with the person to whom the information relates;

(7) "Personal information" means an individual's first name or first initial and his or her last name in combination with any one (1) or more of the following data elements when either the name or the data element is not encrypted or redacted:

(A) Social security number;

(B) Driver's license number or Arkansas identification card number;

(C) Account number, credit card number, 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; and

(D) Medical information;

(8) (A) "Records" means any material that contains sensitive personal information in electronic form.

(B) "Records" does not include any publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number; and

(9) "State agencies" or "state agency" means any agency, institution, authority, department, board, commission, bureau, council, or other agency of the State of Arkansas supported by cash funds or the appropriation of state or federal funds.

History. Acts 2005, No. 1526, § 1.

4-110-104. PROTECTION OF PERSONAL INFORMATION.

(a) A person or business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

(b) A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

History. Acts 2005, No. 1526, § 1.

4-110-105. DISCLOSURE OF SECURITY BREACHES.

(a) (1) Any person or business that acquires, 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 of the security of the system to any resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(2) The disclosure shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section, or any measures necessary to determine the scope of the breach and to 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 system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) (1) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

(2) The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.

(e) For purposes of this section, notice may be provided by one (1) of the following methods:

(1) Written notice;

(2) Electronic mail notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001, as it existed on January 1, 2005; or

(3) (A) Substitute notice if the person or business demonstrates that:

(i) The cost of providing notice would exceed two hundred fifty thousand dollars ($250,000);

(ii) The affected class of persons to be notified exceeds five hundred thousand (500,000); or

(iii) The person or business does not have sufficient contact information.

(B) Substitute notice shall consist of all of the following:

(i) Electronic mail notice when the person or business has an electronic mail address for the subject persons;

(ii) Conspicuous posting of the notice on the website of the person or business if the person or business maintains a website; and

(iii) Notification by statewide media.

(f) Notwithstanding subsection (e) of this section, 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 section shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies affected persons in accordance with its policies in the event of a breach of the security of the system.

History. Acts 2005, No. 1526, § 1.

4-110-106. EXEMPTIONS.

(a) (1) The provisions of this chapter do not apply to a person or business that is regulated by a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breaches of the security of personal information than that provided by this chapter.

(2) Compliance with the state or federal law shall be deemed compliance with this chapter with regard to the subjects covered by this chapter.

(b) This section does not relieve a person or business from a duty to comply with any other requirements of other state and federal law regarding the protection and privacy of personal information.

History. Acts 2005, No. 1526, § 1.

4-110-107. WAIVER.

Any waiver of a provision of this chapter is contrary to public policy, void, and unenforceable.

History. Acts 2005, No. 1526, § 1.

4-110-108. PENALTIES.

Any violation of this chapter is punishable by action of the Attorney General under the provisions of § 4-88-101 et seq.

History. Acts 2005, No. 1526, § 1.

CALIFORNIA

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.

COLORADO

6-1-716. NOTIFICATION OF SECURITY BREACH.

(1) **Definitions.** As used in this section, unless the context otherwise requires:

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

(b) "Commercial entity" means any private legal entity, whether for-profit or not-for-profit.

(c) "Notice" means:

(I) Written notice to the postal address listed in the records of the individual or commercial entity;

(II) Telephonic notice;

(III) Electronic notice, if a primary means of communication by the individual or commercial entity with a Colorado resident is by electronic means or the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. sec. 7001 et seq.; or

(IV) Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed two hundred fifty thousand dollars, the affected class of persons to be notified exceeds two hundred fifty thousand Colorado residents, or the individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:

(A) E-mail notice if the individual or the commercial entity has e-mail addresses for the members of the affected class of Colorado residents;

(B) Conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains one; and

(C) Notification to major statewide media.

(d) (I) "Personal information" means a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable:

(A) Social security number;

(B) Driver's license number or identification card number;

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

(II) "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.

(2) **Disclosure of breach.**

(a) An individual or a commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The individual or the commercial entity shall give notice as soon as possible to the affected Colorado resident unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

(b) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a Colorado resident occurred or is likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets.

(c) Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and the law enforcement agency has notified the individual or commercial entity that conducts business in Colorado not to send notice required by this section. Notice required by this section shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation and has notified the individual or commercial entity that conducts business in Colorado that it is appropriate to send the notice required by this section.

(d) If an individual or commercial entity is required to notify more than one thousand Colorado residents of a breach of the security of the system pursuant to this section, the individual or commercial entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 1618a (p), of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified. Nothing in this paragraph (d) shall be construed to require the individual or commercial entity to provide to the consumer reporting agency the names or other personal information of breach notice recipients. This paragraph (d) shall not apply to a person who is subject to title V of the federal "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 et seq.

(3) **Procedures deemed in compliance with notice requirements.**

(a) Under this section, an individual or a commercial entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information and whose procedures are otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notice requirements of this section if the individual or the commercial entity notifies affected Colorado customers in accordance with its policies in the event of a breach of security of the system.

(b) An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section.

(4) **Violations.** The attorney general may bring an action in law or equity to address violations of this section and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law.

Source: L. 2006: Entire section added, p. 536, § 1, effective September 1.

Editor's note: Section 2 of chapter 145, Session Laws of Colorado 2006, provides that the act enacting this section applies to breaches of the security of the system, as defined in section 6-1-716 (1) (a), occurring on or after September 1, 2006.

CONNECTICUT

SEC. 36A-701B. BREACH OF SECURITY RE COMPUTERIZED DATA CONTAINING PERSONAL INFORMATION. DISCLOSURE OF BREACH. DELAY FOR CRIMINAL INVESTIGATION. MEANS OF NOTICE. UNFAIR TRADE PRACTICE.

(a) For purposes of this section, "breach of security" means unauthorized access to or acquisition of electronic files, media, databases or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable; "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: (1) Social Security number; (2) driver's license number or state identification card number; or (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. "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.

(b) Any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall disclose any breach of security following the discovery of the breach to any resident of this state whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person through such breach of security. Such disclosure shall be made without unreasonable delay, subject to the provisions of subsection (d) of this section and the completion of an investigation by such person to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system. Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.

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

(d) Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after such law enforcement agency determines that notification will not compromise the criminal investigation and so notifies the person of such determination.

(e) Any notice required by the provisions of this section may be provided by one of the following methods: (1) Written notice; (2) telephone notice; (3) electronic notice, provided such notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001; (4) substitute notice, provided such person demonstrates that the cost of providing notice in accordance with subdivision (1), (2) or (3) of this subsection would exceed two hundred fifty thousand dollars, that the affected class of subject persons to be notified exceeds five hundred thousand persons or the person does not have sufficient contact information. Substitute notice shall consist of the following: (A) Electronic mail notice when the person, business or agency has an electronic mail address for the affected persons; (B) conspicuous posting of the notice on the web site of the person, business or agency if the person maintains one; and (C) notification to major state-wide media, including newspapers, radio and television.

(f) Any person that maintains such person's own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies subject persons in accordance with such person's policies in the event of a breach of security. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in 15 USC 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies subject persons in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security of the system.

(g) Failure to comply with the requirements of this section shall constitute an unfair trade practice for purposes of section 42-110b and shall be enforced by the Attorney General.

(P.A. 05-148, S. 3; 05-288, S. 231, 232.)

History: P.A. 05-148 effective January 1, 2006; P.A. 05-288 made technical changes in Subsecs. (b) and (f), effective January 1, 2006.

DELAWARE

TITLE 6

COMMERCE AND TRADE

SUBTITLE II

OTHER LAWS RELATING TO COMMERCE AND TRADE

CHAPTER 12B. COMPUTER SECURITY BREACHES

§ 12B-101. DEFINITIONS.

For purposes of this chapter:

(1) "Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure;

(2) "Commercial entity" includes corporations, business trusts, estates, trusts, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit;

(3) "Notice" means:

   a. Written notice;

   b. Telephonic notice;

   c. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 of Title 15 of the United States Code; or

   d. Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $75,000, or that the affected class of Delaware residents to be notified exceeds 100,000 residents, or that the individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:

      1. E-mail notice if the individual or the commercial entity has e-mail addresses for the members of the affected class of Delaware residents; and

      2. Conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains one; and

      3. Notice to major statewide media.

(4) "Personal information" means a Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:

   a. Social Security number;

   b. Driver's license number or Delaware Identification Card number; or

   c. Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records; (75 Del. Laws, c. 61, § 1.)

§ 12B-102. DISCLOSURE OF BREACH OF SECURITY OF COMPUTERIZED PERSONAL INFORMATION BY AN INDIVIDUAL OR A COMMERCIAL ENTITY.

(a) An individual or a commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about a Delaware resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Delaware resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

(b) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a Delaware resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.

(c) Notice required by this chapter may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by this chapter must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation. (75 Del. Laws, c. 61, § 1.)

§ 12B-103. PROCEDURES DEEMED IN COMPLIANCE WITH SECURITY BREACH REQUIREMENTS.

(a) Under this chapter, an individual or a commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notice requirements of this chapter if the individual or the commercial entity notifies affected Delaware residents in accordance with its policies in the event of a breach of security of the system.

(b) Under this chapter, an individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this chapter if the individual or the commercial entity notifies affected Delaware residents in accordance with the maintained procedures when a breach occurs. (75 Del. Laws, c. 61, § 1.)

§ 12B-104. VIOLATIONS.

Pursuant to the enforcement duties and powers of the Consumer Protection Division of the Department of Justice under § 2517 of Title 29, the Attorney General may bring an action in law or equity to address violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both. The provisions of this chapter are not exclusive and do not relieve an individual or a commercial entity subject to this chapter from compliance with all other applicable provisions of law. (75 Del. Laws, c. 61, § 1.)

FLORIDA

817.5681 BREACH OF SECURITY CONCERNING CONFIDENTIAL PERSONAL INFORMATION IN THIRD-PARTY POSSESSION; ADMINISTRATIVE PENALTIES.--

(1) (a) Any person who conducts business in this state and maintains computerized data in a system that includes personal information shall provide notice of any breach of the security of the system, following a determination of the breach, to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) and paragraph (10)(a), or subject to any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system. Notification must be made no later than 45 days following the determination of the breach unless otherwise provided in this section.

(b) Any person required to make notification under paragraph (a) who fails to do so within 45 days following the determination of a breach or receipt of notice from law enforcement as provided in subsection (3) is liable for an administrative fine not to exceed $500,000, as follows:

1. In the amount of $1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,000 for each 30-day period or portion thereof for up to 180 days.
2. If notification is not made within 180 days, any person required to make notification under paragraph (a) who fails to do so is subject to an administrative fine of up to $500,000.

(c) The administrative sanctions for failure to notify provided in this subsection shall apply per breach and not per individual affected by the breach.

(d) The administrative sanctions for failure to notify provided in this subsection shall not apply in the case of personal information in the custody of any governmental agency or subdivision, unless that governmental agency or subdivision has entered into a contract with a contractor or third-party administrator to provide governmental services. In such case, the contractor or third-party administrator shall be a person to whom the administrative sanctions provided in this subsection would apply, although such contractor or third-party administrator found in violation of the notification requirements provided in this subsection would not have an action for contribution or setoff available against the employing agency or subdivision.

(2) (a) Any person who maintains computerized data that includes personal information on behalf of another business entity shall disclose to the business entity for which the information is maintained any breach of the security of the system as soon as practicable, but no later than 10 days following the determination, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The person who maintains the data on behalf of another business entity and the business entity on whose behalf the data is maintained may agree who will provide the notice, if any is required, as provided in paragraph (1)(a), provided only a single notice for each breach of the security of the system shall be required. If agreement regarding notification cannot be reached, the person who has the direct business relationship with the resident of this state shall be subject to the provisions of paragraph (1)(a).

(b) Any person required to disclose to a business entity under paragraph (a) who fails to do so within 10 days after the determination of a breach or receipt of notification from law enforcement as provided in subsection (3) is liable for an administrative fine not to exceed $500,000, as follows:

1. In the amount of $1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,000 for each 30-day period or portion thereof for up to 180 days.
2. If disclosure is not made within 180 days, any person required to make disclosures under paragraph (a) who fails to do so is subject to an administrative fine of up to $500,000.

(c) The administrative sanctions for nondisclosure provided in this subsection shall apply per breach and not per individual affected by the breach.

(d) The administrative sanctions for nondisclosure provided in this subsection shall not apply in the case of personal information in the custody of any governmental agency or subdivision unless that governmental agency or subdivision has entered into a contract with a contractor or third-party administrator to provide governmental services. In such case, the contractor or third-party administrator shall be a person to whom the administrative sanctions provided in this subsection would apply, although such contractor or third-party administrator found in violation of the nondisclosure restrictions in this subsection would not have an action for contribution or setoff available against the employing agency or subdivision.

(3) The notification required by this section may be delayed upon a request by law enforcement if a law enforcement agency determines that the notification will impede a criminal investigation. The notification time period required by this section shall commence after the person receives notice from the law enforcement agency that the notification will not compromise the investigation.

(4) For purposes of this section, the terms "breach" and "breach of the security of the system" mean unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person. Good faith acquisition of personal information by an employee or agent of the person is not a breach or breach of the security of the system, provided the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

(5) For purposes of this section, the term "personal information" means an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted:

(a) Social security number.

(b) Driver's license number or Florida Identification Card number.

(c) Account number, credit card number, 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.

For purposes of this section, the term "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.

(6) For purposes of this section, notice may be provided by one of the following methods:

(a) Written notice;

(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. s. 7001 or if the person or business providing the notice has a valid e-mail address for the subject person and the subject person has agreed to accept communications electronically; or

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

1. Electronic mail or e-mail notice when the person has an electronic mail or e-mail address for the subject persons.
2. Conspicuous posting of the notice on the web page of the person, if the person maintains a web page.
3. Notification to major statewide media.

(7) For purposes of this section, the term "unauthorized person" means any person who does not have permission from, or a password issued by, the person who stores the computerized data to acquire such data, but does not include any individual to whom the personal information pertains.

(8) For purposes of this section, the term "person" means a person as defined in s. 1.01(3). For purposes of this section, the State of Florida, as well as any of its agencies or political subdivisions, and any of the agencies of its political subdivisions, constitutes a person.

(9) Notwithstanding subsection (6), a person who maintains:

(a) The person's own notification procedures as part of an information security or privacy policy for the treatment of personal information, which procedures are otherwise consistent with the timing requirements of this part; or

(b) A notification procedure pursuant to the rules, regulations, procedures, or guidelines established by the person's primary or functional federal regulator,

shall be deemed to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with the person's policies or the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security of the system.

(10) (a) Notwithstanding subsection (2), notification is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for 5 years.

(b) Any person required to document a failure to notify affected persons who fails to document the failure as required in this subsection or who, if documentation was created, fails to maintain the documentation for the full 5 years as required in this subsection is liable for an administrative fine in the amount of up to $50,000 for such failure.

(c) The administrative sanctions outlined in this subsection shall not apply in the case of personal information in the custody of any governmental agency or subdivision, unless that governmental agency or subdivision has entered into a contract with a contractor or third-party administrator to provide governmental services. In such case the contractor or third-party administrator shall be a person to whom the administrative sanctions outlined in this subsection would apply, although such contractor or third-party administrator found in violation of the documentation and maintenance of documentation requirements in this subsection would not have an action for contribution or setoff available against the employing agency or subdivision.

(11) The Department of Legal Affairs may institute proceedings to assess and collect the fines provided in this section.

(12) If a person discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at a single time, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.

History.--s. 2, ch. 2005-229.

GEORGIA

10-1-910.

The General Assembly finds and declares as follows:

(1) The privacy and financial security of individuals is increasingly at risk due to the ever more widespread collection of personal information by both the private and public sectors;

(2) Credit card transactions, magazine subscriptions, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Internet websites are all sources of personal information and form the source material for identity thieves;

(3) Identity theft is one of the fastest growing crimes committed in this state. Criminals who steal personal information such as social security numbers use the information to open credit card accounts, write bad checks, buy cars, purchase property, and commit other financial crimes with other people's identities;

(4) Implementation of technology security plans and security software as part of an information security policy may provide protection to consumers and the general public from identity thieves;

(5) Information brokers should clearly define the standards for authorized users of its data so that a breach by an unauthorized user is easily identifiable;

(6) Identity theft is costly to the marketplace and to consumers; and

(7) Victims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of unauthorized acquisition and possible misuse of a person's personal information is imperative.

10-1-911.

As used in this article, the term:

(1) 'Breach of the security of the system' means unauthorized acquisition of an individual's computerized data that compromises the security, confidentiality, or integrity of personal information of such 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 such information broker is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(2) 'Information broker' means any person or entity 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 third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.

(3) '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 Section 7001 of Title 15 of the United States Code; or

  (C) Substitute notice, if the information broker demonstrates that the cost of providing notice would exceed $250,000.00, that the affected class of individuals to be notified exceeds 500,000, or that the information broker does not have sufficient contact information to provide written or electronic notice to such individuals. Substitute notice shall consist of all of the following:

    (i) E-mail notice, if the information broker has an e-mail address for the individuals to be notified;

    (ii) Conspicuous posting of the notice on the information broker's website page, if the information broker maintains one; and

    (iii) Notification to major state-wide media.

Notwithstanding any provision of this paragraph to the contrary, an information broker 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 article shall be deemed to be in compliance with the notification requirements of this article if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system.

(4) 'Person' means any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association, or other entity. The term 'person' as used in this article shall not be construed to require duplicative reporting by any individual, corporation, trust, estate, cooperative, association, or other entity involved in the same transaction.

(5) '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 items contained in subparagraphs (A) through (D) of this paragraph when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised. The term 'personal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

10-1-912.

(a) Any information broker that maintains computerized data that includes personal information of individuals shall give notice of 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 this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this Code section, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

(b) Any person or business that maintains computerized data on behalf of an information broker that includes personal information of individuals that the person or business does not own shall notify the information broker 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 Code section may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation. The notification required by this Code section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) In the event that an information broker discovers circumstances requiring notification pursuant to this Code section of more than 10,000 residents of this state at one time, the information broker shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by 15 U.S.C. Section 1681a, of the timing, distribution, and content of the notices.

HAWAII

[§ 487N-1.] DEFINITIONS.

As used in this chapter, unless the context otherwise requires:

"Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized, and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of the State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. The term also includes an entity whose business is records destruction.

"Encryption" means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

"Government agency" means any department, division, board, commission, public corporation, or other agency or instrumentality of the State or of any county.

"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 Hawaii identification card number; or
(3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.

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

"Records" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

"Redacted" means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data.

"Security breach" means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach; provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

[§ 487N-2.] NOTICE OF SECURITY BREACH.

(a) Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system.

(b) Any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c).

(c) The notice required by this section shall be delayed if a law enforcement agency informs the business or government agency that notification may impede a criminal investigation or jeopardize national security and requests a delay; provided that such request is made in writing, or the business or government agency documents the request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the business or government agency its determination that notice will no longer impede the investigation or jeopardize national security.

(d) The notice shall be clear and conspicuous. The notice shall include a description of the following:
   (1) The incident in general terms;
   (2) The type of personal information that was subject to the unauthorized access and acquisition;
   (3) The general acts of the business or government agency to protect the personal information from further unauthorized access;
   (4) A telephone number that the person may call for further information and assistance, if one exists; and
   (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

(e) For purposes of this section, notice to affected persons may be provided by one of the following methods:
   (1) Written notice to the last available address the business or government agency has on record;
   (2) Electronic mail notice, for those persons for whom a business or government agency has a valid electronic mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. Section 7001;
   (3) Telephonic notice, provided that contact is made directly with the affected persons; and
   (4) Substitute notice, if the business or government agency demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of subject persons to be notified exceeds two hundred thousand, or if the business or government agency does not have sufficient contact information or consent to satisfy paragraph (1), (2), or (3), for only those affected persons without sufficient contact information or consent, or if the business or government agency is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:
      (A) Electronic mail notice when the business or government agency has an electronic mail address for the subject persons;
      (B) Conspicuous posting of the notice on the website page of the business or government agency, if one is maintained; and
      (C) Notification to major statewide media.

(f) In the event a business provides notice to more than one thousand persons at one time pursuant to this section, the business shall notify in writing, without unreasonable delay, the State of Hawaii's office of consumer protection and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notice.

(g) The following businesses shall be deemed to be in compliance with this section:

(1) A financial institution that is subject to the Federal Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and Customer Notice published in the Federal Register on March 29, 2005 by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, or subject to 12 C.F.R. Part 748, and any revisions, additions, or substitutions relating to said interagency guidance; and

(2) Any health plan or healthcare provider that is subject to and in compliance with the standards for privacy or individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996.

(h) Any waiver of the provisions of this section is contrary to public policy and is void and unenforceable.

[§ 487N-3.] PENALTIES; CIVIL ACTION.

(a) Any business that violates any provision of this chapter shall be subject to penalties of not more than $2,500 for each violation. The attorney general or the executive director of the office of consumer protection may bring an action pursuant to this section. No such action may be brought against a government agency.

(b) In addition to any penalty provided for in subsection (a), any business that violates any provision of this chapter shall be liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation. The court in any action brought under this section may award reasonable attorneys' fees to the prevailing party. No such action may be brought against a government agency.

(c) The penalties provided in this section shall be cumulative to the remedies or penalties available under all other laws of this State.

[§ 487N-4.] REPORTING REQUIREMENTS.

A government agency shall submit a written report to the legislature within twenty days after discovery of a security breach at the government agency that details information relating to the nature of the breach, the number of individuals affected by the breach, a copy of the notice of security breach that was issued, the number of individuals to whom the notice was sent, whether the notice was delayed due to law enforcement considerations, and any procedures that have been implemented to prevent the breach from reoccurring. In the event that a law enforcement agency informs the government agency that notification may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until twenty days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security.

IDAHO

28-51-104. DEFINITIONS. FOR PURPOSES OF SECTIONS 28-51-104 THROUGH 28-51-107, IDAHO CODE:

(1) "Agency" means any "public agency" as defined in section 9-337, Idaho Code.

(2) "Breach of the security of the system" means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an agency, individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an agency, individual or a commercial entity for the purposes of the agency, individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(3) "Commercial entity" includes corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture and any other legal entity, whether for profit or not-for-profit.

(4) "Notice" means:

  (a) Written notice to the most recent address the agency, individual or commercial entity has in its records;

  (b) Telephonic notice;

  (c) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. section 7001; or

  (d) Substitute notice, if the agency, individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed twenty-five thousand dollars ($25,000), or that the number of Idaho residents to be notified exceeds fifty thousand (50,000), or that the agency, individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:

    (i) E-mail notice if the agency, individual or the commercial entity has e-mail addresses for the affected Idaho residents; and

    (ii) Conspicuous posting of the notice on the website page of the agency, individual or the commercial entity if the agency, individual or the commercial entity maintains one; and

    (iii) Notice to major statewide media.

(5) "Personal information" means an Idaho resident's first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:

  (a) Social security number;

  (b) Driver's license number or Idaho identification card number; or

  (c) Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account. The term "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.

(6) "Primary regulator" of a commercial entity or individual licensed or chartered by the United States is that commercial entity's or individual's primary federal regulator, the primary regulator of a commercial entity or individual licensed by the department of finance is the department of finance, the primary regulator of a commercial entity or individual licensed by the department of insurance is the department of insurance and, for all agencies and all other commercial entities or individuals, the primary regulator is the attorney general.

28-51-105. DISCLOSURE OF BREACH OF SECURITY OF COMPUTERIZED PERSONAL INFORMATION BY AN AGENCY, INDIVIDUAL OR A COMMERCIAL ENTITY.

(1) An agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.

(2) An agency, individual or a commercial entity that maintains computerized data that includes personal information that the agency, individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about an Idaho resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.

(3) Notice required by this section may be delayed if a law enforcement agency advises the agency, individual or commercial entity that the notice will impede a criminal investigation. Notice required by this section must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency advises the agency, individual or commercial entity that notification will no longer impede the investigation.

28-51-106. PROCEDURES DEEMED IN COMPLIANCE WITH SECURITY BREACH REQUIREMENTS.

(1) An agency, individual or a commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of section 28-51-105, Idaho Code, is deemed to be in compliance with the notice requirements of section 28-51-105, Idaho Code, if the agency, individual or the commercial entity notifies affected Idaho residents in accordance with its policies in the event of a breach of security of the system.

(2) An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with section 28-51-105, Idaho Code, if the individual or the commercial entity complies with the maintained procedures when a breach of the security of the system occurs.

28-51-107. VIOLATIONS.

In any case in which an agency's, commercial entity's or individual's primary regulator has reason to believe that an agency, individual or commercial entity subject to that primary regulator's jurisdiction under section 28-51-104(6), Idaho Code, has violated section 28-51-105, Idaho Code, by failing to give notice in accordance with that section, the primary regulator may bring a civil action to enforce compliance with that section and enjoin that agency, individual or commercial entity from further violations. Any agency, individual or commercial entity that intentionally fails to give notice in accordance with section 28-51-105, Idaho Code, shall be subject to a fine of not more than twenty-five thousand dollars ($25,000) per breach of the security of the system.

ILLINOIS

BUSINESS TRANSACTIONS

(815 ILCS 530/) Personal Information Protection Act.

(815 ILCS 530/1)

SEC. 1. SHORT TITLE. THIS ACT MAY BE CITED AS THE PERSONAL INFORMATION PROTECTION ACT.

(Source: P.A. 94-36, eff. 1-1-06.)

(815 ILCS 530/5)

SEC. 5. DEFINITIONS. IN THIS ACT:

"Data Collector" may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

"Breach of the security of the system data" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

"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:

(1) Social Security number.

(2) Driver's license number or State identification card number.

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

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

(Source: P.A. 94-36, eff. 1-1-06.)

(815 ILCS 530/10)

SEC. 10. NOTICE OF BREACH.

(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

(b) Any data collector that maintains computerized data that includes personal information that the data collector does not own or license 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.

(b-5) The notification required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(c) For purposes of this Section, notice to consumers 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 for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media.

(d) Notwithstanding subsection (c), a data collector 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 Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

(Source: P.A. 94-36, eff. 1-1-06; 94-947, eff. 6-27-06.)

(815 ILCS 530/12)

SEC. 12. NOTICE OF BREACH; STATE AGENCY.

(a) Any State agency that collects personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data or written material following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

(b) For purposes of this Section, notice to residents 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 for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the State agency demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the State agency does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the State agency has an email address for the subject persons; (ii) conspicuous posting of the notice on the State agency's web site page if the State agency maintains one; and (iii) notification to major statewide media.

(c) Notwithstanding subsection (b), a State 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 Act shall be deemed in compliance with the notification requirements of this Section if the State agency notifies subject persons in accordance with its policies in the event of a breach of the security of the system data or written material.

(d) If a State agency is required to notify more than 1,000 persons of a breach of security pursuant to this Section, the State agency shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notices. Nothing in this subsection (d) shall be construed to require the State agency to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients.

(Source: P.A. 94-947, eff. 6-27-06.)

(815 ILCS 530/15)

SEC. 15. WAIVER. ANY WAIVER OF THE PROVISIONS OF THIS ACT IS CONTRARY TO PUBLIC POLICY AND IS VOID AND UNENFORCEABLE.

(Source: P.A. 94-36, eff. 1-1-06.)

(815 ILCS 530/20)

SEC. 20. VIOLATION. A VIOLATION OF THIS ACT CONSTITUTES AN UNLAWFUL PRACTICE UNDER THE CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT.

(Source: P.A. 94-36, eff. 1-1-06.)

(815 ILCS 530/25)

SEC. 25. ANNUAL REPORTING.

Any State agency that collects personal data and has had a breach of security of the system data or written material shall submit a report within 5 business days of the discovery or notification of the breach to the General Assembly listing the breaches and outlining any corrective measures that have been taken to prevent future breaches of the security of the system data or written material. Any State agency that has submitted a report under this Section shall submit an annual report listing all breaches of security of the system data or written materials and the corrective measures that have been taken to prevent future breaches.

(Source: P.A. 94-947, eff. 6-27-06.)

INDIANA

IC 24-4.9-2-2 "BREACH OF THE SECURITY OF A SYSTEM"

Sec. 2. (a) "Breach of the security of a system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.

(b) The term does not include the following:

(1) Good faith acquisition of personal information by an employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure.

(2) Unauthorized acquisition of a portable electronic device on which personal information is stored, if access to the device is protected by a password that has not been disclosed.

As added by P.L.125-2006, SEC.6.

IC 24-4.9-2-9 "PERSON"

Sec. 9. "Person" means an individual, a corporation, a business trust, an estate, a trust, a partnership, an association, a nonprofit corporation or organization, a cooperative, or any other legal entity.

As added by P.L.125-2006, SEC.6.

IC 24-4.9-2-10 "PERSONAL INFORMATION"

Sec. 10. "Personal information" means:

(1) a Social Security number that is not encrypted or redacted; or

(2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:

(A) A driver's license number.

(B) A state identification card number.

(C) A credit card number.

(D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

The term does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.

As added by P.L.125-2006, SEC.6.

IC 24-4.9-3-1 DISCLOSURE OF BREACH

Sec. 1. (a) Except as provided in section 4(c), 4(d), and 4(e) of this chapter, after discovering or being notified of a breach of the security of a system, the data base owner shall disclose the breach to an Indiana resident whose:

(1) unencrypted personal information was or may have been acquired by an unauthorized person; or

(2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key; if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident.

(b) A data base owner required to make a disclosure under subsection (a) to more than one thousand (1,000) consumers shall also disclose to each consumer reporting agency (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system.

As added by P.L.125-2006, SEC.6.

IC 24-4.9-3-2 NOTIFICATION OF DATA BASE OWNER

Sec. 2. A person that maintains computerized data but that is not a data base owner shall notify the data base owner if the person discovers that personal information was or may have been acquired by an unauthorized person.

As added by P.L.125-2006, SEC.6.

IC 24-4.9-3-3 DELAY OF DISCLOSURE OR NOTIFICATION

Sec. 3. (a) A person required to make a disclosure or notification under this chapter shall make the disclosure or notification without unreasonable delay. For purposes of this section, a delay is reasonable if the delay is:

(1) necessary to restore the integrity of the computer system;

(2) necessary to discover the scope of the breach; or

(3) in response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will:

(A) impede a criminal or civil investigation; or

(B) jeopardize national security.

(b) A person required to make a disclosure or notification under this chapter shall make the disclosure or notification as soon as possible after:

(1) delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach; or

(2) the attorney general or a law enforcement agency notifies the person that delay will no longer impede a criminal or civil investigation or jeopardize national security.

As added by P.L.125-2006, SEC.6.

IC 24-4.9-3-4 METHOD OF DISCLOSURE; EXCEPTIONS

Sec. 4. (a) Except as provided in subsection (b), a data base owner required to make a disclosure under this chapter shall make the disclosure using one (1) of the following methods:

(1) Mail.

(2) Telephone.

(3) Facsimile (fax).

(4) Electronic mail, if the data base owner has the electronic mail address of the affected Indiana resident.

(b) If a data base owner required to make a disclosure under this chapter is required to make the disclosure to more than five hundred thousand (500,000) Indiana residents, or if the data base owner required to make a disclosure under this chapter determines that the cost of the disclosure will be more than two hundred fifty thousand dollars ($250,000), the data base owner required to make a disclosure under this chapter may elect to make the disclosure by using both of the following methods:

(1) Conspicuous posting of the notice on the web site of the data base owner, if the data base owner maintains a web site.

(2) Notice to major news reporting media in the geographic area where Indiana residents affected by the breach of the security of a system reside.

(c) A data base owner that maintains its own disclosure procedures as part of an information privacy policy or a security policy is not required to make a separate disclosure under this chapter if the data base owner's information privacy policy or security policy is at least as stringent as the disclosure requirements described in:

(1) sections 1 through 4(b) of this chapter;

(2) subsection (d); or

(3) subsection (e).

(d) A data base owner that maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under:

(1) the federal USA Patriot Act (P.L. 107-56);

(2) Executive Order 13224;

(3) the federal Driver's Privacy Protection Act (18 U.S.C. 2781 et seq.);

(4) the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(5) the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or

(6) the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191);

is not required to make a disclosure under this chapter if the data base owner's information privacy, security policy, or compliance plan requires that Indiana residents be notified of a breach of the security of a system without unreasonable delay and the data base owner complies with the data base owner's information privacy, security policy, or compliance plan.

(e) A financial institution that complies with the disclosure requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, as applicable, is not required to make a disclosure under this chapter.

(f) A person required to make a disclosure under this chapter may elect to make all or part of the disclosure in accordance with subsection (a) even if the person could make the disclosure in accordance with subsection (b).

As added by P.L.125-2006, SEC.6.

IC 24-4.9-4 CHAPTER 4. ENFORCEMENT

IC 24-4.9-4-1 FAILURE TO DISCLOSE OR NOTIFY; DECEPTIVE ACT

Sec. 1. (a) A person that is required to make a disclosure or notification in accordance with IC 24-4.9-3 and that fails to comply with any provision of this article commits a deceptive act that is actionable only by the attorney general under this chapter.

(b) A failure to make a required disclosure or notification in connection with a related series of breaches of the security of a system constitutes one (1) deceptive act.

As added by P.L.125-2006, SEC.6.

IC 24-4.9-4-2 ACTION BY ATTORNEY GENERAL

Sec. 2. The attorney general may bring an action under this chapter to obtain any or all of the following:

(1) An injunction to enjoin future violations of IC 24-4.9-3.

(2) A civil penalty of not more than one hundred fifty thousand dollars ($150,000) per deceptive act.

(3) The attorney general's reasonable costs in:

(A) the investigation of the deceptive act; and

(B) maintaining the action.

As added by P.L.125-2006, SEC.6.

KANSAS

(Note: The following language was taken from the enacted senate bill; 2005 Kan. S.B. 196)

Be it enacted by the Legislature of the State of Kansas:

NEW SECTION 1.

(a) It shall be unlawful for any person to knowingly and with the intent to defraud, possess or use a scanning device to access, read, obtain, memorize or store, temporarily or permanently, information encoded on the computer chip or magnetic strip or stripe of a payment card.

(b) It shall be unlawful for any person to knowingly and with the intent to defraud, possess or use a reencoder to place encoded information on the computer chip or magnetic strip or stripe of a payment card or any electronic medium that allows an authorized transaction to occur.

(c) As used in this section:

(1) "Scanning device" means a scanner, reader or any other electronic device that is used to access, read, scan, obtain, memorize or store, temporarily or permanently, information encoded on the computer chip or magnetic strip or stripe of a payment card.

(2) "Reencoder" means an electronic device that places encoded information from the computer chip, magnetic strip or stripe of a payment card onto the computer chip, magnetic strip or stripe of a different payment card or any electronic medium that allows an authorized transaction to occur.

(3) "Payment card" means a credit card, debit card or any other card that is issued to an authorized user and that allows the user to obtain, purchase or receive goods, services, money or anything else of value.

(d) Violation of this section shall be a severity level 6, nonperson felony.

(e) This section shall be a part of and supplemental to the Kansas criminal code.

NEW SEC. 2.

(a) (1) Unless required by federal law, no document available for public inspection or copying shall contain an individual's social security number if such document contains such individual's personal information. "Personal information" shall include, but not be limited to, name, address, phone number or e-mail address.

(2) The provisions of paragraph (1) of this subsection shall not apply to documents recorded in the official records of any recorder of deeds of the county or to any documents filed in the official records of the court and shall be included, but not limited to, such documents of any records that when filed constitutes [sic]:

(1) A consensual or nonconsensual lien;

(2) an eviction record;

(3) a judgment;

(4) a conviction or arrest;

(5) a bankruptcy;

(6) a secretary of state filing; or

(7) a professional license.

(b) (1) No person, including an individual, firm, corporation, association, partnership, joint venture or other business entity, or any employee or agent therefor, shall solicit, require or use for commercial purposes an individual's social security number unless such number is necessary for such person's normal course of business and there is a specific use for such number for which no other identifying number may be used.

(2) Paragraph (1) of this subsection does not apply to documents or records that are recorded or required to be open to the public pursuant to state or federal law, or by court rule or order, and this paragraph does not limit access to these documents or records.

(3) Paragraph (1) of this subsection does not apply to the collection, use or release of social security numbers for the following purposes:

(A) Mailing of documents that include social security numbers sent as part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the social security number;

(B) internal verification or administrative purposes;

(C) investigate or prevent fraud, conduct background checks, conduct social or scientific research, collect a debt, obtain a credit report from or furnish data to a consumer reporting agency pursuant to the fair credit reporting act, 15 U.S.C. Section 1681, et seq., undertake a permissible purpose enumerated under the Gramm-Leach Bliley Act, 15 U.S.C. Section 6802 (e), or locate an individual who is missing, a lost relative, or due a benefit, such as pension, insurance or unclaimed property benefit; or

(D) otherwise required by state or federal law or regulation.

(c) An individual who is aggrieved by a violation of this section may recover a civil penalty of not more than $ 1,000 for each violation.

NEW SEC. 3.

As used in sections 3 and 4, and amendments thereto:

(a) "Consumer" means an individual who is a resident of this state.

(b) "Encrypted" means transformation of data through the use of algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable.

(c) "Notice" means:

(1) Written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001; or

(3) substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $ 100,000, or that the affected class of consumers to be notified exceeds 5,000, or that the individual or the commercial entity does not have sufficient contact information to provide notice.

(d) "Redact" means alteration or truncation of data such that no more than the following are accessible as part of the personal information:

(1) Five digits of a social security number; or

(2) the last four digits of a driver's license number, state identification card number or account number.

(e) "Substitute notice" means:

(1) E-mail notice if the individual or the commercial entity has e-mail addresses for the affected class of consumers;

(2) conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains a web site; and

(3) notification to major statewide media.

(f) "Person" means any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency or other entity.

(g) "Personal information" means a consumer's first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted:

(1) Social security number;

(2) driver's license number or state identification card number; or

(3) financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account. The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

(h) "Security breach" means the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used for or is not subject to further unauthorized disclosure.

NEW SEC. 4.

(a) A person that conducts business in this state, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information shall, when it becomes aware of any breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information has occurred or is reasonably likely to occur, the person or government, governmental subdivision or agency shall give notice as soon as possible to the affected Kansas resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

(b) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the data following discovery of a breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.

(c) Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by this section shall be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.

(d) Notwithstanding any other provision in this section, an individual or a commercial entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the individual or the commercial entity notifies affected consumers in accordance with its policies in the event of a breach of security of the system.

(e) An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section. This section does not relieve an individual or a commercial entity from a duty to comply with other requirements of state and federal law regarding the protection and privacy of personal information.

(f) In the event that a person discovers circumstances requiring notification pursuant to this section of more than 1,000 consumers at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681a(p), of the timing, distribution and content of the notices.

(g) For violations of this section, except as to insurance companies licensed to do business in this state, the attorney general is empowered to bring an action in law or equity to address violations of this section and for other relief that may be appropriate. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law.

(h) For violations of this section by an insurance company licensed to do business in this state, the insurance commissioner shall have the sole authority to enforce the provisions of this section.

LOUISIANA

§3072. LEGISLATIVE FINDINGS

The legislature hereby finds and declares that:

(1) The privacy and financial security of individuals are increasingly at risk due to the ever more widespread collection of personal information.

(2) Credit card transactions, magazine subscriptions, telephone numbers, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Internet web sites are all sources of personal information and form the source material of identity theft.

(3) The crime of identity theft is on the rise in the United States. Criminals who steal personal information use the information to open credit card accounts, write bad checks, buy automobiles, and commit other financial crimes using the identity of another person.

(4) Identity theft is costly to the marketplace and to consumers.

(5) Victims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of possible misuse of a person's personal information is imperative.

Acts 2005, No. 499, §1, eff. Jan. 1, 2006.

§3073. DEFINITIONS

As used in this Chapter, the following terms shall have the following meanings:

(1) "Agency" means the state, a political subdivision of the state, and any officer, agency, board, commission, department or similar body of the state or any political subdivision of the state.

(2) "Breach of the security of the system" means the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by an agency or person. Good faith acquisition of personal information by an employee or agent of an agency or person for the purposes of the agency or person is not a breach of the security of the system, provided that the personal information is not used for, or is subject to, unauthorized disclosure.

(3) "Person" means any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity.

(4) (a) "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 the name or the data element is not encrypted or redacted:
    (i) Social security number.
    (ii) Driver's license number.
    (iii) 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.

(b) "Personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Acts 2005, No. 499, §1, eff. Jan. 1, 2006.

§3074. DISCLOSURE UPON BREACH IN THE SECURITY OF PERSONAL INFORMATION; NOTIFICATION REQUIREMENTS; EXEMPTION

A. Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall, following discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

B. Any agency or person that maintains computerized data that includes personal information that the agency or person does not own shall notify the owner or licensee of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of security of the system.

C. The notification required pursuant to Subsections A and B of this Section shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in Subsection D of this Section, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.

D. If a law enforcement agency determines that the notification required under this Section would impede a criminal investigation, such notification may be delayed until such law enforcement agency determines that the notification will no longer compromise such investigation.

E. Notification may be provided by one of the following methods:

(1) Written notification.

(2) Electronic notification, if the notification provided is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001.

(3) Substitute notification, if an agency or person demonstrates that the cost of providing notification would exceed two hundred fifty thousand dollars, or that the affected class of persons to be notified exceeds five hundred thousand, or the agency or person does not have sufficient contact information. Substitute notification shall consist of all of the following:

(a) E-mail notification when the agency or person has an e-mail address for the subject persons.

(b) Conspicuous posting of the notification on the Internet site of the agency or person, if an Internet site is maintained.

(c) Notification to major statewide media.

F. Notwithstanding Subsection E of this Section, an agency or person that maintains a notification procedure as part of its information security policy for the treatment of personal information which is otherwise consistent with the timing requirements of this Section shall be deemed to be in compliance with the notification requirements of this Section if the agency or person notifies subject persons in accordance with the policy and procedure in the event of a breach of security of the system.

G. Notification under this title[2] is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers.

Acts 2005, No. 499, §1, eff. Jan. 1, 2006.

---

2. As appears in enrolled bill. Should be “Section”.

§3075. RECOVERY OF DAMAGES

A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information.

Acts 2005, No. 499, §1, eff. Jan. 1, 2006.

§3076. FINANCIAL INSTITUTION; COMPLIANCE

A financial institution that is subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the office of the comptroller of the currency and the office of thrift supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance with this Chapter.

Acts 2005, No. 499, §1, eff. Jan. 1, 2006.

§3077. RULEMAKING

The provisions of this Chapter shall not take effect until rules are promulgated by the attorney general's office.

Acts 2005, No. 499, §1, eff. Jan. 1, 2006.

MAINE

§1346. SHORT TITLE

This chapter may be known and cited as "the Notice of Risk to Personal Data Act." [2005, c. 379, §1 (new); §4 (aff).]

PL 2005, Ch. 379, §1 (NEW).

PL 2005, Ch. 379, §4 (AFF).

§1347. DEFINITIONS (CONTAINS TEXT WITH VARYING EFFECTIVE DATES)

As used in this chapter, unless the context otherwise indicates, the following terms have the following meanings. [2005, c. 379, §1 (new); §4 (aff).]

1. **(TEXT EFFECTIVE UNTIL 1/31/07) 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.
   [2005, c. 379, §1 (new); §4 (aff).]

1. **(TEXT EFFECTIVE 1/31/07) 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 a person. Good faith acquisition of personal information by an employee or agent of 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.
   [2005, c. 583, §1 (amd); §14 (aff).]

2. **Encryption.** "Encryption" means the disguising of data using generally accepted practices.
   [2005, c. 379, §1 (new); §4 (aff).]

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.
   [2005, c. 379, §1 (new); §4 (aff).]

4. **Notice.** "Notice" means:
   A. Written notice; [2005, c. 379, §1 (new); §4 (aff).]
   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 [2005, c. 379, §1 (new); §4 (aff).]
   C. (TEXT EFFECTIVE UNTIL 1/31/07) 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.

   [2005, c. 379, §1 (new); §4 (aff).]

C. (TEXT EFFECTIVE 1/31/07) Substitute notice, if the 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 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 person has e-mail addresses for the individuals to be notified;

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

(3) Notification to major statewide media.

[2005, c. 583, §2 (amd); §14 (aff).]

[2005, c. 379, §1 (new); §4 (aff); c. 583, §2 (amd); §14 (aff).]

5. **(TEXT EFFECTIVE UNTIL 1/31/07) 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.

[2005, c. 379, §1 (new); §4 (aff).]

5. **(TEXT EFFECTIVE 1/31/07) Person.** "Person" means an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity, including agencies of State Government, the University of Maine System, the Maine Community College System, Maine Maritime Academy and private colleges and universities. "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.

[2005, c. 583, §3 (amd); §14 (aff).]

6. **(TEXT EFFECTIVE UNTIL 1/31/07) 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; [2005, c. 379, §1 (new); §4 (aff).]

B. Driver's license number or state identification card number; [2005, c. 379, §1 (new); §4 (aff).]

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; [2005, c. 379, §1 (new); §4 (aff).]

D. Account passwords or personal identification numbers or other access codes; or [2005, c. 379, §1 (new); §4 (aff).]

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. [2005, c. 379, §1 (new); §4 (aff).]

"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.

[2005, c. 379, §1 (new); §4 (aff).]

6. **(TEXT EFFECTIVE 1/31/07) 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; [2005, c. 379, §1 (new); §4 (aff).]

B. Driver's license number or state identification card number; [2005, c. 379, §1 (new); §4 (aff).]

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; [2005, c. 379, §1 (new); §4 (aff).]

D. Account passwords or personal identification numbers or other access codes; or [2005, c. 379, §1 (new); §4 (aff).]

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. [2005, c. 379, §1 (new); §4 (aff).]

"Personal information" does not include information from 3rd-party claims databases maintained by property and casualty insurers or publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

[2005, c. 583, §4 (amd); §14 (aff).]

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

[2005, c. 379, §1 (new); §4 (aff).]

8. **(TEXT EFFECTIVE UNTIL 1/31/07) 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.

[2005, c. 379, §1 (new); §4 (aff).]

8. **(TEXT EFFECTIVE 1/31/07) Unauthorized person.** "Unauthorized person" means a person who does not have authority or permission of a person maintaining personal information to access personal information maintained by the person or who obtains access to such information by fraud, misrepresentation, subterfuge or similar deceptive practices.

[2005, c. 583, §5 (amd); §14 (aff).]

PL 2005, Ch. 379, §1 (NEW).

PL 2005, Ch. 379, §4 (AFF).

PL 2005, Ch. 583, §1-5 (AMD).

PL 2005, Ch. 583, §14 (AFF).

§1348. SECURITY BREACH NOTICE REQUIREMENTS (CONTAINS TEXT WITH VARYING EFFECTIVE DATES)

1. **(TEXT EFFECTIVE UNTIL 1/31/07) 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.

[2005, c. 379, §1 (new); §4 (aff).]

1. **(TEXT EFFECTIVE 1/31/07) Notification to residents.** The following provisions apply to notification to residents by information brokers and other persons.

A. If an information broker that maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the information broker shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and 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 has been, or is reasonably believed to have been, acquired by an unauthorized person. [2005, c. 583, §6 (new); §14 (aff).]

B. If any other person who maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the person shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and 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 if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur. [2005, c. 583, §6 (new); §14 (aff).]

The notices 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.

[2005, c. 583, §6 (rpr); §14 (aff).]

2. **(TEXT EFFECTIVE UNTIL 1/31/07) 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.

[2005, c. 379, §1 (new); §4 (aff).]

2. **(TEXT EFFECTIVE 1/31/07) Notification to person maintaining personal information.** A 3rd-party entity that maintains, on behalf of a person, computerized data that includes personal information that the 3rd-party entity does not own shall notify the person maintaining personal information 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.

[2005, c. 583, §7 (amd); §14 (aff).]

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.

[2005, c. 379, §1 (new); §4 (aff).]

4. **(TEXT EFFECTIVE UNTIL 1/31/07) 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).

[2005, c. 379, §1 (new); §4 (aff).]

4. **(TEXT EFFECTIVE 1/31/07) Notification to consumer reporting agencies.** If 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 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). Notification must include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach.

[2005, c. 583, §8 (amd); §14 (aff).]

5. **(TEXT EFFECTIVE UNTIL 1/31/07) 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.

[2005, c. 379, §1 (new); §4 (aff).]

5. **(TEXT EFFECTIVE 1/31/07) Notification to state regulators.** When notice of a breach of the security of the system is required under subsection 1, the person shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the Attorney General.
[2005, c. 583, §9 (amd); §14 (aff).]
PL 2005, Ch. 379, §1 (NEW).
PL 2005, Ch. 379, §4 (AFF).
PL 2005, Ch. 583, §14 (AFF).
PL 2005, Ch. 583, §6-9 (AMD).

§1349. ENFORCEMENT; PENALTIES (CONTAINS TEXT WITH VARYING EFFECTIVE DATES)

1. **(TEXT EFFECTIVE UNTIL 1/31/07) 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.
[2005, c. 379, §1 (new); §4 (aff).]

1. **(TEXT EFFECTIVE 1/31/07) Enforcement.** The appropriate state regulators within the Department of Professional and Financial Regulation shall enforce this chapter for any person that is licensed or regulated by those regulators. The Attorney General shall enforce this chapter for all other persons.
[2005, c. 583, §10 (amd); §14 (aff).]

2. **(TEXT EFFECTIVE UNTIL 1/31/07) 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; [2005, c. 379, §1 (new); §4 (aff).]
   B. Equitable relief; or [2005, c. 379, §1 (new); §4 (aff).]
   C. Enjoinment from further violations of this chapter. [2005, c. 379, §1 (new); §4 (aff).]
   [2005, c. 379, §1 (new); §4 (aff).]

2. **(TEXT EFFECTIVE 1/31/07) Civil violation.** 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 person is in violation of this chapter, except that this paragraph does not apply to State Government, the University of Maine System, the Maine Community College System or Maine Maritime Academy; [2005, c. 583, §11 (amd); §14 (aff).]
   B. Equitable relief; or [2005, c. 379, §1 (new); §4 (aff).]
   C. Enjoinment from further violations of this chapter. [2005, c. 379, §1 (new); §4 (aff).]
   [2005, c. 583, §11 (amd); §14 (aff).]

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.
[2005, c. 379, §1 (new); §4 (aff).]

4. **(TEXT EFFECTIVE 1/31/07) Exceptions.** A person that complies with the security breach notification requirements of rules, regulations, procedures or guidelines established pursuant to federal law or the law of this State is deemed to be in compliance with the requirements of this chapter as long as the law, rules, regulations or guidelines provide for notification procedures at least as protective as the notification requirements of this chapter.
[2005, c. 583, §12 (new); §14 (aff).]
PL 2005, Ch. 379, §1 (NEW).
PL 2005, Ch. 379, §4 (AFF).
PL 2005, Ch. 583, §10-12 (AMD).
PL 2005, Ch. 583, §14 (AFF).

§1350-A. RULES; EDUCATION AND COMPLIANCE (CONTAINS TEXT WITH VARYING EFFECTIVE DATES)

(WHOLE SECTION TEXT EFFECTIVE 1/31/07)

The following provisions govern rules and education and compliance. [2005, c. 583, §13 (new); §14 (aff).]

1. **Rules.** With respect to persons under the jurisdiction of the regulatory agencies of the Department of Professional and Financial Regulation, the appropriate state regulators within that department may adopt rules as necessary for the administration and implementation of this chapter. With respect to all other persons, the Attorney General may adopt rules as necessary for the administration and implementation of this chapter. Rules adopted pursuant to this subsection are routine technical rules as defined in Title 5, chapter 375, subchapter 2-A.

   [2005, c. 583, §13 (new); §14 (aff).]

2. **Education and compliance.** The appropriate state regulators within the Department of Professional and Financial Regulation shall undertake reasonable efforts to inform persons under the department's jurisdiction of their responsibilities under this chapter. With respect to all other persons, the Attorney General shall undertake reasonable efforts to inform such persons of their responsibilities under this chapter.

   [2005, c. 583, §13 (new); §14 (aff).]

   PL 2005, Ch. 583, §13 (NEW).

   PL 2005, Ch. 583, §14 (AFF).

MINNESOTA

DATA WAREHOUSES; DISCLOSURE OF PERSONAL INFORMATION

325E.61 DATA WAREHOUSES; NOTICE REQUIRED FOR CERTAIN DISCLOSURES.

Subdivision 1. **Disclosure of personal information; notice required.**

(a) Any person or business that conducts business in this state, and that owns or licenses 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 this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (c), or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.

(b) Any person or business that maintains 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 and section 13.055, subdivision 6, may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation.

(d) For purposes of this section and section 13.055, subdivision 6, "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 system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section and section 13.055, subdivision 6, "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 the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:

  (1) Social Security number;

  (2) driver's license number or Minnesota identification card number; or

  (3) account number or 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 and section 13.055, subdivision 6, "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 and section 13.055, subdivision 6, "notice" may be provided by one of the following methods:

  (1) written notice to the most recent available address the person or business has in its records;

  (2) electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures in United States Code, title 15, section 7001; or

(3) substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $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 must consist of all of the following:

(i) e-mail notice when the person or business has an e-mail address for the subject persons;

(ii) conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and

(iii) notification to major statewide media.

(h) Notwithstanding paragraph (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 section and section 13.055, subdivision 6, shall be deemed to be in compliance with the notification requirements of this section and section 13.055, subdivision 6, if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Subd. 2. **Coordination with consumer reporting agencies.** If a person discovers circumstances requiring notification under this section and section 13.055, subdivision 6, of more than 500 persons at one time, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.

Subd. 3. **Waiver prohibited.** Any waiver of the provisions of this section and section 13.055, subdivision 6, is contrary to public policy and is void and unenforceable.

Subd. 4. **Exemption.** This section and section 13.055, subdivision 6, do not apply to any "financial institution" as defined by United States Code, title 15, section 6809(3).

Subd. 5. [Renumbered 13.055, subd 6]

Subd. 6. **Remedies and enforcement.** The attorney general shall enforce this section and section 13.055, subdivision 6, under section 8.31.

History: *2005 c 167 s 1; 2006 c 212 art 1 s 17,24; 2006 c 233 s 7,8*

MONTANA

30-14-1701. *(EFFECTIVE MARCH 1, 2006)* PURPOSE. THE PURPOSE OF 30-14-1701 THROUGH 30-14-1705 IS TO ENHANCE THE PROTECTION OF INDIVIDUAL PRIVACY AND TO IMPEDE IDENTITY THEFT AS PROHIBITED BY 45-6-332.

30-14-1702. *(EFFECTIVE MARCH 1, 2006)* DEFINITIONS. AS USED IN 30-14-1701 THROUGH 30-14-1705, UNLESS THE CONTEXT REQUIRES OTHERWISE, THE FOLLOWING DEFINITIONS APPLY:

(1) (a) "Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or any other country or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records. The term also includes industries regulated by the public service commission or under Title 30, chapter 10.

(b) The term does not include industries regulated under Title 33.

(2) "Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

(3) "Individual" means a natural person.

(4) "Personal information" means an individual's name, signature, address, or telephone number, in combination with one or more additional pieces of information about the individual, consisting of the individual's passport number, driver's license or state identification number, insurance policy number, bank account number, credit card number, debit card number, passwords or personal identification numbers required to obtain access to the individual's finances, or any other financial information as provided by rule. A social security number, in and of itself, constitutes personal information.

(5) (a) "Records" means any material, regardless of the physical form, on which personal information is recorded.

(b) The term does not include publicly available directories containing personal information that an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

30-14-1703. *(EFFECTIVE MARCH 1, 2006)* RECORD DESTRUCTION. A BUSINESS SHALL TAKE ALL REASONABLE STEPS TO DESTROY OR ARRANGE FOR THE DESTRUCTION OF A CUSTOMER'S RECORDS WITHIN ITS CUSTODY OR CONTROL CONTAINING PERSONAL INFORMATION THAT IS NO LONGER NECESSARY TO BE RETAINED BY THE BUSINESS BY SHREDDING, ERASING, OR OTHERWISE MODIFYING THE PERSONAL INFORMATION IN THOSE RECORDS TO MAKE IT UNREADABLE OR UNDECIPHERABLE.

History: En. Sec. 6, Ch. 518, L. 2005.

30-14-1704. (*EFFECTIVE MARCH 1, 2006*) COMPUTER SECURITY BREACH.

(1) Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3), or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(2) 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 system immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person.

(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay in notification. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section, the following definitions apply:

(a) "Breach of the security of the data system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. 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 data system, provided that the personal information is not used or subject to further unauthorized disclosure.

(b) (i) "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:

(A) social security number;

(B) driver's license number or state identification card number;

(C) account number or 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.

(ii) Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(5) (a) For purposes of this section, notice may be provided by one of the following methods:

(i) written notice;

(ii) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001;

(iii) telephonic notice; or

(iv) substitute notice, if the person or business demonstrates that:

(A) the cost of providing notice would exceed $250,000;

(B) the affected class of subject persons to be notified exceeds 500,000; or

(C) the person or business does not have sufficient contact information.

(b) Substitute notice must consist of the following:

(i) an electronic mail notice when the person or business has an electronic mail address for the subject persons; and

(ii) conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; or

(iii) notification to applicable local or statewide media.

(6) Notwithstanding subsection (5), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and that does not unreasonably delay notice is considered 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 data system.

(7) If a business discloses a security breach to any individual pursuant to this section and gives a notice to the individual that suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual. The coordination may not unreasonably delay the notice to the affected individuals.

History: En. Sec. 7, Ch. 518, L. 2005.

30-14-1705. *(EFFECTIVE MARCH 1, 2006)* DEPARTMENT TO RESTRAIN UNLAWFUL ACTS -- PENALTY.

(1) Whenever the department has reason to believe that a person has violated this part and that proceeding would be in the public interest, the department may bring an action in the name of the state against the person to restrain by temporary or permanent injunction or temporary restraining order the use of the unlawful method, act, or practice upon giving appropriate notice to that person pursuant to 30-14-111(2).

(2) The provisions of 30-14-111(3) and (4) and 30-14-112 through 30-14-115 apply to this part.

(3) A violation of this part is a violation of 30-14-103, and the penalties for a violation of this part are as provided in 30-14-142.

History: En. Sec. 8, Ch. 518, L. 2005.

NEBRASKA

SECTION 87-801 ***ACT, HOW CITED.***

Sections 87-801 to 87-807 shall be known and may be cited as the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006.

Source: Laws 2006, LB 876, § 1. Revised Statutes Cumulative Supplement, 2006

SECTION 87-802 ***TERMS, DEFINED.***

For purposes of the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006:

(1) Breach of the security of the system means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency is not a breach of the security of the system;

(2) Commercial entity includes a corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency, or instrumentality, or any other legal entity, whether for profit or not for profit;

(3) Encrypted means converted by use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key;

(4) Notice means:

  (a) Written notice;

  (b) Telephonic notice;

  (c) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001, as such section existed on January 1, 2006;

  (d) Substitute notice, if the individual or commercial entity required to provide notice demonstrates that the cost of providing notice will exceed seventy-five thousand dollars, that the affected class of Nebraska residents to be notified exceeds one hundred thousand residents, or that the individual or commercial entity does not have sufficient contact information to provide notice. Substitute notice under this subdivision requires all of the following:

    (i) Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents;

    (ii) Conspicuous posting of the notice on the web site of the individual or commercial entity if the individual or commercial entity maintains a web site; and

    (iii) Notice to major statewide media outlets; or

  (e) Substitute notice, if the individual or commercial entity required to provide notice has ten employees or fewer and demonstrates that the cost of providing notice will exceed ten thousand dollars. Substitute notice under this subdivision requires all of the following:

    (i) Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents;

    (ii) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the individual or commercial entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;

(iii) Conspicuous posting of the notice on the web site of the individual or commercial entity if the individual or commercial entity maintains a web site; and

(iv) Notification to major media outlets in the geographic area in which the individual or commercial entity is located;

(5) Personal information means a Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:

(a) Social security number;

(b) Motor vehicle operator's license number or state identification card number;

(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account;

(d) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or

(e) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records; and

(6) Redact means to alter or truncate data such that no more than the last four digits of a social security number, motor vehicle operator's license number, state identification card number, or account number is accessible as part of the personal information.

Source: Laws 2006, LB 876, § 2. Revised Statutes Cumulative Supplement, 2006

SECTION 87-803 ***BREACH OF SECURITY; INVESTIGATION; NOTICE TO RESIDENT.***

(1) An individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident. Notice shall be made as soon as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

(2) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach if use of personal information about a Nebraska resident for an unauthorized purpose occurred or is reasonably likely to occur. Cooperation includes, but is not limited to, sharing with the owner or licensee information relevant to the breach, not including information proprietary to the individual or commercial entity.

(3) Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.

Source: Laws 2006, LB 876, § 3. Revised Statutes Cumulative Supplement, 2006

SECTION 87-804 ***COMPLIANCE WITH NOTICE REQUIREMENTS; MANNER.***

(1) An individual or a commercial entity that maintains its own notice procedures which are part of an information security policy for the treatment of personal information and which are otherwise consistent with the timing requirements of section 87-803, is deemed to be in compliance with the notice requirements of section 87-803 if the individual or the commercial entity notifies affected Nebraska residents in accordance with its notice procedures in the event of a breach of the security of the system.

(2) An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with section 87-803 if the individual or commercial entity notifies affected Nebraska residents in accordance with the maintained procedures in the event of a breach of the security of the system.

Source: Laws 2006, LB 876, ? 4. Revised Statutes Cumulative Supplement, 2006

SECTION 87-805 ***WAIVER; VOID AND UNENFORCEABLE.***

Any waiver of the provisions of the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 is contrary to public policy and is void and unenforceable.

Source: Laws 2006, LB 876, § 5. Revised Statutes Cumulative Supplement, 2006

SECTION 87-806 ***ATTORNEY GENERAL; POWERS.***

For purposes of the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, the Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of the act.

Source: Laws 2006, LB 876, § 6. Revised Statutes Cumulative Supplement, 2006

SECTION 87-807 ***ACT; APPLICABILITY.***

The Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 applies to the discovery of or notification pertaining to a breach of the security of the system that occurs on or after July 14, 2006.

Source: Laws 2006, LB 876, § 7. Revised Statutes Cumulative Supplement, 2006

NEVADA

GENERAL PROVISIONS

NRS 603A.010 Definitions. As used in this chapter, unless the context otherwise requires, the words and terms defined in NRS 603A.020, 603A.030 and 603A.040 have the meanings ascribed to them in those sections.
(Added to NRS by 2005, 2503)

NRS 603A.020 "Breach of the security of the system data" defined. "Breach of the security of the system data" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector. The term does not include the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, so long as the personal information is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure.
(Added to NRS by 2005, 2503)

NRS 603A.030 "Data collector" defined. "Data collector" means any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information.
(Added to NRS by 2005, 2504)

NRS 603A.040 "Personal information" defined. "Personal information" means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:

1. Social security number.
2. Driver's license number or identification card number.
3. Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.

→ The term does not include publicly available information that is lawfully made available to the general public.
(Added to NRS by 2005, 2504; A 2005, 22nd Special Session, 109)

APPLICABILITY

NRS 603A.100 Waiver of provisions of chapter prohibited. Any waiver of the provisions of this chapter is contrary to public policy, void and unenforceable.
(Added to NRS by 2005, 2506)

REGULATION OF BUSINESS PRACTICES

NRS 603A.200 DESTRUCTION OF CERTAIN RECORDS.

1. A business that maintains records which contain personal information concerning the customers of the business shall take reasonable measures to ensure the destruction of those records when the business decides that it will no longer maintain the records.
2. As used in this section:
   (a) "Business" means a proprietorship, corporation, partnership, association, trust, unincorporated organization or other enterprise doing business in this State.

(b) "Reasonable measures to ensure the destruction" means any method that modifies the records containing the personal information in such a way as to render the personal information contained in the records unreadable or undecipherable, including, without limitation:

(1) Shredding of the record containing the personal information; or

(2) Erasing of the personal information from the records.

(Added to NRS by 2005, 2504)

NRS 603A.210 SECURITY MEASURES.

1. A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.
2. A contract for the disclosure of the personal information of a resident of this State which is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.
3. If a state or federal law requires a data collector to provide greater protection to records that contain personal information of a resident of this State which are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this section.

(Added to NRS by 2005, 2504)

NRS 603A.220 DISCLOSURE OF BREACH OF SECURITY OF SYSTEM DATA; METHODS OF DISCLOSURE.

1. Any data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection 3, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.
2. Any data collector that maintains computerized data which includes personal information that the data collector does not own shall notify the owner or licensee of the information of any breach of the security of the system data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
3. 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 must be made after the law enforcement agency determines that the notification will not compromise the investigation.
4. For purposes of this section, except as otherwise provided in subsection 5, the notification required by this section may be provided by one of the following methods:
   (a) Written notification.
   (b) Electronic notification, if the notification provided is consistent with the provisions of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq.
   (c) Substitute notification, if the data collector demonstrates that the cost of providing notification would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000 or the data collector does not have sufficient contact information. Substitute notification must consist of all the following:
      (1) Notification by electronic mail when the data collector has electronic mail addresses for the subject persons.

(2) Conspicuous posting of the notification on the Internet website of the data collector, if the data collector maintains an Internet website.

(3) Notification to major statewide media.

5. A data collector which:

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

(b) Is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq., shall be deemed to be in compliance with the notification requirements of this section.

6. If a data collector determines that notification is required to be given pursuant to the provisions of this section to more than 1,000 persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency, as that term is defined in 15 U.S.C. § 1681a(p), that compiles and maintains files on consumers on a nationwide basis, of the time the notification is distributed and the content of the notification.

(Added to NRS by 2005, 2504)

REMEDIES AND PENALTIES

NRS 603A.900 Civil action. A data collector that provides the notification required pursuant to NRS 603A.220 may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. A data collector that prevails in such an action may be awarded damages which may include, without limitation, the reasonable costs of notification, reasonable attorney's fees and costs and punitive damages when appropriate. The costs of notification include, without limitation, labor, materials, postage and any other costs reasonably related to providing the notification.

(Added to NRS by 2005, 2506)

NRS 603A.910 Restitution. In addition to any other penalty provided by law for the breach of the security of the system data maintained by a data collector, the court may order a person who is convicted of unlawfully obtaining or benefiting from personal information obtained as a result of such breach to pay restitution to the data collector for the reasonable costs incurred by the data collector in providing the notification required pursuant to NRS 603A.220, including, without limitation, labor, materials, postage and any other costs reasonably related to providing such notification.

(Added to NRS by 2005, 2506)

NRS 603A.920 Injunction. If the Attorney General or a district attorney of any county has reason to believe that any person is violating, proposes to violate or has violated the provisions of this chapter, he may bring an action against that person to obtain a temporary or permanent injunction against the violation.

(Added to NRS by 2005, 2506)

NEW HAMPSHIRE

359-C:19 DEFINITIONS. –

In this subdivision:

I. "Computerized data" means personal information stored in an electronic format.

II. "Encrypted" means the transformation of data through the use of an algorithmic process into a form for which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements completely unreadable or unusable. Data shall not be considered to be encrypted for purposes of this subdivision if it is acquired in combination with any required key, security code, access code, or password that would permit access to the encrypted data.

III. "Person" means an individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state.

IV. (a) "Personal information" means an individual's first name or 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 other government identification number.

(3) Account number, credit card number, 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.

(b) "Personal information" shall not include information that is lawfully made available to the general public from federal, state, or local government records.

V. "Security breach" means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business shall not be considered a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Source. 2006, 242:1, eff. Jan. 1, 2007.

359-C:20 NOTIFICATION OF SECURITY BREACH REQUIRED. –

I. (a) Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision.

(b) Any person engaged in trade or commerce that is subject to RSA 358-A:3, I shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office. The notice shall include the anticipated date of the notice to the individuals and the approximate number of individuals in this state who will be notified. Nothing in this section shall be construed to require the person to provide to any regulator or the New Hampshire attorney general's office the names of the individuals entitled to receive the notice or any personal information relating to them. The disclosure shall be made to affected individuals as quickly as possible, after the determination required under this section.

(c) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was acquired by an unauthorized person. Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential or business information or trade secrets.

II. Notification pursuant to paragraph I may be delayed if a law enforcement agency, or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security.

III. The notice required under this section shall be provided by one of the following methods:

(a) Written notice.

(b) Electronic notice, if the agency or business' primary means of communication with affected individuals is by electronic means.

(c) Telephonic notice, provided that a log of each such notification is kept by the person or business who notifies affected persons.

(d) Substitute notice, if the person demonstrates that the cost of providing notice would exceed $5,000, that the affected class of subject individuals to be notified exceeds 1,000, or the person does not have sufficient contact information or consent to provide notice pursuant to subparagraphs I(a)-I(c). Substitute notice shall consist of all of the following:

(1) E-mail notice when the person has an e-mail address for the affected individuals.

(2) Conspicuous posting of the notice on the person's business website, if the person maintains one.

(3) Notification to major statewide media.

(e) Notice pursuant to the person's internal notification procedures maintained as part of an information security policy for the treatment of personal information.

IV. Notice under this section shall include at a minimum:

(a) A description of the incident in general terms.

(b) The approximate date of breach.

(c) The type of personal information obtained as a result of the security breach.

(d) The telephonic contact information of the person subject to this section.

V. Any person engaged in trade or commerce that is subject to RSA 358-A:3, I which maintains procedures for security breach notification pursuant to the laws, rules, regulations, guidances, or guidelines issued by a state or federal regulator shall be deemed to be in compliance with this subdivision if it acts in accordance with such laws, rules, regulations, guidances, or guidelines.

VI. (a) If a person is required to notify more than 1,000 consumers of a breach of security pursuant to this section, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. section 1681a(p), of the anticipated date of the notification to the consumers, the approximate number of consumers who will be notified, and the content of the notice. Nothing in this paragraph shall be construed to require the person to provide to any consumer reporting agency the names of the consumers entitled to receive the notice or any personal information relating to them.

(b) Subparagraph (a) shall not apply to a person who is subject to Title V of the Gramm, Leach-Bliley Act, 15 U.S.C. section 6801 et seq.

Source. 2006, 242:1, eff. Jan. 1, 2007.

359-C:21 VIOLATION. –

I. Any person injured by any violation under this subdivision may bring an action for damages and for such equitable relief, including an injunction, as the court deems necessary and proper. If the court finds for the plaintiff, recovery shall be in the amount of actual damages. If the court finds that the act or practice was a willful or knowing violation of this chapter, it shall award as much as 3 times, but not less than 2 times, such amount. In addition, a prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees, as determined by the court. Any attempted waiver of the right to the damages set forth in this paragraph shall be void and unenforceable. Injunctive relief shall be available to private individuals under this chapter without bond, subject to the discretion of the court.

II. The New Hampshire attorney general's office shall enforce the provisions of this subdivision pursuant to RSA 358-A:4.

III. The burden shall be on the person responsible for the determination under RSA 359-C:20, I to demonstrate compliance with this subdivision.

Source. 2006, 242:1, eff. Jan. 1, 2007.

NEW JERSEY

56:8-161 DEFINITIONS RELATIVE TO SECURITY OF PERSONAL INFORMATION.

As used in sections 10 through 15 of this amendatory and supplementary act:

"Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

"Business" means a sole proprietorship, partnership, corporation, association, or other entity, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this State, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution.

"Communicate" means to send a written or other tangible record or to transmit a record by any means agreed upon by the persons sending and receiving the record.

"Customer" means an individual who provides personal information to a business.

"Individual" means a natural person.

"Internet" means the international computer network of both federal and non-federal interoperable packet switched data networks.

"Personal information" means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or 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. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

For the purposes of sections 10 through 15 of this amendatory and supplementary act, personal information shall 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.

"Private entity" means any individual, corporation, company, partnership, firm, association, or other entity, other than a public entity.

"Public entity" includes the State, and any county, municipality, district, public authority, public agency, and any other political subdivision or public body in the State. For the purposes of sections 10 through 15 of this amendatory and supplementary act, public entity does not include the federal government.

"Publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public.

"Records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed, or electromagnetically transmitted. Records does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed.

L.2005,c.226,s.10.

56:8-162 METHODS OF DESTRUCTION OF CERTAIN CUSTOMER RECORDS.

A business or public entity shall destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means.

L.2005,c.226,s.11.

56:8-163 DISCLOSURE OF BREACH OF SECURITY TO CUSTOMERS.

a. Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.

b. Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

c. (1) Any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

(2) The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.

d. 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 101 of the federal "Electronic Signatures in Global and National Commerce Act" (15 U.S.C. s.7001); or

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

(a) E-mail notice when the business or public entity has an e-mail address;

(b) Conspicuous posting of the notice on the Internet web site page of the business or public entity, if the business or public entity maintains one; and

(c) Notification to major Statewide media.

e. Notwithstanding subsection d. of this section, a business or public entity 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 requirements of this section, shall be deemed to be in compliance with the notification requirements of this section if the business or public entity notifies subject customers in accordance with its policies in the event of a breach of security of the system.

f. In addition to any other disclosure or notification required under this section, in the event that a business or public entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the business or public entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the federal "Fair Credit Reporting Act" (15 U.S.C. s.1681a), of the timing, distribution and content of the notices. L.2005,c.226,s.12.

NEW YORK

§ 899-AA. NOTIFICATION; PERSON WITHOUT VALID AUTHORIZATION HAS ACQUIRED PRIVATE INFORMATION.

1. As used in this section, the following terms shall have the following meanings:
   (a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;
   (b) "Private information" shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:
      (1) social security number;
      (2) driver's license number or non-driver identification card number; or
      (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;

   "Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.
   (c) "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

   In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:
      (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
      (2) indications that the information has been downloaded or copied; or
      (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
   (d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to any person or business required to make a notification under subdivision two of this section.
2. Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. 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 four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

3. Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.
4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.
5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:
   (a) written notice;
   (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.
   (c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or
   (d) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:
      (1) e-mail notice when such business has an e-mail address for the subject persons;
      (2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and
      (3) notification to major statewide media.
6. (a) whenever the attorney general shall believe from evidence satisfactory to him that there is a violation of this article he may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to ten dollars per instance of failed notification, provided that the latter amount shall not exceed one hundred fifty thousand dollars.
   (b) the remedies provided by this section shall be in addition to any other lawful remedy available.
   (c) no action may be brought under the provisions of this section unless such action is commenced within two years immediately after the date of the act complained of or the date of discovery of such act.
7. Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

8. (a) In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

   (b) In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

9. The provisions of this section shall be exclusive and shall preempt any provisions of local law, ordinance or code, and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section.

NORTH CAROLINA

§ 75-65. PROTECTION FROM SECURITY BREACHES.

(a) Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. For the purposes of this section, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.

(b) Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section.

(c) The notice required by this section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

(d) The notice shall be clear and conspicuous. The notice shall include a description of the following:
   (1) The incident in general terms.
   (2) The type of personal information that was subject to the unauthorized access and acquisition.
   (3) The general acts of the business to protect the personal information from further unauthorized access.
   (4) A telephone number that the person may call for further information and assistance, if one exists.
   (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

(e) For purposes of this section, notice to affected persons may be provided by one of the following methods:
   (1) Written notice.
   (2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001.
   (3) Telephonic notice provided that contact is made directly with the affected persons.

(4) Substitute notice, if the 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 if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2), or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

a. E-mail notice when the business has an electronic mail address for the subject persons.

b. Conspicuous posting of the notice on the Web site page of the business, if one is maintained.

c. Notification to major statewide media.

(f) In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.

(g) Any waiver of the provisions of this Article is contrary to public policy and is void and unenforceable.

(h) A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance with this section.

(i) A violation of this section is a violation of G.S. 75 1.1. No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation.

(j) Causes of action arising under this Article may not be assigned. (2005 414, s. 1.)

NORTH DAKOTA

CHAPTER 51-30

NOTICE OF SECURITY BREACH FOR PERSONAL INFORMATION

51-30-01. DEFINITIONS.

In this chapter, unless the context or subject matter otherwise requires:

1. "Breach of the security system" means unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or data bases unreadable or unusable. Good-faith acquisition of personal information by an employee or agent of the person is not a breach of the security of the system, if the personal information is not used or subject to further unauthorized disclosure.
2. a. "Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted:
   (1) The individual's social security number;
   (2) The operator's license number assigned to an individual by the department of transportation under section 39-06-14;
   (3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1;
   (4) The individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts;
   (5) The individual's date of birth;
   (6) The maiden name of the individual's mother;
   (7) An identification number assigned to the individual by the individual's employer; or
   (8) The individual's digitized or other electronic signature.

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

51-30-02. NOTICE TO CONSUMERS.

Any person that conducts business in this state, 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 the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.

51-30-03. NOTICE TO OWNER OR LICENSEE OF PERSONAL INFORMATION.

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

51-30-04. DELAYED NOTICE.

The notification required by this chapter may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this chapter must be made after the law enforcement agency determines that the notification will not compromise the investigation.

51-30-05. METHOD OF NOTICE.

Notice under this chapter 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; or
3. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person does not have sufficient contact information. Substitute notice consists of the following:
   a. E-mail notice when the person has an e-mail address for the subject persons;
   b. Conspicuous posting of the notice on the person's web site page, if the person maintains one; and
   c. Notification to major statewide media.

51-30-06. ALTERNATE COMPLIANCE.

Notwithstanding section 51-30-05, a person 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 chapter is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system. A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice is deemed to be in compliance with this chapter.

51-30-07. ENFORCEMENT - POWERS - REMEDIES - PENALTIES.

The attorney general may enforce this chapter. The attorney general, in enforcing this chapter, has all the powers provided in chapter 51-15 and may seek all the remedies in chapter 51-15. A violation of this chapter is deemed a violation of chapter 51-15. The remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties under chapter 51-15, or otherwise provided by law.

OHIO

§ 1349.19. DISCLOSURE OR NOTIFICATION OF BREACH OF SECURITY OF COMPUTERIZED PERSONAL INFORMATION SYSTEM.

(A) As used in this section:

(1) (a) "Breach of the security of the system" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.

(b) For purposes of division (A)(1)(a) of this section:

(i) Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security of the system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure.

(ii) Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a breach of the security of the system.

(2) "Business entity" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, or the parent or subsidiary of a financial institution.

(3) "Consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" means a consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's creditworthiness, credit standing, or credit capacity, each of the following regarding consumers residing nationwide:

(a) Public record information;

(b) Credit account information from persons who furnish that information regularly and in the ordinary course of business.

(4) "Encryption" means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

(5) "Individual" means a natural person.

(6) "Person" has the same meaning as in section 1.59 of the Revised Code, except that "person" includes a business entity only if the business entity conducts business in this state.

(7) (a) "Personal information" means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:

(i) Social security number;

(ii) Driver's license number or state identification card number;

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

(b) "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 any of the following media that are widely distributed:

(i) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television;

(ii) Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media described in division (A)(7)(b)(i) of this section;

(iii) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation;

(iv) Any type of media similar in nature to any item, entity, or activity identified in division (A)(7)(b)(i), (ii), or (iii) of this section.

(8) "Record" means any information that is stored in an electronic medium and is retrievable in perceivable form. "Record" does not include any publicly available directory containing information an individual voluntarily has consented to have publicly disseminated or listed, such as name, address, or telephone number.

(9) "Redacted" means altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data.

(10) "System" means any collection or group of related records that are kept in an organized manner, that are maintained by a person, and from which personal information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. "System" does not include any published directory, any reference material or newsletter, or any routine information that is maintained for the purpose of internal office administration of the person, if the use of the directory, material, newsletter, or information would not adversely affect an individual, and there has been no unauthorized external breach of the directory, material, newsletter, or information.

(B) (1) Any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. The disclosure described in this division may be made pursuant to any provision of a contract entered into by the person with another person prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of this section and does not waive any provision of this section. For purposes of this section, a resident of this state is an individual whose principal mailing address as reflected in the records of the person is in this state.

(2) The person shall make the disclosure described in division (B)(1) of this section in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system.

(C) Any person that, on behalf of or at the direction of another person or on behalf of or at the direction of any governmental entity, is the custodian of or stores computerized data that includes personal information shall notify that other person or governmental entity of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of this state.

(D) The person may delay the disclosure or notification required by division (B), (C), or (G) of this section if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the person shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security.

(E) For purposes of this section, a person may disclose or make a notification by any of the following methods:

(1) Written notice;

(2) Electronic notice, if the person's primary method of communication with the resident to whom the disclosure must be made is by electronic means;

(3) Telephone notice;

(4) Substitute notice in accordance with this division, if the person required to disclose demonstrates that the person does not have sufficient contact information to provide notice in a manner described in division (E)(1), (2), or (3) of this section, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed two hundred fifty thousand dollars, or that the affected class of subject residents to whom disclosure or notification is required exceeds five hundred thousand persons. Substitute notice under this division shall consist of all of the following:

(a) Electronic mail notice if the person has an electronic mail address for the resident to whom the disclosure must be made;

(b) Conspicuous posting of the disclosure or notice on the person's web site, if the person maintains one;

(c) Notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds seventy-five per cent of the population of this state.

(5) Substitute notice in accordance with this division, if the person required to disclose demonstrates that the person is a business entity with ten employees or fewer and that the cost of providing the disclosures or notices to residents to whom disclosure or notification is required will exceed ten thousand dollars. Substitute notice under this division shall consist of all of the following:

(a) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the business entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;

(b) Conspicuous posting of the disclosure or notice on the business entity's web site, if the entity maintains one;

(c) Notification to major media outlets in the geographic area in which the business entity is located.

(F) (1) A financial institution, trust company, or credit union or any affiliate of a financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the requirements of this section.

(2) This section does not apply to any person or entity that is regulated by sections 1171 to 1179 of the "Social Security Act," chapter 531, 49 Stat. 620 (1935), 42 U.S.C. 1320d to 1320d-8, and any corresponding regulations in 45 C.F.R. Parts 160 and 164.

(G) If a person discovers circumstances that require disclosure under this section to more than one thousand residents of this state involved in a single occurrence of a breach of the security of the system, the person shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the person to the residents of this state. In no case shall a person that is required to make a notification required by this division delay any disclosure or notification required by division (B) or (C) of this section in order to make the notification required by this division.

(H) Any waiver of this section is contrary to public policy and is void and unenforceable.

(I) The attorney general may conduct pursuant to sections 1349.191 [1349.19.1] and 1349.192 [1349.19.2] of the Revised Code an investigation and bring a civil action upon an alleged failure by a person to comply with the requirements of this section.

HISTORY: 151 v H 104, § 1, eff. 2-17-06.

[§ 1349.19.1] § 1349.191. INVESTIGATION BY ATTORNEY GENERAL.

(A) As used in this section and section 1349.192 [1349.19.2] of the Revised Code:

(1) "Agency of a political subdivision" has the same meaning as in section 1347.12 of the Revised Code.

(2) "Business" has the same meaning as in section 1349.19 of the Revised Code.

(3) "State agency" has the same meaning as in section 1.60 of the Revised Code.

(B) The attorney general may conduct an investigation if the attorney general, based on complaints or the attorney general's own inquiries, has reason to believe that a state agency or an agency of a political subdivision has failed or is failing to comply with section 1347.12 of the Revised Code or that a person has failed or is failing to comply with section 1349.19 of the Revised Code.

(C) In any investigation conducted pursuant to this section, the attorney general may administer oaths, subpoena witnesses, adduce evidence, and subpoena the production of any book, document, record, or other relevant matter.

(D) (1) If the attorney general under division (C) of this section subpoenas the production of any relevant matter that is located outside this state, the attorney general may designate a representative, including an official of the state in which that relevant matter is located, to inspect the relevant matter on the attorney general's behalf. The attorney general may carry out similar requests received from officials of other states.

(2) Any person who is subpoenaed to produce relevant matter pursuant to division (C) of this section shall make that relevant matter available at a convenient location within this state or the state of the representative designated under division (D)(1) of this section.

(E) Any person who is subpoenaed as a witness or to produce relevant matter pursuant to division (C) of this section may file in the court of common pleas of Franklin county, the county in this state in which the person resides, or the county in this state in which the person's principal place of business is located a petition to extend for good cause shown the date on which the subpoena is to be returned or to modify or quash for good cause shown that subpoena. The person may file the petition at any time prior to the date specified for the return of the subpoena or within twenty days after the service of the subpoena, whichever is earlier.

(F) Any person who is subpoenaed as a witness or to produce relevant matter pursuant to division (C) of this section shall comply with the terms of the subpoena unless the court orders otherwise prior to the date specified for the return of the subpoena or, if applicable, that date as extended. If a person fails without lawful excuse to obey a subpoena, the attorney general may apply to the court of common pleas for an order that does one or more of the following:

(1) Compels the requested discovery;

(2) Adjudges the person in contempt of court;

(3) Grants injunctive relief to restrain the person from failing to comply with section 1347.12 or 1349.19 of the Revised Code, whichever is applicable;

(4) Grants injunctive relief to preserve or restore the status quo;

(5) Grants other relief that may be required until the person obeys the subpoena.

(G) The court shall impose a civil penalty on any person who violates an order of a court issued under division (F) of this section in the same manner as the imposition of a civil penalty under section 1349.192 [1349.19.2] of the Revised Code for a failure to comply with section 1347.12 or 1349.19 of the Revised Code, whichever is applicable.

HISTORY: 151 v H 104, § 1, eff. 2-17-06.

[§ 1349.19.2] § 1349.192. CIVIL ACTION BY ATTORNEY GENERAL; PENALTIES; LIABILITY FOR COSTS OF INVESTIGATION AND ACTION.

(A) (1) The attorney general shall have the exclusive authority to bring a civil action in a court of common pleas for appropriate relief under this section, including a temporary restraining order, preliminary or permanent injunction, and civil penalties, if it appears that a state agency or an agency of a political subdivision has failed or is failing to comply with section 1347.12 of the Revised Code or that a person has failed or is failing to comply with section 1349.19 of the Revised Code. Upon its finding that a state agency or an agency of a political subdivision has failed to comply with section 1347.12 of the Revised Code or that a person has failed to comply with section 1349.19 of the Revised Code, the court shall impose a civil penalty upon the state agency, agency of a political subdivision, or person as follows:

(a) For each day that the state agency, agency of a political subdivision, or person has intentionally or recklessly failed to comply with the applicable section, subject to divisions (A)(1)(b) and (c) of this section, a civil penalty of up to one thousand dollars for each day the agency or person fails to comply with the section;

(b) If the state agency, agency of a political subdivision, or person has intentionally or recklessly failed to comply with the applicable section for more than sixty days, subject to division (A)(1)(c) of this section, a civil penalty in the amount specified in division (A)(1)(a) of this section for each day of the first sixty days that the agency or person fails to comply with the section and, for each day commencing with the sixty-first day that the state agency, agency of a political subdivision, or person has failed to comply with the section, a civil penalty of up to five thousand dollars for each such day the agency or person fails to comply with the section;

(c) If the state agency, agency of a political subdivision, or person has intentionally or recklessly failed to comply with the applicable section for more than ninety days, a civil penalty in the amount specified in division (A)(1)(a) of this section for each day of the first sixty days that the agency or person fails to comply with the section, a civil penalty of up to five thousand dollars for each day commencing with the sixty-first day and continuing through the ninetieth day that the agency or person fails to comply with the section, and, for each day commencing with the ninety-first day that the state agency, agency of a political subdivision, or person has failed to comply with the section, a civil penalty of up to ten thousand dollars for each such day the agency or person fails to comply with the section.

(2) Any civil penalty that is assessed under division (A)(1) of this section shall be deposited into the consumer protection enforcement fund created by section 1345.51 of the Revised Code.

(3) In determining the appropriate civil penalty to assess under division (A)(1) of this section, the court shall consider all relevant factors, including the following:

(a) If the defendant in the civil action is a state agency, an agency of a political subdivision, or a person that is a business entity, whether or not the high managerial officer, agent, or employee of the agency or business entity having supervisory responsibility for compliance with section 1347.12 or 1349.19 of the Revised Code, whichever is applicable, acted in bad faith in failing to comply with the section.

(b) If the defendant in the civil action is a person other than a business entity, whether or not the person acted in bad faith in failing to comply with section 1349.19 of the Revised Code.

(B) Any state agency or agency of a political subdivision that is found by the court to have failed to comply with section 1347.12 of the Revised Code or any person that is found by the court to have failed to comply with section 1349.19 of the Revised Code shall be liable to the attorney general for the attorney general's costs in conducting an investigation under section 1349.191 [1349.19.1] of the Revised Code and bringing an action under this section.

(C) The rights and remedies that are provided under this section are in addition to any other rights or remedies that are provided by law.

HISTORY: 151 v H 104, § 1, eff. 2-17-06.

PENNSYLVANIA

§ 2302. DEFINITIONS

The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Breach of the security of the system." The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.

"Business." A sole proprietorship, partnership, corporation, association or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered or holding a license or authorization certificate under the laws of this Commonwealth, any other state, the United States or any other country, or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records.

"Encryption." The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

"Entity." A State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth.

"Individual." A natural person.

"Notice." May be provided by any of the following methods of notification:

(1) Written notice to the last known home address for the individual.

(2) Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.

(3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.

(4) (i) Substitute notice, if the entity demonstrates one of the following:
   (A) The cost of providing notice would exceed $ 100,000.
   (B) The affected class of subject persons to be notified exceeds 175,000.
   (C) The entity does not have sufficient contact information.

   (ii) Substitute notice shall consist of all of the following:
   (A) E-mail notice when the entity has an e-mail address for the subject persons.
   (B) Conspicuous posting of the notice on the entity's Internet website if the entity maintains one.
   (C) Notification to major Statewide media.

"Personal information."

(1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:
   (i) Social Security number.
   (ii) Driver's license number or a State identification card number issued in lieu of a driver's license.
   (iii) Financial 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.

(2) The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records.

"Records." Any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed or electromagnetically transmitted. The term does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.

"Redact." The term includes, but is not limited to, alteration or truncation such that no more than the last four digits of a Social Security number, driver's license number, State identification card number or account number is accessible as part of the data.

"State agency." Any agency, board, commission, authority or department of the Commonwealth and the General Assembly.

§ 2303. NOTIFICATION OF BREACH

(a) GENERAL RULE.-- An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

(b) ENCRYPTED INFORMATION.-- An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

(c) VENDOR NOTIFICATION.-- A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

RHODE ISLAND

§ 11-49.2-1 SHORT TITLE. –

This chapter shall be known and may be cited as the "Rhode Island Identity Theft Protection Act of 2005."

§ 11-49.2-2 LEGISLATIVE FINDINGS. –

It is hereby found and declared as follows:

(1) There is a growing concern regarding the possible theft of an individual's identity and a resulting need for measures to protect the privacy of personal information. It is the intent of the general assembly to ensure that personal information about Rhode Island residents is protected. To that end, the purpose of this chapter is to require businesses that own or license personal information about Rhode Islanders to provide reasonable security for that information. For the purpose of this chapter, the phrase "owns or licenses" is intended to include, but is not limited to, personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates.

(2) A business that owns or licenses computerized unencripted [sic] personal information about a Rhode Island resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(3) A business that discloses computerized unencripted [sic] personal information about a Rhode Island resident pursuant to a contract with a nonaffiliated third-party shall require by contract that the third-party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

§ 11-49.2-3 NOTIFICATION OF BREACH. –

(a) Any state agency or person that owns, maintains or licenses computerized data that includes personal information, shall disclose any breach of the security of the system which poses a significant risk of identity theft following discovery or notification of the breach in the security of the data to any resident of Rhode Island whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or a person without authority, to acquire said information. 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 state agency or person that maintains computerized unencripted [sic] data that includes personal information that the state agency or person does not own shall notify the owner or licensee of the information of any breach of the security of the data which poses a significant risk of identity theft 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) The notification must be prompt and reasonable following the determination of the breach unless otherwise provided in this section. Any state agency or person required to make notification under this section and who fails to do so promptly following the determination of a breach or receipt of notice from law enforcement as provided for is [sic] subsection (c) is liable for a fine as set forth in § 11-49.2-6.

§ 11-49.2-4 NOTIFICATION OF BREACH – CONSULTATION WITH LAW ENFORCEMENT. –

Notification of a breach is not required if, after an appropriate investigation or after consultation with relevant federal, state, or local law enforcement agencies, a determination is made that the breach has not and will not likely result in a significant risk of identity theft to the individuals whose personal information has been acquired.

§ 11-49.2-5 DEFINITIONS. –

The following definitions apply to this section:

(a) "Person" shall include any individual, partnership association, corporation or joint venture.

(b) For purposes for [sic] this section, "breach of the security of the system" means unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the state agency or person. 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.

(c) 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 Rhode Island 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.

(d) 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 for the [sic] in Section 7001 of Title 15 of the United States Code;

  (3) Substitute notice, if the state agency or person demonstrates that the cost of providing notice would exceed twenty-five thousand dollars ($25,000), or that the affected class of subject persons to be notified exceeds fifty thousand (50,000), or the state agency or person does not have sufficient contact information. Substitute notice shall consist of all of the following:

    (A) E-mail notice when the state agency or person has an e-mail address for the subject persons;

    (B) Conspicuous posting of the notice on the state agency's or person's website page, if the state agency or person maintains one;

    (C) Notification to major statewide media.

§ 11-49.2-6 PENALTIES FOR VIOLATION. –

(a) Each violation of this chapter is a civil violation for which a penalty of not more than a hundred dollars ($100) per occurrence and not more than twenty-five thousand dollars ($25,000) may be adjudged against a defendant.

(b) No Waiver of Notification. Any waiver of a provision of this section is contrary to public policy and is void and unenforceable.

§ 11-49.2-7 AGENCIES WITH SECURITY BREACH PROCEDURES. –

Any state agency or person that maintains its own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of § 11-49.2-3, shall be deemed to be in compliance with the security breach notification requirements of § 11-49.2-3, provided such person notifies subject persons in accordance with such person's policies in the event of a breach of security. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in 15 USC 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies subject persons in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security of the system. A financial institution, trust company, credit union or its affiliates that is subject to and examined for, and found in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed in compliance with this chapter. A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter.

TENNESSEE

47-18-2101. SHORT TITLE. -

This part shall be known and may be cited as the "Tennessee Identity Theft Deterrence Act of 1999."

47-18-2102. DEFINITIONS. -

As used in this part and in the Tennessee Consumer Protection Act, compiled in part 1 of this chapter, unless the context otherwise requires:

(1) "Ascertainable loss" means an identifiable deprivation, detriment or injury arising from the identity theft or from any unfair, misleading or deceptive act or practice even when the precise amount of the loss is not known. Whenever a violation of this part has occurred, an ascertainable loss shall be presumed to exist;

(2) "Attorney general" means the office of the Tennessee attorney general and reporter;

(3) "Division" means the division of consumer affairs of the department of commerce and insurance;

(4) "Financial document" means any credit card, debit card, check or checking account information or number, savings deposit slip or savings account information or number, or similar financial account or account number, including but not limited to, a money market account, certificate of deposit, or other type of interest generating account with a bank, savings and loan or credit union account, or any other financial institution, mutual fund account, 401K account, individual retirement account, retirement account, or other stock account information, savings bond or other bond, credit line, equity line or other line of credit which the possessor of the account has the right to draw against;

(5) "Identification documents" means any card, certificate or document which identifies or purports to identify the bearer of such document, whether or not intended for use as identification, and includes, but is not limited to, documents purporting to be a driver license, nondriver identification cards, birth certificates, marriage certificates, divorce certificates, passports, immigration documents, social security cards, employee identification cards, cards issued by the government to provide benefits of any sort, health care benefit cards, or health benefit organization, insurance company or managed care organization cards for the purpose of identifying a person eligible for services;

(6) "Identity theft" means:

(A) Obtaining, possessing, transferring, using or attempting to obtain, possess, transfer or use, for unlawful economic benefit, one or more identification documents or personal identification numbers of another person; or

(B) Otherwise obtaining, possessing, transferring, using or attempting to obtain, possess, transfer or use, for unlawful economic benefit, one (1) or more financial documents of another person;

(7) "Person" means a natural person, consumer, individual, governmental agency, partnership, corporation, trust, estate, incorporated or unincorporated association, and any other legal or commercial entity however organized;

(8) "Personal identification number" means any number that is assigned by the government to identify a particular person, including, but not limited to, social security number, federal tax payer identification number, Medicaid, Medicare or TennCare number which identifies a particular person eligible for benefits, any number assigned to a person as part of a licensure or registration process, such as a board of professional responsibility number, driver license number and passport number and any number assigned by an insurance company, health maintenance organization, managed care organization or other health benefit organization, for the purposes of identifying a particular person eligible for services; and

(9) "Tennessee Consumer Protection Act" means the Tennessee Consumer Protection Act of 1977, as amended, as compiled in part 1 of this chapter and related statutes. Related statutes specifically include any statute that indicates within the law, regulation or rule that a violation of that law, regulation or rule is a violation of the Tennessee Consumer Protection Act of 1977. Without limiting the scope of this definition, related statutes include but are not limited to: the Prize and Promotion Act, § 47-18-120; Health Club Act, as compiled in part 3 of this chapter; Buyer's Clubs Act, as compiled in part 5 of this chapter; Home Solicitations Sales Act of 1974, as compiled in part

7 of this chapter; Tennessee Credit Services Businesses Act, as compiled in part 10 of this chapter; Consumer Telemarketing Protection Act of 1990, as compiled in part 15 of this chapter; Unsolicited Telefacsimile Advertising Act, as compiled in part 16 of this chapter; Tennessee Employment Agency Act, as compiled in part 17 of this chapter; and Membership Camping Act, as compiled in title 66, chapter 32, part 3.

47-18-2103. PROHIBITED PRACTICES. -

It is unlawful for any person to directly or indirectly:

(1) Engage in identity theft; or

(2) Engage in any unfair, deceptive, misleading act or practice for the purpose of directly or indirectly engaging in identity theft.

47-18-2104. PRIVATE RIGHTS OF ACTION. -

(a) Any party commencing a private action pursuant to this part must provide a copy of the complaint and all other initial pleadings to the division of consumer affairs and upon entry of any judgment, order or decree of the action, shall mail a copy of such judgment, order or decree to the division of consumer affairs within five (5) days of entry of the judgment, order or decree.

(b) A copy of any notice of appeal shall be served by the appellant upon the director of the division, who in the public interest may intervene.

(c) A private action to enforce any liability created under this part may be brought within two (2) years from the date the liability arises, except that where a defendant has concealed the liability to that person, under this part, the action may be brought within two (2) years after discovery by the person of the liability. No action brought by the division shall be subject to the limitation of actions contained herein.

(d) In any private action commenced under this part, if the private party establishes that identity theft was engaged in willfully or knowingly, the court may award three (3) times the actual damages and may provide such other relief as it considers necessary and proper.

(e) The action may be brought in a court of competent jurisdiction in the county where the identity theft or unfair, deceptive or misleading act or practice took place, is taking place, or is about to take place, or in the county in which such person resides, has such person's principal place of business, conducts, transacts, or has transacted business, or, if the person cannot be found in any of the foregoing locations, in the county in which such person can be found.

(f) Without regard to any other remedy or relief to which a person is entitled, anyone affected by a violation of this part may bring an action to obtain a declaratory judgment that the act or practice violates the provisions of this part and to enjoin the person who has violated, is violating, or who is otherwise likely to violate this part; provided, that such action shall not be filed once the division has commenced a proceeding pursuant to this part or the Tennessee Consumer Protection Act, as compiled in part 1 of this chapter.

(g) Upon a finding by the court that a provision of this part has been violated, the court may award to the person bringing such action reasonable attorneys' fees and costs.

47-18-2105. CIVIL PENALTIES AND REMEDIES. -

(a) Whenever the division has reason to believe that any person has engaged in, is engaging in, or based upon information received from another law enforcement agency, is about to engage in any act or practice declared unlawful by this part and that proceedings would be in the public interest, the attorney general and reporter, at the request of the division, may bring an action in the name of the state against such person to restrain by temporary restraining order, temporary injunction, or permanent injunction the use of such act or practice. Additionally, the state may request an asset freeze or any other appropriate and necessary orders against such person.

(b) The action may be brought in the chancery or circuit court in Davidson County or in a court of competent jurisdiction in the county where the identity theft, unfair, misleading or deceptive act or practice took place or is about to take place or in the county in which such person resides, has such person's principal place of business, conducts, transacts, or has transacted business, or if the person cannot be found in any of the foregoing locations, in the county in which such person can be found.

(c) The courts are authorized to issue orders and injunctions to restrain and prevent violations of this part or issue any other necessary or appropriate relief or orders. Such orders and injunctions shall be issued without bond to the state of Tennessee.

(d) Notwithstanding any other provision of law, a violation of this part shall be punishable by a civil penalty of whichever of the following is greater: ten thousand dollars ($10,000), five thousand dollars ($5,000) per day for each day that a person's identity has been assumed or ten (10) times the amount obtained or attempted to be obtained by the person using the identity theft. This civil penalty is supplemental, cumulative and in addition to any other penalties and relief available under the Tennessee Consumer Protection Act, compiled in part 1 of this chapter, or other laws, regulations or rules.

(e) In any successful action commenced under this part, any ascertainable loss that a person has incurred as a result of the identity theft or misleading, deceptive or unfair practices used to engage in identify [sic] theft shall be recovered as restitution for each such person. The person shall also be awarded statutory interest on that ascertainable loss.

(f) In any successful action commenced by the division under this part, the court shall also order reimbursement to the division of the reasonable attorneys' fees, costs and expenses of the investigation and prosecution under this part.

(g) No court costs or litigation fees or costs of any sort can be taxed against the state in any action commenced under this part.

(h) Any knowing or willful violation of the terms of an injunction or order issued pursuant to this part in an action commenced by the attorney general and reporter shall be punishable by a civil penalty of not more than five thousand dollars ($5,000) for each and every violation of the order recoverable by the state, in addition to any other appropriate relief, including, but not limited to, contempt sanctions and the awarding of attorneys' fees and costs to the state for any filings relating to violations of any order under this part.

(i) An order or judgment issued as a result of an action commenced by the division shall in no way affect individual rights of action which may exist independent of the recovery of money or property received under such order or judgment. If a particular person receives restitution as a result of an action commenced by the attorney general and reporter, those funds shall act only as a set-off against any award of money received in the person's private right of action proceedings.

47-18-2106. VIOLATION OF TENNESSEE CONSUMER PROTECTION ACT. -

(a) A violation of this part constitutes a violation of the Tennessee Consumer Protection Act of 1977, compiled in part 1 of this chapter.

(b) For the purpose of application of the Tennessee Consumer Protection Act, compiled in part 1 of this chapter, any violation of the provisions of this part shall be construed to constitute an unfair or deceptive act or practice affecting trade or commerce and subject to the penalties and remedies as provided in that act, in addition to the penalties and remedies set forth in this part.

(c) If the division has reason to believe that any person has violated any provision of this part, the attorney general and reporter, at the request of the division, may institute a proceeding under this chapter.

47-18-2107. RELEASE OF PERSONAL CONSUMER INFORMATION. -

(a) As used in this section, unless the context otherwise requires:

(1) "Breach of the security of the system" means unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder. Good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system; provided, that the personal information is not used or subject to further unauthorized disclosure;

(2) "Information holder" means any person or business that conducts business in this state, or any agency of the state of Tennessee or any of its political subdivisions, that owns or licenses computerized data that includes personal information; and

(3) (A) "Personal information" means an individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements, when either the name or the data elements are not encrypted:

(i) Social security number;

(ii) Driver license number; or

(iii) 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; and

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

(b) Any information holder 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 Tennessee 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 subsection (d), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(c) Any information holder that maintains computerized data that includes personal information that the information holder 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.

(d) 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.

(e) For purposes of this section, notice may be provided by one (1) 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 15 U.S.C. § 7001; or

(3) Substitute notice, if the information holder 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 five hundred thousand (500,000), or the information holder does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice, when the information holder has an e-mail address for the subject persons;

(B) Conspicuous posting of the notice on the information holder's internet website page, if the information holder maintains such website page; and

(C) Notification to major statewide media.

(f) Notwithstanding subsection (e), an information holder 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 section, 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.

(g) In the event that a person discovers circumstances requiring notification pursuant to this section of more than one thousand (1,000) persons at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a, of the timing, distribution and content of the notices.

(h) Any customer of an information holder who is a person or business entity, but who is not an agency of the state or any political subdivision of the state, and who is injured by a violation of this section, may institute a civil action to recover damages and to enjoin the person or business entity from further action in violation of this section. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

(i) The provisions of this section shall not apply to any person who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102.

TEXAS

BUSINESS & COMMERCE CODE

CHAPTER 48. UNAUTHORIZED USE OF IDENTIFYING INFORMATION

SUBCHAPTER A. GENERAL PROVISIONS

SEC. 48.001. SHORT TITLE.

This chapter may be cited as the Identity Theft Enforcement and Protection Act.

Added by Acts 2005, 79th Leg., ch. 294, Sec. 2, eff. Sept. 1, 2005.

SEC. 48.002. DEFINITIONS.

In this chapter:

(1) "Personal identifying information" means information that alone or in conjunction with other information identifies an individual, including an individual's:
   (A) name, social security number, date of birth, or government-issued identification number;
   (B) mother's maiden name;
   (C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
   (D) unique electronic identification number, address, or routing code; and
   (E) telecommunication access device.

(2) "Sensitive personal information":
   (A) means an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
      (i) social security number;
      (ii) driver's license number or government-issued identification number; or
      (iii) account number or 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; and
   (B) does not include publicly available information that is lawfully made available to the general public from the federal government or a state or local government.

(3) "Telecommunication access device" has the meaning assigned by Section 32.51, Penal Code.

(4) "Victim" means a person whose identifying information is used by an unauthorized person.

Added by Acts 2005, 79th Leg., ch. 294, Sec. 2, eff. Sept. 1, 2005.

SUBCHAPTER B. IDENTITY THEFT

SEC. 48.101. UNAUTHORIZED USE OR POSSESSION OF PERSONAL IDENTIFYING INFORMATION.

(a) A person may not obtain, possess, transfer, or use personal identifying information of another person without the other person's consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name.

(b) It is a defense to an action brought under this section that an act by a person:
   (1) is covered by the Fair Credit Reporting Act (15 U.S.C. Section 1681 et seq.); and
   (2) is in compliance with that Act and regulations adopted under that Act.

(c) This section does not apply to:
   (1) a financial institution as defined by 15 U.S.C. Section 6809; or
   (2) a covered entity as defined by Section 601.001 or 602.001, Insurance Code.

Added by Acts 2005, 79th Leg., ch. 294, Sec. 2, eff. Sept. 1, 2005.

SEC. 48.102. BUSINESS DUTY TO PROTECT AND SAFEGUARD SENSITIVE PERSONAL INFORMATION.

(a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

(b) A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by:

(1) shredding;

(2) erasing; or

(3) otherwise modifying the sensitive personal information in the records to make the information unreadable or undecipherable through any means.

(c) This section does not apply to a financial institution as defined by 15 U.S.C. Section 6809.

Added by Acts 2005, 79th Leg., ch. 294, Sec. 2, eff. Sept. 1, 2005.

SEC. 48.103. NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA.

(a) In this section, "breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person. Good faith acquisition of sensitive personal information by an employee or agent of the person or business for the purposes of the person is not a breach of system security unless the sensitive personal information is used or disclosed by the person in an unauthorized manner.

(b) A person that conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any resident of this state whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(c) Any person that maintains computerized data that includes sensitive personal information that the person does not own shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(d) A person may delay providing notice as required by Subsections (b) and (c) at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that it will not compromise the investigation.

(e) A person may give notice as required by Subsections (b) and (c) by providing:

(1) written notice;

(2) electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001; or

(3) notice as provided by Subsection (f).

(f) If the person or business demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:

(1) electronic mail, if the person has an electronic mail address for the affected persons;

(2) conspicuous posting of the notice on the person's website; or

(3) notice published in or broadcast on major statewide media.

(g) Notwithstanding Subsection (e), a person that maintains its own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy.

(h) If a person is required by this section to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify, without unreasonable delay, all consumer reporting agencies, as defined by 15 U.S.C. Section 1681a, that maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.

Added by Acts 2005, 79th Leg., ch. 294, Sec. 2, eff. Sept. 1, 2005.

SUBCHAPTER C. REMEDIES AND OFFENSES

SEC. 48.201. CIVIL PENALTY; INJUNCTION.

(a) A person who violates this chapter is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. The attorney general may bring suit to recover the civil penalty imposed by this subsection.

(b) If it appears to the attorney general that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the attorney general may bring an action in the name of this state against the person to restrain the violation by a temporary restraining order or a permanent or temporary injunction.

(c) An action brought under Subsection (b) shall be filed in a district court in Travis County or:

(1) in any county in which the violation occurred; or

(2) in the county in which the victim resides, regardless of whether the alleged violator has resided, worked, or done business in the county in which the victim resides.

(d) The plaintiff in an action under this section is not required to give a bond. The court may also grant any other equitable relief that the court considers appropriate to prevent any additional harm to a victim of identity theft or a further violation of this chapter or to satisfy any judgment entered against the defendant, including the issuance of an order to appoint a receiver, sequester assets, correct a public or private record, or prevent the dissipation of a victim's assets.

(e) The attorney general is entitled to recover reasonable expenses incurred in obtaining injunctive relief, civil penalties, or both, under this section, including reasonable attorney's fees, court costs, and investigatory costs. Amounts collected by the attorney general under this section shall be deposited in the general revenue fund and may be appropriated only for the investigation and prosecution of other cases under this chapter.

(f) The fees associated with an action under this section are the same as in a civil case, but the fees may be assessed only against the defendant.

Added by Acts 2005, 79th Leg., ch. 294, Sec. 2, eff. Sept. 1, 2005.

SEC. 48.202. COURT ORDER TO DECLARE INDIVIDUAL A VICTIM OF IDENTITY THEFT.

(a) A person who is injured by a violation of Section 48.101 or who has filed a criminal complaint alleging commission of an offense under Section 32.51, Penal Code, may file an application with a district court for the issuance of a court order declaring that the person is a victim of identity theft. A person may file an application under this section regardless of whether the person is able to identify each person who allegedly transferred or used the person's identifying information in an unlawful manner.

(b) A person is presumed to be a victim of identity theft under this section if the person charged with an offense under Section 32.51, Penal Code, is convicted of the offense.

(c) After notice and hearing, if the court is satisfied by a preponderance of the evidence that the applicant has been injured by a violation of Section 48.101 or is the victim of an offense under Section 32.51, Penal Code, the court shall enter an order containing:

(1) a declaration that the person filing the application is a victim of identity theft resulting from a violation of Section 48.101 or an offense under Section 32.51, Penal Code, as appropriate;

(2) any known information identifying the violator or person charged with the offense;

(3) the specific personal identifying information and any related document used to commit the alleged violation or offense; and

(4) information identifying any financial account or transaction affected by the alleged violation or offense, including:

(A) the name of the financial institution in which the account is established or of the merchant involved in the transaction, as appropriate;

(B) any relevant account numbers;

(C) the dollar amount of the account or transaction affected by the alleged violation or offense; and

(D) the date of the alleged violation or offense.

(d) An order rendered under this section must be sealed because of the confidential nature of the information required to be included in the order. The order may be opened and the order or a copy of the order may be released only:

(1) to the proper officials in a civil proceeding brought by or against the victim arising or resulting from a violation of this chapter, including a proceeding to set aside a judgment obtained against the victim;

(2) to the victim for the purpose of submitting the copy of the order to a governmental entity or private business to:

(A) prove that a financial transaction or account of the victim was directly affected by a violation of this chapter or the commission of an offense under Section 32.51, Penal Code; or

(B) correct any record of the entity or business that contains inaccurate or false information as a result of the violation or offense;

(3) on order of the judge; or

(4) as otherwise required or provided by law.

(e) A court at any time may vacate an order issued under this section if the court finds that the application or any information submitted to the court by the applicant contains a fraudulent misrepresentation or a material misrepresentation of fact.

(f) A copy of an order provided to a person under Subsection (d)(1) must remain sealed throughout and after the civil proceeding. Information contained in a copy of an order provided to a governmental entity or business under Subsection (d)(2) is confidential and may not be released to another person except as otherwise required or provided by law.

Added by Acts 2005, 79th Leg., ch. 294, Sec. 2, eff. Sept. 1, 2005.

SEC. 48.203. DECEPTIVE TRADE PRACTICE. A VIOLATION OF SECTION 48.101 IS A DECEPTIVE TRADE PRACTICE ACTIONABLE UNDER SUBCHAPTER E, CHAPTER 17.

Added by Acts 2005, 79th Leg., ch. 294, Sec. 2, eff. Sept. 1, 2005.

UTAH

13-44-101 (EFFECTIVE 01/01/07). TITLE.

This chapter is known as the "Consumer Credit Protection Act."

13-44-102 (EFFECTIVE 01/01/07). DEFINITIONS.

As used in this chapter:

(1) (a) "Breach of system security" means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.

(b) "Breach of system security" does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner.

(2) "Consumer" means a natural person.

(3) (a) "Personal information" means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date [sic] element is unencrypted or not protected by another method that renders the data unreadable or unusable:

(i) Social Security number;

(ii) (A) financial account number, or credit or debit card number; and

(B) any required security code, access code, or password that would permit access to the person's account; or

(iii) driver license number or state identification card number.

(b) "Personal information" does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.

(4) "Record" includes materials maintained in any form, including paper and electronic.

13-44-201 (EFFECTIVE 01/01/07). PROTECTION OF PERSONAL INFORMATION.

(1) Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to:

(a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and

(b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person.

(2) The destruction of records under Subsection (1)(b) shall be by:

(a) shredding;

(b) erasing; or

(c) otherwise modifying the personal information to make the information indecipherable.

(3) This section does not apply to a financial institution as defined by 15 U.S.C. Section 6809.

13-44-202 (EFFECTIVE 01/01/07). PERSONAL INFORMATION – DISCLOSURE OF SYSTEM SECURITY BREACH.

(1) (a) A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes.

(b) If an investigation under Subsection (1)(a) reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident.

(2) A person required to provide notification under Subsection (1) shall provide the notification in the most expedient time possible without unreasonable delay:
  (a) considering legitimate investigative needs of law enforcement, as provided in Subsection (4)(a);
  (b) after determining the scope of the breach of system security; and
  (c) after restoring the reasonable integrity of the system.

(3) (a) A person who maintains computerized data that includes personal information that the person does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur.
  (b) Cooperation under Subsection (3)(a) includes sharing information relevant to the breach with the owner or licensee of the information.

(4) (a) Notwithstanding Subsection (2), a person may delay providing notification under Subsection (1) at the request of a law enforcement agency that determines that notification may impede a criminal investigation.
  (b) A person who delays providing notification under Subsection (4)(a) shall provide notification in good faith without unreasonable delay in the most expedient time possible after the law enforcement agency informs the person that notification will no longer impede the criminal investigation.

(5) (a) A notification required by this section may be provided:
    (i) in writing by first-class mail to the most recent address the person has for the resident;
    (ii) electronically, if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001;
    (iii) by telephone, including through the use of automatic dialing technology not prohibited by other law; or
    (iv) by publishing notice of the breach of system security in a newspaper of general circulation.
  (b) If a person maintains the person's own notification procedures as part of an information security policy for the treatment of personal information the person is considered to be in compliance with this chapter's notification requirements if the procedures are otherwise consistent with this chapter's timing requirements and the person notifies each affected Utah resident in accordance with the person's information security policy in the event of a breach.
  (c) A person who is regulated by state or federal law and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with this part if the person notifies each affected Utah resident in accordance with the other applicable law in the event of a breach.

(6) A waiver of this section is contrary to public policy and is void and unenforceable.

13-44-301 (EFFECTIVE 01/01/07). ENFORCEMENT.

(1) The attorney general may enforce this chapter's provisions.

(2) (a) Nothing in this chapter creates a private right of action.
  (b) Nothing in this chapter affects any private right of action existing under other law, including contract or tort.

(3) A person who violates this chapter's provisions is subject to a civil fine of:
  (a) no greater than $2,500 for a violation or series of violations concerning a specific consumer; and
  (b) no greater than $100,000 in the aggregate for related violations concerning more than one consumer.

(4) In addition to the penalties provided in Subsection (3), the attorney general may seek injunctive relief to prevent future violations of this chapter in:
  (a) the district court located in Salt Lake City; or
  (b) the district court for the district in which resides a consumer who is affected by the violation.

VERMONT

§ 2430. DEFINITIONS

The following definitions shall apply throughout this chapter unless otherwise required:

(1) "Business" means a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this state, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but in no case shall it include the state, a state agency, or any political subdivision of the state.

(2) "Consumer" means an individual residing in this state.

(3) "Data collector" may include, but is not limited to, the state, state agencies, political subdivisions of the state, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

(4) "Encryption" means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

(5) (A) "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 or protected by another method that renders them unreadable or unusable by unauthorized persons:

(i) Social Security number;

(ii) Motor vehicle operator's license number or nondriver identification card number;

(iii) Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;

(iv) Account passwords or personal identification numbers or other access codes for a financial account.

(B) "Personal information" does not mean publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(6) "Records" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

(7) "Redaction" means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data.

(8) (A) "Security breach" means unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.

(B) "Security breach" does not include good faith but unauthorized acquisition or access of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure. (Added 2005, No. 162 (Adj. Sess.), § 1, eff. Jan. 1, 2007.)

§ 2435. NOTICE OF SECURITY BREACHES

(a) This section shall be known as the Security Breach Notice Act.

(b) Notice of breach.

(1) Except as set forth in subsection (d) of this section, any data collector that owns or licenses computerized personal information that includes personal information concerning a consumer shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach. Notice of the breach shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of the law enforcement agency, as provided in subdivision (3) of this subsection, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

(2) Any data collector that maintains or possesses computerized data containing personal information of a consumer that the business does not own or license or any data collector that conducts business in Vermont that maintains or possesses records or data containing personal information that the data collector does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subdivision (3) of this subsection.

(3) The notice required by this subsection shall be delayed upon request of a law enforcement agency. A law enforcement agency may request the delay if it believes that notification may impede a law enforcement investigation, or a national or homeland security investigation or jeopardize public safety or national or homeland security interests. In the event law enforcement makes the request in a manner other than in writing, the data collector shall document such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. A law enforcement agency shall promptly notify the data collector when the law enforcement agency no longer believes that notification may impede a law enforcement investigation, or a national or homeland security investigation or jeopardize public safety or national or homeland security interests. The data collector shall provide notice required by this section without unreasonable delay upon receipt of a written communication, which includes facsimile or electronic communication, from the law enforcement agency withdrawing its request for delay.

(4) The notice shall be clear and conspicuous. The notice shall include a description of the following:

(A) The incident in general terms.

(B) The type of personal information that was subject to the unauthorized access or acquisition.

(C) The general acts of the business to protect the personal information from further unauthorized access or acquisition.

(D) A toll-free telephone number that the consumer may call for further information and assistance.

(E) Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

(5) For purposes of this subsection, notice to consumers may be provided by one of the following methods:

(A) Direct notice to consumers, which may be by one of the following methods:

(i) Written notice mailed to the consumer's residence;

(ii) Electronic notice, for those consumers for whom the data collector has a valid e-mail address if:

(I) the data collector does not have contact information set forth in subdivisions (i) and (iii) of this subdivision (5)(A), the data collector's primary method of communication with the consumer is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or

(II) the notice provided is consistent with the provisions regarding electronic records and signatures for notices as set forth in 15 U.S.C. § 7001; or

(iii) Telephonic notice, provided that telephonic contact is made directly with each affected consumer, and the telephonic contact is not through a prerecorded message.

(B) Substitute notice, if the data collector demonstrates that the cost of providing written or telephonic notice, pursuant to subdivision (A)(i) or (iii) of this subdivision (5), to affected consumers would exceed $5,000.00 or that the affected class of affected consumers to be provided written or telephonic notice, pursuant to subdivision (A)(i) or (iii) of this subdivision (5), exceeds 5,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) conspicuous posting of the notice on the data collector's website page if the data collector maintains one; and

(ii) notification to major statewide and regional media.

(c) In the event a data collector provides notice to more than 1,000 consumers at one time pursuant to this section, the data collector shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice. This subsection shall not apply to a person who is licensed or registered under Title 8 by the department of banking, insurance, securities, and health care administration.

(d) (1) Notice of a security breach pursuant to subsection (b) of this section is not required if the data collector establishes that misuse of personal information is not reasonably possible and the data collector provides notice of the determination that the misuse of the personal information is not reasonably possible pursuant to the requirements of this subsection. If the data collector establishes that misuse of the personal information is not reasonably possible, the data collector shall provide notice of its determination that misuse of the personal information is not reasonably possible and a detailed explanation for said determination to the Vermont attorney general or to the department of banking, insurance, securities, and health care administration in the event that the data collector is a person or entity licensed or registered with the department under Title 8 or this title. The data collector may designate its notice and detailed explanation to the Vermont attorney general or the department of banking, insurance, securities, and health care administration as "trade secret" if the notice and detailed explanation meet the definition of trade secret contained in subdivision 317(c)(9) of Title 1.

(2) If a data collector established that misuse of personal information was not reasonably possible under subdivision (1) of this subsection, and subsequently obtains facts indicating that misuse of the personal information has occurred or is occurring, the data collector shall provide notice of the security breach pursuant to subsection (b) of this section.

(e) Any waiver of the provisions of this subchapter is contrary to public policy and is void and unenforceable.

(f) A financial institution that is subject to the following guidances, and any revisions, additions, or substitutions relating to said interagency guidance shall be exempt from this section:

(1) The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; or

(2) Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration.

(g) Enforcement.

(1) With respect to all data collectors and other entities subject to this subchapter, other than a person or entity licensed or registered with the department of banking, insurance, securities, and health care administration under Title 8 or this title, the attorney general and state's attorney shall have sole and full authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain and impose remedies for a violation of this subchapter or any rules or regulations made pursuant to this chapter as the attorney general and state's attorney have under chapter 63 of this title. The attorney general may refer the matter to the state's attorney in an appropriate case. The superior courts shall have jurisdiction over any enforcement matter brought by the attorney general or a state's attorney under this subsection.

(2) With respect to a data collector that is a person or entity licensed or registered with the department of banking, insurance, securities, and health care administration under Title 8 or this title, the department of banking, insurance, securities and health care administration shall have the full authority to investigate potential violations of this subchapter and to prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations adopted pursuant to this subchapter, as the department has under Title 8 or this title or any other applicable law or regulation.

SUBSECTION (H) REPEALED EFFECTIVE JUNE 30, 2008; SEE NOTE SET OUT BELOW.

(h) Vermont law enforcement agencies, including the department of public safety, shall not be considered a data collector. Except as provided in subdivisions (b)(2) and (b)(3) of this section, Vermont law enforcement agencies, including the department of public safety, shall be exempt from this subchapter. (Added 2005, No. 162 (Adj. Sess.), § 1, eff. Jan. 1, 2007.)

§ 2440. SOCIAL SECURITY NUMBER PROTECTION

(a) This section shall be known as the Social Security Number Protection Act.

(b) Except as provided in subsection (c) of this section, a business may not do any of the following:

(1) Intentionally communicate or otherwise make available to the general public an individual's Social Security number.

(2) Intentionally print or imbed an individual's Social Security number on any card required for the individual to access products or services provided by the person or entity.

(3) Require an individual to transmit his or her Social Security number over the internet unless the connection is secure or the Social Security number is encrypted.

(4) Require an individual to use his or her Social Security number to access an internet website, unless a password or unique personal identification number or other authentication device is also required to access the internet website.

(5) Print an individual's Social Security number on any materials that are mailed to the individual, unless state or federal law requires the Social Security number to be on the document to be mailed.

(6) Sell, lease, lend, trade, rent, or otherwise intentionally disclose an individual's Social Security number to a third party without written consent to the disclosure from the individual, when the party making the disclosure knows or in the exercise of reasonable diligence would have reason to believe that the third party lacks a legitimate purpose for obtaining the individual's Social Security number.

(c) Subsection (b) of this section shall not apply:

(1) When a Social Security number is included in an application or in documents related to an enrollment process, or to establish, amend, or terminate an account, contract, or policy; or to confirm the accuracy of the Social Security number for the purpose of obtaining a credit report pursuant to 15 U.S.C. § 1681(b)(2). A Social Security number that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on an envelope without the envelope having been opened.

(2) To the collection, use, or release of a Social Security number reasonably necessary for administrative purposes or internal verification.

(3) To the opening of an account or the provision of or payment for a product or service authorized by an individual.

(4) To the collection, use, or release of a Social Security number to investigate or prevent fraud; conduct background checks; conduct social or scientific research; collect a debt; obtain a credit report from or furnish data to a consumer reporting agency pursuant to the fair credit reporting act, 15 U.S.C. § 1681, et seq.; undertake a permissible purpose enumerated under Gramm Leach Bliley, 12 C.F.R. § 216.13-15; or locate an individual who is missing, is a lost relative, or is due a benefit, such as a pension, insurance, or unclaimed property benefit.

(5) To a business acting pursuant to a court order, warrant, subpoena, or when otherwise required by law, or in response to a facially valid discovery request pursuant to rules applicable to a court or administrative body that has jurisdiction over the disclosing entity.

(6) To a business providing the Social Security number to a federal, state, or local government entity, including a law enforcement agency, the department of public safety, and a court, or their agents or assigns.

(7) To a Social Security number that has been redacted.

(8) (A) To a business that has used, prior to January 1, 2007, an individual's Social Security number in a manner inconsistent with subsection (b) of this section, which may continue using that individual's Social Security number in that manner on or after January 1, 2007, if all of the following conditions are met:

(i) The use of the Social Security number is continuous. If the use is stopped for any reason, subsection (b) of this section shall apply.

(ii) The individual is provided an annual disclosure that informs the individual that he or she has the right to stop the use of his or her Social Security number in a manner prohibited by subsection (b) of this section.

(iii) A written request by an individual to stop the use of his or her Social Security number in a manner prohibited by subsection (b) of this section is implemented within 30 days of the receipt of the request. There shall not be a fee or charge for implementing the request.

(iv) The person or entity does not deny services to an individual because the individual makes a written request pursuant to this subsection.

(B) Nothing in this subdivision (8) is intended to apply to the collection, use or dissemination of Social Security numbers collected prior to January 1, 2007 and exempted from the provisions of subsection (b) of this section pursuant to subdivisions (1) through (7) or (9) and (10) of this subsection.

(9) To information obtained from a recorded document in the official records of the town clerk or municipality.

(10) To information obtained from a document filed in the official records of the courts.

(d) Except as provided in subsection (e) of this section, the state and any state agency, political subdivision of the state, and agent or employee of the state, a state agency, or a political subdivision of the state, may not do any of the following:

(1) Collect a Social Security number from an individual unless authorized or required by law, state or federal regulation, or grant agreement to do so or unless the collection of the Social Security number or records containing the Social Security number is related to the performance of that agency's duties and responsibilities as prescribed by law.

(2) Fail, when collecting a Social Security number from an individual in a hard copy format, to segregate that number on a separate page from the rest of the record, or as otherwise appropriate, in order that the Social Security number can be more easily redacted pursuant to a valid public records request.

(3) Fail, when collecting a Social Security number from an individual, to provide, at the time of or prior to the actual collection of the Social Security number by that agency, that individual, upon request, with a statement of the purpose or purposes for which the Social Security number is being collected and used.

(4) Use the Social Security number for any purpose other than the purpose set forth in the statement required under subdivision (3) of this subsection.

(5) Intentionally communicate or otherwise make available to the general public a person's Social Security number.

(6) Intentionally print or imbed an individual's Social Security number on any card required for the individual to access government services.

(7) Require an individual to transmit the individual's Social Security number over the internet, unless the connection is secure or the Social Security number is encrypted.

(8) Require an individual to use the individual's Social Security number to access an internet website, unless a password or unique personal identification number or other authentication device is also required to access the internet website.

(9) Print an individual's Social Security number on any materials that are mailed to the individual, unless a state or federal law, regulation, or grant agreement requires that the Social Security number be on the document to be mailed. A Social Security number that is permitted to be mailed under this subdivision may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on an envelope, without the envelope having been opened.

(e) Subsection (d) of this section does not apply to:

(1) Social Security numbers disclosed to another governmental entity or its agents, employees, contractors, grantees, or grantors of a governmental entity if disclosure is necessary for the receiving entity to perform its duties and responsibilities. The receiving governmental entity and its agents, employees, and contractors shall maintain the confidential and exempt status of such numbers. As used in this subsection, "necessary" means reasonably needed to promote the efficient, accurate, or economical conduct of an entity's duties and responsibilities.

(2) Social Security numbers disclosed pursuant to a court order, warrant, or subpoena, or in response to a facially valid discovery request pursuant to rules applicable to a court or administrative body that has jurisdiction over the disclosing entity.

(3) Social Security numbers disclosed for public health purposes pursuant to and in compliance with requirements of the department of health under Title 18.

(4) The collection, use, or release of a Social Security number reasonably necessary for administrative purposes or internal verification. Internal verification includes the sharing of information for internal verification between and among governmental entities and their agents, employees, contractors, grantees, and grantors.

(5) Social Security numbers that have been redacted.

(6) (A) A state agency or state political subdivision that has used, prior to January 1, 2007, an individual's Social Security number in a manner inconsistent with subsection (d) of this section, which may continue using that individual's Social Security number in that manner on or after January 1, 2007, if all of the following conditions are met:

(i) The use of the Social Security number is continuous. If the use is stopped for any reason, subsection (d) of this section shall apply.

(ii) The individual is provided an annual disclosure that informs the individual that he or she has the right to stop the use of his or her Social Security number in a manner prohibited by subsection (d) of this section.

(iii) A written request by an individual to stop the use of his or her Social Security number in a manner prohibited by subsection (d) of this section is implemented within 30 days of the receipt of the request. There shall not be a fee or charge for implementing the request.

(iv) The state agency or state political subdivision does not deny services to an individual because the individual makes a written request pursuant to this subdivision.

(B) Nothing in this subdivision (e)(6) is intended to apply to the collection, use or dissemination of Social Security numbers collected prior to January 1, 2007 and exempted from the provisions of subsection (d) of this section pursuant to subdivisions (1) through (5) or (7) through (11) of this subsection.

(7) Certified copies of vital records issued by the health department and other authorized officials pursuant to part 6 of Title 18.

(8) A recorded document in the official records of the town clerk or municipality.

(9) A document filed in the official records of the courts.

(10) The collection, use, or dissemination of Social Security numbers by law enforcement agencies and the department of public safety in the execution of their duties and responsibilities.

(11) The collection, use, or release of a Social Security number to investigate or prevent fraud; conduct background checks; conduct social or scientific research; collect a debt; obtain a credit report from or furnish data to a consumer reporting agency pursuant to the fair credit reporting act, 15 U.S.C. § 1681 et seq.; undertake a permissible purpose enumerated under Gramm Leach Bliley, 12 C.F.R. § 216.13-15; or locate an individual who is missing, is a lost relative, or is due a benefit, such as a pension, insurance, or unclaimed property benefit.

(f) Any person has the right to request that a town clerk or clerk of court remove from an image or copy of an official record placed on a town's or court's internet website available to the general public or an internet website available to the general public to display public records by the town clerk or clerk of court, the person's Social Security number, employer taxpayer identification number, driver's license number, state identification number, passport number, checking account number, savings account number, credit card or debit card number, or personal identification number (PIN) code or passwords contained in that official record. A town clerk or clerk of court is authorized to redact the personal information identified in a request submitted under this section. The request must be made in writing, legibly signed by the requester, and delivered by mail, facsimile, or electronic transmission, or delivered in person to the town clerk or clerk of court. The request must specify the personal information to be redacted, information that identifies the document that contains the personal information and unique information that identifies the location within the document that contains the Social Security number, employer taxpayer identification number, driver's license number, state identification number, passport number, checking account number, savings account number, credit card number, or debit card number, or personal identification number (PIN) code or passwords to be redacted. The request for redaction shall be considered a public record with access restricted to the town clerk, the clerk of court, their staff, or upon order of the court. The town clerk or clerk of court shall have no duty to inquire beyond the written request to verify the identity of a person requesting redaction and shall have no duty to remove redaction for any reason upon subsequent request by an individual or by order of the court, if impossible to do so. No fee will be charged for the redaction pursuant to such request. Any person who requests a redaction without proper authority to do so shall be guilty of an infraction, punishable by a fine not to exceed $500.00 for each violation.

(g) Enforcement.

(1) With respect to businesses, the state, state agencies, political subdivisions of the state, and agents or employees of the state, a state agency, or a political subdivision of the state, subject to this subchapter, other than a person or entity licensed or registered with the department of banking, insurance, securities, and health care administration under Title 8 or this title, the attorney general and state's attorney shall have sole and full authority to investigate potential violations of this subchapter, to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter, or any rules made pursuant to this subchapter, and to adopt rules under this subchapter, as the attorney general and state's attorney have under chapter 63 of this title. The attorney general may refer the matter to the state's attorney in an appropriate case. The superior courts shall have jurisdiction over any enforcement matter brought by the attorney general or a state's attorney under this subsection.

(2) With respect to a person or entity licensed or registered with the department of banking, insurance, securities, and health care administration under Title 8 or this title, the department shall have full authority to investigate potential violations of this subchapter, and to prosecute, obtain and impose remedies for a violation of this subchapter or any rules adopted pursuant to this subchapter as the department has under Title 8 or this title, or any other applicable law or regulation.

(3) With respect to the information provided by the Vermont department of public safety and law enforcement agencies, and any agent or employee thereof, to the Vermont attorney general or state's attorney pursuant to subdivision (1) of this subsection, the information provided or made available by the agency or department to the attorney general may be designated by the agency or department as confidential, and shall not be released under the provisions of 1 V.S.A. § 317. (Added 2005, No. 162 (Adj. Sess.), § 1, eff. July 1, 2007.)

§ 2445. SAFE DESTRUCTION OF DOCUMENTS CONTAINING PERSONAL INFORMATION

(a) As used in this section:

(1) "Business" means sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this state, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but in no case shall it include the state, a state agency, or any political subdivision of the state. The term includes an entity that destroys records.

(2) "Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

(3) "Personal information" means the following information that identifies, relates to, describes, or is capable of being associated with a particular individual: his or her signature, Social Security number, physical characteristics or description, passport number, driver's license or state identification card number, insurance policy number, bank account number, credit card number, debit card number, or any other financial information.

(4) (A) "Record" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted.

(B) "Record" does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

(b) A business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or indecipherable through any means for the purpose of:

(1) ensuring the security and confidentiality of customer personal information;

(2) protecting against any anticipated threats or hazards to the security or integrity of customer personal information; and

(3) protecting against unauthorized access to or use of customer personal information that could result in substantial harm or inconvenience to any customer.

(c) An entity that is in the business of disposing of personal financial information that conducts business in Vermont or disposes of personal information of residents of Vermont must take all reasonable measures to dispose of records containing personal information by implementing and monitoring compliance with policies and procedures that protect against unauthorized access to or use of personal information during or after the collection and transportation and disposing of such information.

(d) This section does not apply to any of the following:

(1) Any bank, credit union, or financial institution as defined under the federal Gramm Leach Bliley law that is subject to the regulation of the Office of the Comptroller of the Currency, the Federal Reserve, the National Credit Union Administration, the Securities and Exchange Commission, the federal deposit insurance corporation, the office of thrift supervision of the U.S. department of the treasury, or the department of banking, insurance, securities, and health care administration and is subject to the privacy and security provisions of the Gramm Leach Bliley Act, 15 U.S.C. § 6801 et seq.

(2) Any health insurer or health care facility that is subject to and in compliance with the standards for privacy of individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996.

(3) Any consumer reporting agency that is subject to and in compliance with the Federal Credit Reporting Act, 15 U.S.C. § 1681 et seq., as amended.

(e) Enforcement.

(1) With respect to all businesses subject to this section, other than a person or entity licensed or registered with the department of banking, insurance, securities and health care administration under Title 8 or this title, the attorney general and state's attorney shall have sole and full authority to investigate potential violations of this section, and to prosecute, obtain and impose remedies for a violation of this section, or any rules adopted pursuant to this section, and to adopt rules under this act, as the attorney general and state's attorney have under chapter 63 of this title. The superior courts shall have jurisdiction over any enforcement matter brought by the attorney general or a state's attorney under this subsection.

(2) With respect to a person or entity licensed or registered with the department of banking, insurance, securities, and health care administration under Title 8 or this title to do business in this state, the department of banking, insurance, securities, and health care administration shall have full authority to investigate potential violations of this act, and to prosecute, obtain, and impose remedies for a violation of this act, or any rules or regulations made pursuant to this act, as the department has under Title 8 and this title, or any other applicable law or regulation. (Added 2005, No. 162 (Adj. Sess.), § 1, eff. Jan. 1, 2007.)

WASHINGTON

RCW 19.255.010

DISCLOSURE, NOTICE — DEFINITIONS — RIGHTS, REMEDIES.

(1) Any person or business that conducts business in this state 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 this state 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 subsection (3) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(2) 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.

(3) 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.

(4) 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 when the personal information is not used or subject to further unauthorized disclosure.

(5) 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:

  (a) Social security number;

  (b) Driver's license number or Washington identification card number; or

  (c) Account number or 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.

(6) 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.

(7) For purposes of this section and except under subsection (8) of this section, "notice" may be provided by one of the following methods:

  (a) Written notice;

  (b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or

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

    (i) E-mail notice when the person or business has an e-mail address for the subject persons;

    (ii) Conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one; and

    (iii) Notification to major statewide media.

(8) 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 section is 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.

(9) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.

(10) (a) Any customer injured by a violation of this section may institute a civil action to recover damages.

(b) Any business that violates, proposes to violate, or has violated this section 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.

(d) A person or business under this section shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity.

[2005 c 368 § 2.]

Notes:

Similar provision: RCW 42.56.590.

WISCONSIN

895.507 NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION.

(1) DEFINITIONS. In this section:

(a) 1. "Entity" means a person, other than an individual, that does any of the following:

a. Conducts business in this state and maintains personal information in the ordinary course of business.

b. Licenses personal information in this state.

c. Maintains for a resident of this state a depository account as defined in s. 815.18 (2) (e).

d. Lends money to a resident of this state.

2. "Entity" includes all of the following:

a. The state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the constitution or any law, including the legislature and the courts.

b. A city, village, town, or county.

(am) "Name" means an individual's last name combined with the individual's first name or first initial.

(b) "Personal information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:

1. The individual's social security number.

2. The individual's driver's license number or state identification number.

3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account.

4. The individual's deoxyribonucleic acid profile, as defined in s. 939.74 (2d) (a).

5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

(c) "Publicly available information" means any information that an entity reasonably believes is one of the following:

1. Lawfully made widely available through any media.

2. Lawfully made available to the general public from federal, state, or local government records or disclosures to the general public that are required to be made by federal, state, or local law.

(2) NOTICE REQUIRED.

(a) If an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.

(b) If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident of this state who is the subject of the personal information.

(bm) If a person, other than an individual, that stores personal information pertaining to a resident of this state, but does not own or license the personal information, knows that the personal information has been acquired by a person whom the person storing the personal information has not authorized to acquire the personal information, and the person storing the personal information has not entered into a contract with the person that owns or licenses the personal information, the person storing the personal information shall notify the person that owns or licenses the personal information of the acquisition as soon as practicable.

(br) If, as the result of a single incident, an entity is required under par. (a) or (b) to notify 1,000 or more individuals that personal information pertaining to the individuals has been acquired, the entity shall without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the timing, distribution, and content of the notices sent to the individuals.

(cm) Notwithstanding pars. (a), (b), (bm), and (br), an entity is not required to provide notice of the acquisition of personal information if any of the following applies:

1. The acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.
2. The personal information was acquired in good faith by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity.

(3) TIMING AND MANNER OF NOTICE; OTHER REQUIREMENTS.

(a) Subject to sub. (5), an entity shall provide the notice required under sub. (2) within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination as to reasonableness under this paragraph shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.

(b) An entity shall provide the notice required under sub. (2) by mail or by a method the entity has previously employed to communicate with the subject of the personal information. If an entity cannot with reasonable diligence determine the mailing address of the subject of the personal information, and if the entity has not previously communicated with the subject of the personal information, the entity shall provide notice by a method reasonably calculated to provide actual notice to the subject of the personal information.

(c) Upon written request by a person who has received a notice under sub. (2) (a) or (b), the entity that provided the notice shall identify the personal information that was acquired.

(3m) REGULATED ENTITIES EXEMPT. This section does not apply to any of the following:

(a) An entity that is subject to, and in compliance with, the privacy and security requirements of 15 USC 6801 to 6827, or a person that has a contractual obligation to such an entity, if the entity or person has in effect a policy concerning breaches of information security.

(b) An entity that is described in 45 CFR 164.104 (a), if the entity complies with the requirements of 45 CFR part 164.

(4) EFFECT ON CIVIL CLAIMS. Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.

(5) REQUEST BY LAW ENFORCEMENT NOT TO NOTIFY. A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required under sub. (2) for any period of time and the notification process required under sub. (2) shall begin at the end of that time period. Notwithstanding subs. (2) and (3), if an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.

(6m) LOCAL ORDINANCES OR REGULATIONS PROHIBITED. No city, village, town, or county may enact or enforce an ordinance or regulation that relates to notice or disclosure of the unauthorized acquisition of personal information.

(7m) EFFECT OF FEDERAL LEGISLATION. If the joint committee on administrative rules determines that the federal government has enacted legislation that imposes notice requirements substantially similar to the requirements of this section and determines that the legislation does not preempt this section, the joint committee on administrative rules shall submit to the revisor of statutes for publication in the Wisconsin administrative register a notice of its determination. This section does not apply after publication of a notice under this subsection.

History: 2005 a. 138.