SB

222

SFIN

FILE

SB 222

was referred to the Senate Finance Committee

Hearing(s) were held

The bill did not move from Committee

Alaska State Legislature

SENATOR
GENE THERRIAULT
Mailing Address:
1904, Cushman, Suite 101
Fairbanks, Alaska 99701
(907) 488-0857
Fax: (907) 488-1271

While in session:
State Capitol
Juneau, Alaska
99801-1182
(907) 465-4797
Fax: (907) 465-3884
Senate District F

Senate

Sponsor Statement

Senate Bill 222

Consumer Privacy Protection Act

I have introduced Senate Bill 222 to address the ever-increasing risks to consumers as their personal information is collected, distributed, and discarded by both private sector and government entities.

Senate Bill 222 tightens security measures pertaining to personal information as well as timelines to better notify consumers of potential problems so they may take remedial action as quickly as possible.

Consumers have every right to expect their private records are well protected and that their personal credit information is accurate. They also must have reasonable recourse when potentially damaging inaccurate information is made public including ample opportunities for redress and restitution in a timely manner.

In summary, Senate Bill 222 requires parties that handle and distribute sensitive consumer information to be accountable and responsible in those activities.

THE
FOLLOWING
DOCUMENT(S)
ARE
POOR
ORIGINAL
COPIES

National Card Coalition

Security Breach

Enacted Legislation

February 20, 2006

Post Office Box 3188
Laurel, MD 20709-3188
(202) 783-7766 phone

Security Breach Enacted Legislation

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice - OCC Bulletin 2005-13 **Breach Provisions Effective:** 03/29/05 **Enforcement:** Functional regulator **Penalties:** Refer to GLBA, 15 U.S.C. 6801, Section 501(b) and Interagency Guidelines Establishing Information Security Standards (Security Guidelines) **Summary:** Pursuant to the Gramm-Leach-Bliley Act, the federal banking agencies issued joint proposed guidance regarding security breaches in 2003 but did not finalize that guidance until March 29, 2005 when they issued the final Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. This Guidance interprets Section 501(b) of GLBA and Interagency Guidelines Establishing Information Security Standards (the "Security Guidelines") and describes response programs, including customer notification procedures, that financial institutions should develop and implement to address unauthorized access to or use of customer info. that could result in substantial harm or inconvenience to customer. **Preemption of state law** not addressed http://www.occ.treas.gov/ftp/bulletin/2005-13.doc	Financial institutions regulated by federal banking agencies. Every financial institution should develop and implement response program designed to address incidents of unauthorized access to customer info. maintained by institution or its service provider. Final guidance provides each financial institution with greater flexibility to design risk-based response program tailored to size, complexity and nature of its operations.	**Trigger** Reasonable **investigation** to promptly determine likelihood that sensitive customer info. has been or will be misused. Notice required if determination that misuse has occurred or is reasonably possible. **Method** No specific method for providing notice is required - any manner designed to ensure that a customer can reasonably be expected to receive it (i.e., telephone, mail, email) ***Guidance specifies notice content.*** **Timing** As soon as possible.	Customer name, address or telephone # in conjunction with any one or more data elements: • SS # • State DL # • account # • credit or debit card # • personal ID # or code that would permit access to a customer's account • any combination of components of customer info. that would allow someone to log onto or access customer's account, such as user name and password or password and account number. Does not exclude info. that is publicly available.	Delay for law enforcement **investigation.**	**3rd Party Notice** An institution's contract with its service provider should require service provider to take appropriate actions to address incidents of unauthorized access to financial institution's customer info., including notification to institution as soon as possible of any such incident, to enable institution to expeditiously implement its response program. Encouraged but not required to notify CRAs and federal regulators.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Arkansas S 1167 **Sponsor:** Capps (D) **Introduced:** 03/07/05 **Enacted:** 03/31/05 **Act/Chapter Number:** 1526 **Breach Provisions Effective:** 08/12/05 **Enforcement:** AG action; AG criminal action for knowing and willful violation, private right of action. **Penalties:** Class A misdemeanor, punishable by up to 1 year in prison and fine of up to $1K for knowing and willful violation; restitution; injunction; enjoinment; civil penalties up to $10K per violation; actual damages and reasonable attorney's fees. **Summary:** Relates to the protection of personal info. and the disclosure of security breaches of computerized data that includes personal info., that was reasonably believed to have been acquired by an unauthorized person, in an expedient manner using various specified methods. **State agency** security breaches included in act via "business" definition. **Identity theft measure** also includes provisions for destruction of customer records containing personal info. http://www.arkleg.state.ar.us/ftproot/acts/2005/public/act1526.pdf	Person or business that acquires, owns or licenses computerized data that includes personal info. **Security breach** defined as unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal info. maintained by a person or business. Does not include good faith acquisition of personal info. by employee/agent of person/ business for legitimate purposes of person/business if personal info. is not otherwise used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people, or • not enough info. to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when either name or data element is not encrypted or redacted. • SS # • State DL or ID # • account, credit card or debit card # in combination with required access/security code or password • medical info. Does ***not*** exclude info. that is publicly available.	Delay for law enforcement **investigation.** Notice not required if reasonable **investigation** determines no reasonable likelihood of harm to customers. **Safe harbor** for providing notice pursuant to an internal info. security policy.	3rd Party Notice Person doing business maintaining computerized data including personal info. not owned must immediately notify information owner/licensee of any system breach immediately following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person.	**Exempts from act's security breach subchapter** businesses regulated by state or federal law that provides greater protection to personal info. and at least as thorough disclosure requirements for breach.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
California S 1386 **Sponsor:** Peace(D) **Introduced:** 2/12/02 **Enacted:** 09/26/02 **Act/Chapter Number:** 915 **Breach Provisions Effective:** 07/01/03 **Enforcement:** Private right of action. **Penalties:** Damages; civil penalty up to $3K per violation; enjoinment. **Summary:** Requires a State agency, or a person or business that conducts business in the State that owns or licenses computerized data that includes personal info. to disclose in specified ways, any breach of the security of the data to any State resident whose unencrypted personal info. was or may have been acquired by an unauthorized person. **Preempts** all rules, regulations, codes, statutes, or ordinances or all cities, counties, cities and counties, municipalities, and other local agencies. **State agency** security breaches addressed in Section 2 of act. http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html	Person or business that conducts business in CA and owns or licenses computerized data that includes personal info. Security breach defined as unauthorized acquisition of computerized data that compromises security, confidentiality, or integrity of personal info. maintained by person/business. Good faith acquisition of personal info. by employee or agent of person/business for purposes of person/business is not breach of system security, provided personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people; or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when either name or data elements are not encrypted: • SS # • State DL or ID # • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation.** **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person doing business maintaining computerized data including personal info. not owned must immediately notify information owner/licensee of any system breach immediately following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Connecticut S 650 **Sponsor:** Looney (D) **Introduced:** 1/21/05 **Enacted:** 06/24/05 **Act/Chapter Number:** 05-148 **Breach Provisions Effective:** 01/01/06 **Enforcement:** AG action; consumer civil and class action. **Penalties:** Temporary/permanent restraining orders; enjoinment; civil penalties of 5-25K per violation; actual damages; costs and reasonable attorneys' fees. **Summary:** Requires businesses to inform the public if there has been a security breach. **State agency** security breaches not addressed in act. **Identity theft measure** also includes provisions for security freezes and other credit report protections. http://www.cga.ct.gov/2005/act/Pa/2005PA-00148-R00SB-00650-PA.htm	Person who conducts business in CT and owns, licenses or maintains computerized data that includes personal info. **Security breach** defined as unauthorized access to or acquisition of electronic files, media, databases or computerized data containing personal info. when access to personal info. has not been secured by encryption or by any other method or technology that renders personal info. unreadable or unusable.	**Trigger** Personal info. was or is reasonably believed to have been accessed by an unauthorized person. **Method** Written, electronic or telephonic. **Timing** Without unreasonable delay consistent with law enforcement needs and other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people; or • not enough info to provide written electronic or telephonic notice **Substitute Method** Email, website posting and major statewide media notification	Individual's first name or first initial and last name in combination with any one or more of following data: • SS # • State DL or ID # • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records or widely distributed media	Delay for law enforcement **investigation**. Notice is not required if, after an appropriate **investigation** and consultation with law enforcement, it can be reasonably determined that the breach will not likely result in harm to any individual whose info. was acquired and accessed. Safe harbor for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person that maintains computerized data including personal info. not owned shall notify info. owner/ licensee of any security breach of data immediately following discovery if personal info. was or is reasonably believed to have been accessed by unauthorized person.	**In compliance with chapter's security breach notification section** pursuant to rules, regulations, procedures or guidelines established by person's primary or functional federal regulator, provided notice is made in accordance with established security breach procedures if system security breach occurs.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Delaware H 116 **Sponsor:** Gilligan **Introduced:** 4/1405 **Enacted:** 06/28/05 **Act/Chapter Number:** 61 **Breach Provisions Effective:** 06/28/05 **Enforcement:** AG action. **Penalties:** Direct economic damages. **Summary:** Requires individual or commercial entity that conducts business in Delaware and that owns/licenses computerized data that includes personal info. about resident of Delaware, when it becomes aware of system security breach, conduct in good faith reasonable and prompt investigation to determine likelihood that personal info. has been or will be misused. Notice shall be given as soon as possible to affected Delaware residents if investigation determines that misuse of info. has occurred or is reasonably likely to occur. **State agency** security breaches included in act via "commercial entity" definition. http://www.delcode.state.de.us/title6/c012b/index.htm#TopOfPage	Individual or commercial entity that conducts business in DE and owns/licenses computerized data that includes personal info. Security breach defined as unauthorized acquisition of unencrypted computerized data that compromises security, confidentiality, or integrity of personal info. maintained by individual or commercial entity. Good faith acquisition of personal info. by an employee/agent of individual or commercial entity for purposes of individual or commercial entity is not a system security breach, provided that personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Misuse of personal info. has occurred or is reasonably likely to occur. **Method** Written, electronic or telephonic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs and other necessary measures. **Substitute Trigger** • cost exceeds $75K, or • affects more than 100K people, or • not enough info to provide written, electronic or telephonic notice **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements, when either the name or the data elements are not encrypted: • SS # • State DL or ID # • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation**. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Individual or commercial entity that maintains computerized data that includes personal info. that individual or commercial entity does not own or license shall give notice to and cooperate with owner/licensee of info. regarding any system security breach immediately following discovery of such, if misuse of personal info. occurred or is reasonably likely to occur. Cooperation includes sharing with owner or licensee info. relevant to breach.	**In compliance with chapter** if regulated by state or federal law, maintains security breach procedures pursuant to laws, rules, regulations, guidance or guidelines established by primary or functional state/federal regulator; and notifies affected residents as per maintained security breach procedures when breach occurs.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Florida H 481 **Sponsor:** Waters (R) **Introduced:** 03/08/05 **Enacted:** 06/14/05 **Act/Chapter Number:** 2005-229 **Breach Provisions Effective:** 07/01/05 **Enforcement:** Dept. of Legal Affairs (AG) action. **Penalties:** Administrative fine per breach not to exceed $500K ($1K /day each day breach goes undisclosed up to 30 days, thereafter $50K for each 30-day period or portion thereof up to 180 days; if notification not made within 180 days, administrative fine up to $500K); failure to document "notice not required" determination liable for administrative fine up to $50K. **Summary:** Relates to undisclosed computer data security breaches. **State agency** security breaches included via "person" definition.. agency breaches of personal info. in custody of gov. agency or subdivision exempt from adminstrative sanctions of act unless governmental agency or subdivision has entered into contract with contractor or 3rd-party administrator to provide governmental services, at which point contractor or 3rd-party administrator is responsible. **Identity theft measure** also includes other non-business identity theft related provisions. http://election.dos.state.fl.us/laws/05laws/ch_2005-229.pdf	Person who conducts business in FL and maintains computerized data that includes personal info. **Security breach** defined as unlawful and unauthorized acquisition of computerized data that materially compromises security, confidentiality, or integrity of personal info. maintained by person. Good faith acquisition of personal info. by employee/ agent of person is not security system breach, provided info. is not used for purpose unrelated to business or subject to further unauthorized use.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by unauthorized person. **Method** Written or electronic notice. **Timing** Notice must be made ***no later than 45 days*** from determination of breach unless otherwise provided, including law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K, or • affects more than 500K people, or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	**Individual's first** name, first initial and last name, or any middle name and last name, in combination with any one or more of following data elements when data elements are not encrypted: • SS # • State DL or ID # • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records or widely distributed media	Delay for law enforcement **investigation**. Notice not required if determintion is made, after investigation or consultation with law enforcement, that breach has not or will not likely result in harm to individuals. Determination must be documented in writing and maintained for 5 years. Safe harbor for providing method of notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person who maintains computerized data including personal info. on behalf of another business entity shall disclose to business entity for which info. is maintained any system security breach as soon as practicable, **but no later than 10 days** following determination, if personal info was or is reasonably believed to have been acquired by unauthorized person (see statute for further info. regarding notification responsibility). If notice required to more than 1,000 persons at a time, then also must notify CRA of notice timing, distribution and content.	**In compliance with chapter's security breach notification section** provided notice is made in accordance with person's policies or rules, regulations, procedures or guidelines established by person's primary or functional federal regulator if system security breach occurs.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Georgia S 230 **Sponsor:** Hamrick (R) **Introduced:** 02/22/05 **Enacted:** 05/05/05 **Act/Chapter Number:** 163 **Breach Provisions Effective:** 05/05/05 **Enforcement:** Act is silent. **Penalties:** Act is silent. **Summary:** Requires info. brokers give notice to consumers of certain security breaches. **State agency** security breaches not specifically addressed in act; governmental agencies whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes are exempt from "info. broker" definition. http://www.legis.ga.gov/legis/2005_06/versions/sb230_AP_12.htm	**Info. broker** that maintains computerized data including personal info. Info. broker defined as person or entity who for monetary fees/dues collects, assembles, evaluates, compiles, reports, transmits, transfers or communicates info. concerning individuals for primary purpose of furnishing to nonaffiliated 3rd parties. **Security breach** defined as unauthorized acquisition of individual's computerized data compromising security, confidentiality, or integrity of individual's personal info. maintained by info. broker. Good faith acquisition of personal info. by info. broker employee/ agent for info. broker purposes is not system security breach, provided personal info. is not used/subject to unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic notice. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K, or • affects more than 500K people, or • not enough info. to provide written or electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one/more of following data elements when either name or data elements are not encrypted or redacted: • SS # • State DL # or ID# • account, credit card or debit card # if usable w/out additional identifying info., access codes or passwords • account passwords or personal ID #s or other access codes • any above items when not in connection with individual's first name or first initial and last name, if info. compromised would be sufficient to perform or attempt to perform ID theft. Excludes info. publicly available from federal, state or local government records	Delay for law enforcement **Investigation.** Safe harbor for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person that maintains computerized data on behalf of info. broker, including personal info. not owned, shall notify info. broker of any security breach of data immediately following discovery if personal info. was or is reasonably believed to have been, acquired by unauthorized person. If notice required for more than 10,000 persons at a time, then also must notify CRAs of notice timing, distribution and content.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Illinois H 1633 **Sponsor:** Madigan (D) **Introduced:** 02/14/05 **Enacted:** 06/16/05 **Act/Chapter Number:** 94-0036 **Breach Provisions Effective:** 01/01/06 **Enforcement:** AG action; private right of action. **Penalties:** Enjoinment; injunction, restitution; revocation; forfeiture or suspension of any license, charter, franchise, certificate or other evidence of authority of to do business in state; civil fine up to $50K per violation; additional fine up to $10K per violation against person over 65 years old; actual economic damages (punitive damages, injunctive relief, and/or reasonable attorney's fees and costs). **Summary:** Provides that any data collector shall notify a resident if there has been a breach of the security of the system data, without regard for whether the data has been accessed for legal or illegal purposes. **State agency** security breaches included in act via "data collector" definition. http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=094-0036&print=true	Any data collector that owns/licenses personal info. ...cerning IL ...dent. Data ...ector definition includes financial institutions. Security breach defined as unauthorized acquisition of computerized data compromising security, confidentiality, or integrity of personal info. maintained by data collector. Does not include good faith acquisition of personal info. by data collector employee/ agent for data collector's legitimate purpose, provided personal info. is not used for purpose unrelated to data collector's business or subject to further unauthorized disclosure.	Trigger **Discovery or notification of breach alone triggers notice requirement; no further standard articulated.** Method Written or electronic notice. Timing Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. Substitute Trigger • cost exceeds $250K, or • affects more than 500K people, or • not enough info to provide written/ electronic notice. Substitute Method Email, website posting and major statewide media notification	Individual's first name or first initial and last name in combination with any one or more of following data elements when either name or data elements are not encrypted or redacted • SS # • State DL# or ID# • account, credit card or debit card #, or account or credit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Does NOT allow delay for law enforcement investigation. Safe harbor for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	3rd Party Notice Data collector that maintains computerized data including personal info. not owned shall notify information owner or licensee of any security breach of data immediately following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Louisiana S 205 **Sponsor:** Duplessis (D) **Introduced:** 04/15/05 **Enacted:** 07/12/05 **Act/Chapter Number:** 499 **Breach Provisions Effective:** 01/01/06 **Enforcement:** Private right of action. **Penalties:** Actual damages, based on rules to be promulgated by AG. **Summary:** Database Security Breach Notification Law. **State agency** security breaches included. http://www.legis.state.la.us/billdata/streamdocument.asp?did=320093	Person that conducts business in LA or owns or licenses computerized data that includes personal info. **Security** breach defined as compromise of security, confidentiality, or integrity of computerized data that results in, or is reasonable basis to conclude has resulted in, unauthorized acquisition of and access to personal info. maintained by agency/person. **Good faith** acquisition of personal info. by agency/person employee/ agent for purposes of agency/person is not system security breach, provided that personal info is not used for, or subject to, unauthorized disclosure.	**Trigger** Unencrypted or not redacted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people; or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when name or data elements are not encrypted or redacted: • SS # • State DL # • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **Investigation.** Notice not required if, after reasonable **investigation**, person or business determines that no reasonable likelihood of harm to customers. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Agency/person that maintains computerized data which includes personal info. not owned shall notify information owner/licensee of any security breach of data following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person.	**In compliance with chapter** for financial institutions subject to and in compliance with federal interagency banking guidance.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Maine H 1180a **Sponsor:** Pelletier-Simpson (D) **Introduced:** 05/12/05 **Enacted:** 06/10/05 **Act/Chapter Number:** 379 **Breach Provisions Effective:** 01/31/06 **Enforcement:** Appropriate state regulator action for licensed/regulated info. brokers; AG action for all other info. brokers. **Penalties:** Up to $500 fine per violation up to $2.5K for each day information broker is in violation; equitable relief; enjoinment. **Summary:** Requires info. broker engaged in business in Maine that is in possession of electronic data containing personal info. to disclose any unauthorized acquisition or suspected unauthorized acquisition of that personal info. to a person whose personal info. may have been acquired. Report due 02/01/06 addressing business data security and security breaches. **State agency** security breaches not specifically addressed in act, governmental agencies whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes are exempt from "info. broker" definition. Report due 02/01/06 addressing security of information maintained by State Government. http://janus.state.me.us/legis/ros/lom/LOM123rd/9Pub351-400/Pub351-378.htm#P1036_197584	**Info. broker** that maintains computerized data including personal info. Info. broker defined as person who for monetary fees/dues engages in business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating individual's info. for primary purpose of furnishing to nonaffiliated 3rd parties. **Security breach** defined as unauthorized acquisition of individual's computerized data that compromises security, confidentiality or integrity of individual's personal info. maintained by info. broker. Good faith acquisition of personal info. by info. broker employee or agent for purposes of info. broker is not system security breach if personal info. is not used for or subject to unauthorized disclosure.	**Trigger** Personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $5K; or • affects more than 1000 people; or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when name or data elements are not encrypted or redacted: • SS # • State DL# or ID# • account, credit card or debit card # if usable w/out additional identifying info., access codes or passwords • account passwords or personal ID #s or other access codes • any above items when not in connection with individual's first name or first initial and last name, if info. compromised would be sufficient to perform or attempt to perform ID theft. Excludes info. publicly available from government records or widely distributed media.	Delay for law enforcement **Investigation.** **No safe harbor** provision.	**3rd Party Notice** Person that maintains computerized data not owned on behalf of info. broker, and data includes personal info., shall notify info. broker of any data security breach following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person. When security breach notification is required, info. broker must also notify appropriate state regulators within Dept. of Professional and Financial Regulation, or AG if info. broker not [illegible] by Dept. [illegible] required for more than 1,000 persons at a time, then info. broker also must notify CRAs	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Minnesota H 2121 **Sponsor:** Johnson J (R) **Introduced:** 3/29/05 **Enacted:** 06/02/05 **Act/Chapter Number:** 167 **Breach Provisions Effective:** 01/01/06 **Enforcement:** AG action; private right of action. **Penalties:** Investigation; injunction; civil penalties up to $25K; actual damages; investigation costs; reasonable attorney's fees; other equitable relief. **Summary:** Requires businesses to notify persons whose personal info. has been disclosed to unauthorized persons. **State agency** security breaches are addressed in enacted **2005 HF 225** (Chapter 163). http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP&year=2005&chapter=167	Person/business that conducts business in MN and owns or licenses any data that includes personal info. Security breach defined as unauthorized acquisition of computerized data compromising security, confidentiality, or integrity of personal info. maintained by person/business. Good faith acquisition of personal info. by person/business employee or agent for purposes of person/business is not security system breach, provided personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people, or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification	Individual's first name or first initial and last name in combination with any one or more of following data elements when name or data elements is not encrypted • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password Excludes info publicly available from federal, state or local government records	Delay for law enforcement **investigation**. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person/business that maintains computerized data including personal info. not owned shall notify information owner/licensee of any security breach of data following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person. If notice required for more than 500 persons at a time, then also must notify CRAs **within 48 hours** of notice timing, distribution and content.	**Exempts from chapter** financial institutions as defined by US Code Title 15, section 6809(3), GLBA Title V.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Montana H 732 **Sponsor:** Roberts (R) **Introduced:** 02/15/05 **Enacted:** 04/28/05 **Act/Chapter Number:** 518 **Breach Provisions Effective:** 03/01/06 **Enforcement:** AG action. **Penalties:** investigation; injunction; restrainment; voluntary compliance; civil fines up to $10K. **Summary:** Requires businesses to report a breach of computer security. **State agency** security breaches not addressed in act. **Identity theft measure** also includes provisions related to credit report blocks, credit card solicitation/renewal protections, and destruction of business records. http://data.opi.state.mt.us/bills/2005/billhtml/HB0732.htm	Person or business that conducts business in MT and owns or licenses computerized data that includes personal info. **Security breach** defined as unauthorized acquisition of computerized data that materially compromises security, confidentiality or integrity of personal info. maintained and causes or is reasonably believed to cause loss or injury to a Montana resident. Good faith acquisition of personal info. by employee/agent of person/business for purposes of person/business is not data system security breach, provided personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written, electronic or telephonic. **Timing** Without unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K, or • affects more than 500K people, or • not enough info to provide written, electronic or telephonic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when name or data elements are not encrypted: • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation**, but law enforcement agency must specifically request notification delay. **Safe harbor** for providing notice pursuant to internal info. security policy that does not unreasonably delay notice.	**3rd Party Notice** Person/business that maintains computerized data including personal info. not owned shall notify information owner/licensee of any security breach of data immediately following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person. If notice to Montana resident implies individual may obtain report from CRA, then business shall coordinate with CRA on timing, content and distribution of notice.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Nevada A 1a **Sponsor:** Assembly Committee of the Whole **Introduced:** 6/07/05 **Enacted:** 06/17/05 **Act/Chapter Number:** 6 **Breach Provisions Effective:** 06/17/05 **Enforcement:** N/A -see SB 347 **Penalties:** N/A -see SB 347 **Summary:** Makes technical corrections to certain legislative measures relating to protection of Social Security numbers, drivers licenses, ID cards and financial account numbers; amends measures relating to discipline of medical licensees, payday loans, collection agencies, felony DUI sentencing and credit unions. **Repeals enacted 2005 AB 334 (Chapter 486), Section 6, regarding business security breaches, and amends enacted 2005 SB 347, Section 21, regarding "personal info." definition.** http://www.leg.state.nv.us/22ndSpecial/bills/AB/AB1_EN.pdf	N/A -see SB 347	N/A -see SB 347	Individual's first name or first initial and last name in combination with any one or more of following data elements when name and data elements are not encrypted: • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password (employer identification # included in Section 21 of SB 347 as originally enacted is removed) Excludes info. that is publicly available.	N/A -see SB 347	N/A -see SB 347	N/A -see SB 347

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Nevada S 347 **Sponsor:** Wiener (D) **Introduced:** 3/25/05 **Enacted:** 06/17/05 **Act/Chapter Number:** 485 **Breach Provisions Effective:** 01/01/06 **Enforcement:** AG or county DA action. **Penalties:** Injunction; data collector may bring action against security breach perpetrator for damages/restitution. **Summary:** Requires data collectors provide notification of any breach of security involving system data. **State agency** security breaches are addressed in enacted **2005 AB 334** (Chapter 486). **Identity theft measure** also includes provisions related to financial forgery laboratories, credit card issuer identity theft policies, protection and destruction of business records containing personal info., electronic data encryption, and identity theft penalties. http://www.leg.state.nv.us/73rd/bills/SB/SB347_EN.pdf	Data collector that owns or licenses computerized data which includes personal info. Data collector by definition includes financial institution. Security breach defined as unauthorized acquisition of computerized data that materially compromises security, confidentiality or integrity of personal info. maintained by data collector. Does not include good faith acquisition of personal info. by employee/agent of data collector for data collector's legitimate purpose, so long as personal info. is not used for purpose unrelated to data collector or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people, or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when name and data elements are not encrypted: • SS or employer identification # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password (employer identification # removed via amendments in **AB 1A**) Excludes info. that is publicly available.	Delay for law enforcement **investigation**. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Data collector maintaining computerized data including personal info. data collector doesn't own must immediately notify information owner/licensee when breach is discovered if personal info. was or is reasonably believed to have been acquired by unauthorized person. If notice required for more than 1,000 persons at a time, then also must notify CRAs of time notification is distributed and notification content.	**In compliance with chapter's security breach notification section** for persons subject to and in compliance with GLBA.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
New Jersey A 4001 **Sponsor:** Watson-Coleman (D) **Introduced:** 05/05/05 **Enacted:** 09/22/05 **Act/Chapter Number:** 2005-226. **Breach Provisions Effective:** 01/01/06 **Enforcement:** AG action, private right of action. **Penalties:** Injunction; civil penalties up to $10K for 1st offense and up to $20K for 2nd and each subsequent offense; damages; reasonable attorneys' fees, filing fees and reasonable costs of suit. **Summary:** Requires notification of unencrypted personal info. da'a security breaches. **State agency** security breaches included in act via "public entity" definition. **Identity theft measure** includes provisions related to identity theft related police reports and judicial determinations of factual innocence, identity theft victim database, security freezes, CRA's release of consumer's credit header info., business disposal of consumer's personal info., and SSN use restrictions. http://www.njleg.state.nj.us/2004/Bills/PL05/226_.HTM	Business or public entity doing business in NJ that compiles or maintains computerized records that include personal info. **Security breach** defined as unauthorized access to electronic files, media or data containing personal info. that compromises security, confidentiality or integrity of personal info. when access to personal info. has not been secured by encryption or by any other method or technology that renders personal info. unreadable or unusable. Good faith acquisition of personal info. by employee/ agent of business for legitimate business purpose is not breach of security, provided personal info. is not used for purpose unrelated to business or subject to further unauthorized disclosure.	**Trigger** Personal info. was or is reasonably believed to have been accessed by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K, or • affects more than 500K people, or • not enough info to provide written/ electronic notice **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements. • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password • dissociated data, if linked, and means to link dissociated data is accessed in connection with access to dissociated data Excludes personal info. made available to general public from federal, state or local government records, or widely distributed media.	Delay for law enforcement **investigation**, but law enforcement agency must specifically request notification delay. Notice not required if business or public entity establishes that misuse of info. is not reasonably possible. Determination must be documented in writing and maintained for 5 years. Safe harbor for providing notice pursuant to an internal info security policy and notification is consistent with state requirements.	**3rd Party Notice** Business or public entity compiling or maintaining computerized records including personal info. on behalf of another business or public entity must immediately notify business or public entity, who shall notify its NJ customers when breach is discovered, if personal info. was or is reasonably believed to have been accessed by unauthorized person. If notice required, must report to Division of State Police in Department of Law and Public Safety prior to notifying customers. If notice required for more than 1,000 persons at a time, then also must notify CRAs of notices' timing, distribution and content.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
New York City 0141-2004 **Sponsor:** NYC Council Member **Introduced:** 02/04/04 **Enacted:** 05/19/05 **Act/Chapter Number:** **Breach Provisions Effective:** 09/20/05 **Enforcement:** NYC Commissioner civil action. **Penalties:** Fine of not more than $500; civil penalty of $100 for each violation. **Summary:** Requires businesses to notify consumers in the event of a security breach of personal identifying info. **Identity theft measure** also includes provisions related to disposal of records containting consumer's personal info. http://webdocs.nyccouncil.info/textfiles/Int%200141-2004.htm	Any person required to be licensed by Department of Consumer Affairs, or pursuant to provisions of state law enforced by Department, that owns/leases, or maintains but does not own, data that includes personal identifying info. Security breach defined as unauthorized possession of personal identifying info. that compromises security, confidentiality or integrity of such info. Good faith or inadvertent possession of any personal identifying info. by employee/agent of licensee for legitimate purposes of business of licensee shall not constitute breach of security.	Trigger Personal identifying info. was or is reasonably believed to have been acquired by an unauthorized person. Method Written, electronic or telephonic. Timing As soon as practicable by method reasonable under the circumstances. Substitute Trigger Disclosure is impracticable or inappropriate given circumstances of breach and victims' identity. Substitute Method Via mechanism of licensee's choosing provided mechanism is reasonably targeted to individual in manner that does not further compromise integrity of personal info. disclosed and has been approved, or is in compliance with rules promulgated, by Commissioner.	Includes all of the following data, notwithstanding method by which such information is maintained: • DOB • SS # • State DL or ID # • financial account, credit card, debit card, ATM # or code • personal ID # • mother's maiden name • comptr passwrd • elec. signature • biometric data	No safe harbor provision.	3rd Party Notice Person required to be licensed by Consumer Affairs Dept., or pursuant to provisions of state law enforced by Dept. that maintains but does not own data that includes personal identifying info. must notify data owner, lessor or licensor when security breach is discovered, if personal identifying info. was or is reasonably believed to have been acquired by unauthorized person. Must immediately disclose to Department of Consumer Affairs and police department any security breach following discovery of such breach if such personal identifying info. is reasonably believed to have been acquired by unauthorized person.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
New York A 4254A **Sponsor:** Brennan (D) **Introduced:** 02/09/05 **Enacted:** 08/09/05 **Act/Chapter Number:** 442 **Breach Provisions Effective:** 12/07/05 **Enforcement:** AG action. **Penalties:** Injunction; enjoinment; restrainment; actual damages, including consequential financial losses, if notification was not provided, if court determines violation occurred knowingly/recklessly, allowed civil penalties of greater of $5K or $10 per instance of failed notification up to $150K. **Summary:** Requires any state agency or business which owns or licenses a computerized database which includes vulnerable personal info. shall disclose any breach of security of such system to any resident of New York state whose unencrypted personal info. may have been acquired by an unauthorized person. **Preempts** local laws, ordinances and codes. **State agency** security breaches addressed in Section 3 of act. See enacted **2005 S 5827** (Chapter 491) for additional clarification. http://assembly.state.ny.us/leg/?bn=A04254&sh=t	Person or business that conducts business in NY and owns or licenses computerized data that includes personal info. Security breach defined as unauthorized acquisition or acquisition without valid authorization of computerized data that compromises security, confidentiality, or integrity of personal info. maintained by business. Good faith acquisition of personal info. by employee or agent of business for purposes of business is not a security breach, provided private info. is not used or subject to unauthorized disclosure.	Trigger Unencrypted private info. is reasonably believed to have been acquired by unauthorized person. See enacted **2005 S 5827** (Chapter 491) for clarification. Method Written, telephonic, or electronic for person who has expressly consented to electronic notice. Log required for electronic/telephonic notice. ***Statute specifies notice content.*** Timing Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. Substitute Trigger • cost exceeds $250K; or • affects more than 500K people, or • not enough info to provide written, electronic or telephonic notice. Substitute Method Email, website posting and major statewide media notification.	Private info. in combination with any one or more of following data elements, when either personal info. or data element is not encrypted or encrypted with an encryption key that has also been acquired: • SS # • State DL# or ID# • non-driver ID # • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records. "Personal info." shall mean any info. concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.	Delay for law enforcement **investigation**. No safe harbor **provision**.	3rd Party Notice Person or business maintaining computerized data including private info. not owned must immediately notify owner or licensee upon breach discovery if private info. was or is reasonably believed to have been acquired by unauthorized person. If any notice required, AG, Consumer Protection Board and Cyber Security and Critical Infrastructure Coord. Office must be notified of timing, distribution and content of notice and approximate number affected. If notice required for more than 5,000 persons at a time, then also must notify CRAs of notice timing, distribution, content and approximate number of affected persons. **CRA notification not limited to 3 major CRAs - AG will compile CRA list.**	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
New York S 5827 **Sponsor:** Fuschillo (R) **Introduced:** 06/19/05 **Enacted:** 08/09/05 **Act/Chapter Number:** 491 **Breach Provisions Effective:** 12/07/05 **Enforcement:** AG action. **Penalties:** N/A - see **A 4254**. **Summary:** Makes technical changes to certain provisions of Info. Security Breach and Notification Act; clarifies definition of breach of security system; changes reference of person or entity to state entity in Section 3; provides for telephone notification to affected persons and log of each notification; clarifies awarding of damages. http://assembly.state.ny.us/leg/?bn=S05827&sh=t	N/A - see **A 4254**.	Trigger Such business may consider following factors, among others: (1) indications that info. is in physical possession and control of un-authorized person, such as lost or stolen computer or other device containing info.; or (2) indications that info. has been downloaded or copied; or (3) indications that info. was used by unauthorized person, such as fraudulent accounts opened or instances of ID theft reported.	N/A - see **A 4254**.	N/A - see **A 4254**.	N/A - see **A 4254**.	N/A - see **A 4254**.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
North Carolina S 1048 **Sponsor:** Clodfelter (D) **Introduced:** 03/24/05 **Enacted:** 09/21/05 **Act/Chapter Number:** 2005-414. **Breach Provisions Effective:** 12/01/05 **Enforcement:** AG action; private right of action limited to injured individuals. **Penalties:** Injunction; $5K civil penalty per violation, attorney fees; treble damages for injured consumer. **Summary:** Requires notification of personal info. security breaches. **State agency** security breaches not addressed in act. "Business" definition specifically exempts state agencies. **Identity theft measure** also includes provisions related to security freezes, business disposal of consumer's personal info., and SSN use restrictions. http://www.ncleg.net/Sessions/2005/Bills/Senate/HTML/S1048v6.html	Business that owns or licenses personal info. of NC residents or business that conducts business in NC that owns/licenses personal info. in any form, **whether computerized, paper, otherwise.** Security breach is defined as unauthorized access to and acquisition of unencrypted & unredacted records or data (or encrypted records/ data along with confidential process/key) containing personal info. where illegal use has occurred or is reasonably likely to occur or that creates material risk of harm to consumer. Good faith acquisition of personal info. by employee/agent of business for legitimate purpose is not security breach, provided that personal info. is not used for purpose other than lawful business and is not subject to further unauthorized disclosure.	**Trigger** Personal info. was acquired by unauthorized person where illegal use of personal info. has occurred or is reasonably likely to occur or that creates material risk of harm to consumer. **Method** Written, telephonic or electronic for person who has expressly consented to electronic notice. ***Statute specifies notice content.*** **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K, or • affects more than 500K people, or • not enough info to provide written, electronic or telephonic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with identifying info. as defined in G.S. 14-113.20(b): • SS # • State DL# • Checking, savings, credit/debit card #s • PIN code • biometric data • fingerprints • digital signature • passwords • electronic ID #s, email names or addresses, Internet account numbers or identification names, parent's legal surname prior to marriage, or password if it would permit access to person's financial account or resources. Excludes personal info. available to general public from federal, state or local government records; and publicly available directories containing info. individual has voluntarily consented to have publicly disseminated.	Delay for law enforcement **investigation**, provided law enforcement agency delay request is made in writing or business documents such request contemporaneously in writing, including name of law enforcement officer making request and officer's law enforcement agency engaged in investigation. No **safe harbor** provision.	**3rd Party Notice** Business that maintains or processes records/data including personal info. on behalf of personal info. owner or licensee must immediately notify owner or licensee upon breach discovery consistent with law enforcement needs. If notice required for more than 1,000 persons at a time, then also must notify AG's office and CRAs of notice timing, distribution and content.	**In compliance with act's security breach section** for financial institutions subject to and in compliance with federal interagency banking guidance.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
North Dakota S 2251 **Sponsor:** Trenbeath (R) **Introduced:** 01/17/05 **Enacted:** 04/22/05 **Act/Chapter Number:** 447 **Breach Provisions Effective:** 06/01/05 **Enforcement:** AG action; private right of action. **Penalties:** Investigation; injunction; restrainment; civil penalties of $1-5K per violation; damages and adjudicative proceeding/hearing costs; treble damages. **Summary:** Requires disclosure to consumers of a breach in security by businesses maintaining personal identifying info. in electronic form. **State agency** security breaches not addressed in act. http://www.legis.nd.gov/assembly/59-2005/session-laws/documents/SALES.pdf#CHAPTER447	Any person that conducts business in ND and owns or licenses computerized data that includes personal info. Security breach is defined as unauthorized acquisition of computerized data when access to personal info. has not been secured by encryption or any other method or technology that renders electronic files, media, or data bases unreadable/ unusable. Good-faith acquisition of personal info. by employee/agent of person is not a system security breach if personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people; or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when name and data elements are not encrypted • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password • DOB • mother's maiden name • employee ID # • electronic signature Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation**. Safe harbor for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	3rd Party Notice Person that maintains computerized data including personal info. on behalf of personal info. owner or licensee must immediately notify owner or licensee upon breach discovery, if personal info. was or is reasonably believed to have been acquired by an unauthorized person.	**In compliance with chapter** for financial institutions subject to, examined for, and in compliance with federal interagency banking guidance.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Ohio H 104 **Sponsor:** Martin (R) **Introduced:** 03/01/05 **Enacted:** 11/17/05 **Act/Chapter Number:** 43 **Breach Provisions Effective:** 02/17/06 **Enforcement:** AG action. **Penalties:** Investigation, restrainment, injunction; costs; civil penalties for intentional/reckless noncompliance of $1K/day up to 60 days of noncompliance, $5K/day after 60 days, and $10K/day after 90 days. **Summary:** Requires disclosure to consumers of a breach in security by businesses maintaining personal identifying info. in electronic form. **Preempts** all rules, regulations, resolutions, codes, and ordinances of all counties, municipal corporations, townships, and agencies of counties, municipal corporations, and townships. **State agency** security breaches addressed in Section 1, Subsection 1347.12, of act. http://www.legislature.state.oh.us/bills.cfm?ID=126_HB_104	Person that conducts business in OH and owns or licenses computerized data that includes personal info. Security breach is defined as unauthorized access to and acquisition of computerized data that compromises security or confidentiality of personal info. owned/licensed by person and that causes, reasonably is believed to have caused, or reasonably is believed will cause material risk of ID theft or other fraud to person or property of resident of state. Good-faith acquisition of personal info. by employee/agent of person is not a system security breach if personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted, unredacted, or altered to be unreadable personal info. was or is reasonably believed to have been accessed/acquired by unauthorized person, if such causes or reasonably is believed will cause material risk of ID theft or other fraud to resident. **Method** Written, electronic (if primary method of communication), telephonic, or via contract provision that doesn't conflict with any section provision. **Timing** **No later than 45 days from breach discovery or notification** and within most expedient time possible consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people; or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and ***specified*** major statewide media notification.	Individual's first name or first initial and last name in combination with and linked to any one or more of following data elements, when data elements are not encrypted, redacted, or altered by any method or technology in such manner that data elements are unreadable: • SS # • State DL# or ID# • account, credit card or debit card # in combination with and linked to required access/security code or password Excludes info. publicly available from federal, state or local government records, or specified media that are widely distributed.	Delay for law enforcement **investigation**. **No safe harbor provision.**	**3rd Party Notice** Person that is custodian or stores computerized data including personal info. shall notify owner or governmental entity of any system security breach in expeditious manner, if personal info. was or reasonably is believed to have been, accessed and acquired by unauthorized person and if such causes or reasonably is believed will cause material risk of ID theft or other fraud to resident. If notice required for more than 1,000 persons at a time, then also must notify CRAs of notice timing, distribution and content.	**Exempts from act's security breach notification section** any financial institution, trust company, or credit union or any affiliate of 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 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.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Pennsylvania S 712 **Sponsor:** Wonderling (R) **Introduced:** 06/03/05 **Enacted:** 12/22/05 **Act/Chapter Number:** 2005-94 **Breach Provisions Effective:** 06/20/06 **Enforcement:** AG action; private right of action. **Penalties:** Civil penalties of $1-5K per violation; actual damages, treble damages; reasonable costs and attorney fees. **Summary:** Provides for the notification of residents whose personal information data was or may have been disclosed due to a security system breach. Relates to data that materially compromises the security or confidentiality of personal information. Imposes penalties. Allows telephonic notice under certain circumstances. Requires notice of the breach if encrypted information is accessed in an unencrypted form. Relates to vendor notification regarding breach of a security system. **Preempts** all rules, regulations, codes, statutes or ordinances of all cities, counties, municipalities and other local agencies within Commonwealth regarding matters expressly set forth in Act. **State agency** security breaches included in act via "entity" definition. http://www2.legis.state.pa.us/WU01/LI/BI/BT/2005/0/SB0712P1410.pdf	Entity that conducts business in PA and maintains, stores or manages computerized data that includes personal info. Security breach is defined as unauthorized access and acquisition of computerized data that materially compromises security or confidentiality of personal info. maintained by entity as part of database of personal info. regarding multiple individuals and that causes or entity reasonably believes has caused or will cause loss/injury to any state resident. Good faith acquisition of personal info. by entity employee or agent for purposes of entity is not system security breach if personal info. is not used for purpose other than lawful purpose of entity and is not subject to further unauthorized disclosure.	**Trigger** Unencrypted or unredacted personal info. was or is reasonably believed to have been accessed/acquired by unauthorized person. **Method** Written, telephonic (if customer can reasonably expect to receive and specified info. is provided), or email (prior business relationship only). **Timing** Notice shall be made without unreasonable delay, except for law enforcement investigation delay or in order to take any measures necessary to determine scope of breach and to restore data system's reasonable integrity. **Substitute Trigger** • cost exceeds $100K; or • affects more than 175K people, or • no sufficient contact info. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following unencrypted or unredacted data elements: • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement agency **investigation** if agency determines and advises enity in writing. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with Act's notification requirements.	**3rd Party Notice** Vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any system security breach following discovery by vendor to entity on whose behalf vendor maintains, stores or manages data. Entity shall be responsible for making determinations and discharging any remaining duties under Act. If notice required for more than 1,000 persons at a time, then also must notify CRAs of notice timing, distribution and number.	**In compliance with act** for financial institutions subject to and in compliance with federal interagency banking notification guidance, or entity in compliance with notification requirements pursuant to rules, regulations, procedures or guidelines established by entity's primary or functional Federal regulator.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Rhode Island H 6191A **Sponsor:** Gemma (D) **Introduced:** 03/09/05 **Enacted:** 07/10/05 **Act/Chapter Number:** 225 **Breach Provisions Effective:** 03/01/06 **Enforcement:** AG action. **Penalties:** Civil fines of not more than $100 per occurrence up to $25K. **Summary:** Requires disclosure of computerized unencrypted personal info. data security breaches. **State agency** security breaches included in act. http://www.rilin.state.ri.us/PublicLaws/law05/law05225.htm	Any state agency or person doing business in RI that owns, maintains or licenses computerized data that includes personal info. **Security breach** is defined as unauthorized acquisition of unencrypted computerized data compromises the security,confidentiality, or integrity of personal info. maintained by state agency or person. Good faith acquisition of personal info. by employee/agent of agency/person for purposes of agency/person is not system security breach, provided personal Info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person or person without authority to acquire said info., and such breach poses significant risk of ID theft. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent w/ law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $25K, or • affects more than 50K people, or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when either name or data elements are not encrypted: • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password Does ***not*** exclude info. that is publicly available.	Delay for law enforcement **investigation**. Notification not required if after appropriate **investigation** or after consultation with relevant federal, state, or local law enforcement agencies, determination is made that breach has not and will not likely result in significant risk of ID theft to individuals whose personal info. has been acquired. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	3rd Party Notice State agency or person that maintains computerized unencripted data including personal info. that state agency or person does not own shall notify owner or licensee of info. of any data security breach which poses significant risk of ID theft immediately following discovery, if personal info. was or is reasonably believed to have been acquired by unauthorized person.	**In compliance with chapter's security breach notification requirements** for any person that maintains security breach procedure pursuant to rules, regulations, procedures or guidelines established by primary or functional regulator, as defined in 15 USC 6809(2) and provides notice in accordance thereto when breach occurs. **In compliance with chapter** for financial institutions or their affiliates subject to, examined for, and in compliance with federal interagency banking guidance.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Tennessee S 2220 **Sponsor:** Herron (D) **Introduced:** 02/17/05 **Enacted:** 06/18/05 **Act/Chapter Number:** 473 **Breach Provisions Effective:** 07/01/05 **Enforcement:** AG action, private right of action. **Penalties:** Injunction; restrainment; enjoinment; civil penalties of whichever of following is greater: $10K, $5K/day for each day person's ID has been assumed, 10 times amount obtained or attempted to be obtained by person using ID theft, civil penalties up to $5K per knowing and willful violation; attorneys' fees and costs; damages, including treble. **Summary:** Requires persons, businesses or government agencies that discover a breach of info. security resulting in disclosure of unencrypted personal info. about persons to unauthorized third parties to provide notice of such disclosure. **State agency** security breaches included in act via "info. holder" definition. http://www.legislature.state.tn.us/bills/currentga/Chapter/PC0473.pdf	"Info. holder" (person or business) that conducts business in TN and owns or licenses computerized data that includes personal info. Security breach is defined as unauthorized acquisition of unencrypted computerized data that materially compromises security, confidentiality, or integrity of personal info. maintained by info. holder. Good faith acquisition of personal info. by employee/ agent of info. holder for purposes of info. holder is not system security breach, provided personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people; or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when either name or data elements are not encrypted: • SS # • State DL # • • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation.** **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Info. holder that maintains computerized data including personal info. not owned shall notify owner or licensee of info. of any data security breach if personal info. was or is reasonably believed to have been acquired by unauthorized person. If notice required for more than 1,000 persons at a time, then also must notify CRAs of notice timing, distribution and content.	**Exempts from chapter** financial institutions subject to GLBA Title V.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Texas S 122 **Sponsor:** Hinojosa (D) **Introduced:** 01/11/05 **Enacted:** 06/17/05 **Act/Chapter Number:** 294 **Breach Provisions Effective:** 09/01/05 **Enforcement:** AG action. **Penalties:** Restrainment; injunction; civil penalties of $2-50K per violation; reasonable expenses, attorney's fees, court and investigatory costs. **Summary:** Requires notification of unencrypted computerized personal info. data security breaches. **State agency** security breaches not addressed in act. **Identity theft measure** also includes provisions requiring businesses protect/safeguard any personal identifying info. collected/maintained, and to implement/maintain reasonable procedures, including taking any appropriate corrective action to prevent unlawful use of any personal identifying info. (exempts financial institutions as defined by 15 U.S.C. Section 6809(3). http://www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&BILLSUFFIX=00122&VERSION=5&TYPE=B	Person that conducts business in TX and owns or licenses computerized data that includes sensitive personal info. Security breach is defined as unauthorized acquisition of computerized data that compromises security, confidentiality, or integrity of sensitive personal info. maintained by person. Good faith acquisition of sensitive personal info. by employee agent of person or business for purposes of person is not system security breach unless sensitive personal info. is used or disclosed by person in unauthorized manner.	**Trigger** Sensitive personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** As quickly as possible consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people, or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following items, if name and items are not encrypted: • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation**. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person that maintains computerized data including sensitive personal info. not owned shall notify owner or licensee of info. of any data security breach if sensitive personal info. was or is reasonably believed to have been acquired by unauthorized person. If notice required for more than 10,000 persons at a time, then also must notify CRAs of notice timing, distribution and content.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Washington S 6043 **Sponsor:** Brandland (R) **Introduced:** 2/24/05 **Enacted:** 05/10/05 **Act/Chapter Number:** 368 **Breach Provisions Effective:** 07/24/05 **Enforcement:** Private right of action. **Penalties:** Damages; enjoinment. **Summary:** Requires disclosure of any breach of security of a system following discovery by any agency or business who computerizes data that includes personal info. to the resident of this state whose unencrypted personal info. was, or is reasonably believed to have been, acquired by an authorized person. **State agency** security breaches addressed in Section 1 of act http://www.leg.wa.gov/pub/billinfo/2005-06/Pdf/Bills/Session%20Law%202005/6043-S.sl.pdf	Person or business that conducts business in WA and owns or licenses computerized data that includes personal info. Security breach is defined as unauthorized acquisition of computerized data that compromises security, confidentiality, or integrity of personal info. maintained by person/ business. Good faith acquisition of personal info. by employee/agent of person/business for purposes of person/business is not system security breach when personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/out unreasonable delay,consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K, or • affects more than 500K people, or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when either name or data elements are not encrypted: • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation.** Notice not required for technical breach not reasonably likely to subject customers to risk of criminal activity. Safe harbor for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person or business that maintains computerized data including personal info. not owned shall notify owner or licensee of info. of any data security breach if personal info. was or is reasonably believed to have been acquired by unauthorized person.	None.

Comparison of State Security Breach Notification Laws

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Arkansas	Commercial, charitable, educational, or nonprofit entities including state agencies	Personal information: Name + SSN, DL, account number/identifier with access code, medical information	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached if entity suffering breach determines breach presents a reasonable likelihood of harm to customers.	None	State AG	Does not apply to entity regulated by state or federal law that provides greater protection to personal information	No
California	Any person, government agency or business that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	None	Yes
Connecticut	Persons who conduct business in the state that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	None	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Delaware	Persons who conduct business in the state that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code, medical information	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Must promptly provide written notification of the nature and circumstances of breach to Consumer Protection Division of the Department of Justice	State AG, Consumer Protection Division of the Department of Justice	Does not apply to entity regulated by state or federal law that provides greater protection to personal information	Yes, treble damages plus attorney fees
Florida	Persons who conduct business in the state and maintains computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification within 45 days following discovery of breach to individuals whose unencrypted computerized data containing personal information breached. Notification not required if after consultation with federal/state/local agencies responsible for law enforcement, business determines harm to consumers not likely as a result of breach	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals	Department of Legal Affairs. Penalties for non-notification increase with time since security breach	None	No
Georgia	Information brokers	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Entity suffering breach must coordinate with CRAs if breach includes information on at least 10,000 individuals	State AG	None	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Illinois	Data collection including government agencies, educational institutes, public and private entities that collects, handles, or disseminates nonpublic personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	None	Yes
Indiana	State agencies holding computerized personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Agency suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals	State AG	None	No
Louisiana	Persons who conduct business in the state including state agencies, that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	None	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Maine	Information brokers	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Agency suffering breach must notify appropriate state regulator of breach, must also coordinate with CRAs if breach includes information on at least 1,000 individuals	Department of Professional and Financial Regulation, State AG for information brokers not regulated by Department of Professional and Financial Regulation	None	No
Minnesota	Persons who conduct business in the state and maintains computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Agency suffering breach must coordinate with CRAs if breach includes information on at least 500 individuals	State AG	Does not apply to financial institutions or HIPAA entities	No
Montana	Persons who conduct business in the state and maintains computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Agency suffering breach must coordinate with CRAs	Consumer Protection Office	Insurance-support organizations follow same breach laws, but Montana Insurance Commissioner has authority	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Nevada	Data collectors: includes business entities, government agencies, educational institutions, and associations who handle, collect, or disseminate nonpublic personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals	State AG or a district attorney of any county	Data collectors in compliance with GLB exempted	No
New Jersey	Commercial, charitable, or nonprofit entities including state, county, or local government entities	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached unless entity suffering breach establishes that misuse of information is not reasonably possible. Must keep written documentation of evidence for 5 years	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals. Must also notify State Police in advance of disclosure of breach	State AG	None	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
New York	Persons who conduct business in the state and own or license computerized data containing private information, as well as state or local government agencies	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted, or encrypted with acquired encryption key computerized data containing private information breached	Notification must include contact information of entity suffering breach and a description of the categories of information exposed by the breach. Also require notification to State AG, Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination. Entity suffering breach must coordinate with CRAs if breach includes information on at least 5,000 individuals.	State AG	None	No
North Carolina	Persons who conduct business in the state and owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number, password/PIN that would provide access to a consumer's financial account or resources, digital signatures,	Notification without unreasonable delay to individuals whose unencrypted, un-redacted, or encrypted with acquired encryption key computerized data containing personal	Notification must include: description of breach incident, type of personal information that was breached, contact information for further information. If breach	State AG	Any financial institution subject to and in compliance with Federal Interagency Guidance Response Programs for Unauthorized	No

		biometric data	information breached and illegal use of personal information has occurred or is reasonably likely to occur, or creates a material risk of harm to the consumer	includes information on at least 1,000 individuals, Consumer Protecti on Division of the Attorney General's Office and CRAs must be notified		Access to Consumer Information and Customer Notice exempted	
North Dakota	Persons who conduct business in the state and owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code, date of birth, maiden name of individual's mother, employee number, digital signature	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	Any financial institution subject to and in compliance with Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice exempted	No
Ohio	Persons who conduct business in the state, as well as state or local government agencies	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay (no later than 45 days following discovery of the breach) to individuals whose unencrypted, un-redacted computerized data containing personal information breached and is reasonably believed will cause a risk of ID theft or fraud	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals.	State AG	Financial institutions subjected to federal law requiring notification of security breach incidents exempted. Exempts entities regulated by sections 1171 to 1179 of Social Security Act	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Pennsylvania	Commercial, charitable, or nonprofit entities that maintain, stores, or manages computerized data including personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted, un-redacted, or encrypted with acquired encryption key computerized data containing personal information breached and entity suffering breach reasonably believe has caused or will cause loss or injury	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals.	State AG	Any financial institution subject to and in compliance with Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice exempted. Financial institutions subjected to federal rules or regulations requiring notification of security breach incidents exempted	No
Rhode Island	Any person or business that conducts business in the state and owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	Financial institutions subjected to state or federal law providing greater protections to personal information exempted. Does not apply to HIPAA entities	Yes

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Tennessee	Any business or state or local government agency that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals.	State AG	Financial institutions subject to GLB exempted	Yes
Texas	Any person or business that conducts business in the state and owns or licenses computerized data containing sensitive personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose computerized data containing personal information breached	Entity suffering breach must coordinate with CRAs if breach includes information on at least 10,000 individuals.	State AG	None	No
Washington	Any business or state or local government agency that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose computerized data containing personal information breached. Notification not required if it is a technical breach of security that does not seem reasonably likely to subject consumers to a risk of criminal activity.	None	State AG	None	Yes

Comparison of State Security Freeze Laws

State	Who Can Place Security Freeze	Fees	Effective Date	How to Request Security Freeze	Circumstances when Access to a Frozen Credit Report Allowed[1]	State Security Breach Law?
California	All residents	ID theft victims: None Others: $10 (per CRA) to place freeze, $10 for temporary global lifting of freeze, $12 for temporary lifting of freeze for one creditor	January 1, 2003	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8	Yes
Colorado	All residents	No fee for first freeze; $10 to place a second freeze, $10 for global lift; $12 for temporary lifting for one creditor	July 1, 2006	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	No
Connecticut	All residents	$10 to place, lift, or lift temporarily; $12 for lift for one creditor	January 1, 2006	Freeze can be requested in writing by certified mail or other secure method authorized by CRA	1, 2, 6, 7, 8, 14	Yes
Illinois	Victims of ID theft only	None	January 1, 2006	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8	Yes
Louisiana	All residents	ID theft victims and residents age 62 or older: None Others: $10 to place, $0 to lift	July 1, 2005	Freeze must be requested in writing by certified mail	1, 3, 6, 8, 14, 15, 16, 17, 18	Yes

Maine	All residents	ID theft victims: None Others: up to $10 to place, remove, temporarily lift, have PIN reissues, $12 for lift for a specific creditor	February 1, 2206	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8	Yes
Nevada	All residents	ID theft victims: None Others: up to $15 to place, $18 to lift, $20 for lift for a specific creditor	October 1, 2005	Freeze must be requested in writing by certified mail	1, 2, 3, 6, 7, 8, 14, 15, 19, 20, 21	Yes
New Jersey	All residents	None for initial freeze, up to $5 to remove, temporarily lift or have PIN reissued	January 1, 2006	Freeze can be requested in writing by certified or overnight mail, or by secure electronic mail connection with CRA	1, 2, 3, 5, 6, 7, 8	Yes
North Carolina	All residents	!D theft victims: None Others: up to $10 to place, remove, or suspend the freeze	December 1, 2005	Freeze mu.' he requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8, 9, 14, 18	Yes
Texas	Victims of ID theft only	$8 (adjusted for inflation) to place, none to remove	September 1, 2003	Freeze must be requested in writing by certified mail, placement of security freeze at one CRA must be honored by all	1, 2, 3, 4, 5, 6, 7, 8, 16, 17, 18	Yes
Vermont	Victims of ID theft only	None	July 1, 2005	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8	No

Washington	Victims of ID theft or those notified of a security breach of their computerized personal information	None	July 24, 2005.	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8, 14	Yes

[1] For this section, the following numbers are used:
1= An entity the consumer has a financial obligation or account with
2= Authorized party pursuant to a court order, warrant, or subpoena
3= For child support purposes
4= State agency responsible for investigating Medicaid fraud
5= State agency responsible for investigating delinquent taxes or enforcing state tax laws
6= For prescreening purposes as identified under the FCRA
7= Credit monitoring service to which the consumer has subscribed
8= CRA to provide the consumer with a copy of his or her credit report upon the consumer's request
9= Insurance agent for the purpose of insurance underwriting
10= A pension plan acting to determine the consumer's eligibility for plan benefits or investigating fraud
11= A person conducting a pre-sentence investigation in a criminal matter or parole officer supervising an offender
12= A licensed hospital with which consumer has a contract or debt
13= Law enforcement agencies investigating a crime or conducting a criminal background check
14= Federal, State, or local governmental entity pursuant to their statutory responsibilities
15= Private collection agency assisting the collection of an existing debt
16= CRA which acts only as a reseller and does not maintain a permanent database of credit information
17= A check services or fraud prevention services company
18= A deposit account information service company in reviewing a consumer request for a deposit account
19= An entity which the consumer has an existing business relationship with for any purpose relating to that business relationship
20= A person holding a license issued by state gaming commission
21= Employer using credit report for pre-employment screening or for decisions or investigations of current/former employees

A Chronology of Data Breaches Reported Since the ChoicePoint Incident

Posted: April 20, 2005
Updated January 24, 2006

Privacy Rights Clearinghouse

3100 - 5th Ave., Suite B
San Diego, CA 92103
Voice: (619) 298-3396
Fax: (619) 298-5681
Web: www.privacyrights.org
Contact Us:
www.privacyrights.org/inquiryform.html

HOME

A Chronology of Data Breaches Reported Since the ChoicePoint Incident

The data breaches noted below have been reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers.

The catalyst for reporting data breaches to the affected individuals has been the California law that requires notice of security breaches, the first of its kind in the nation, implemented July 2003.
www.privacyrights.org/ar/SecurityBreach.htm
www.privacy.ca.gov/recommendations/secbreach.pdf

This chronology below begins with ChoicePoint's 2/15/05 announcement of its data breaches because it was a watershed event in terms of disclosure to the affected individuals. Since then, the "best practice" has been to disclose breaches to individuals nationwide -- in a sense, adopting California's notice requirement nationally.

In the meantime, over half the states have considered legislation on security breach notices and security freezes in 2005, and several states passed laws requiring that individuals be notified of security breaches. For a list of those states enacting breach and freeze laws, visit the Consumers Union web site here:
Security breach notice laws: www.consumersunion.org/campaigns/Breach_laws_May05.pdf
Security freeze laws: www.consumersunion.org/campaigns/learn_more/002355indiv.html
State security freeze bills pending in 2006: www.financialprivacynow.org

And visit the PIRG site here: www.pirg.org/consumer/credit/statelaws.htm.

Congress is considering several bills this year in which security breach notices would be mandated nationwide. See http://thomas.loc.gov. See also EPIC's bill-track list, www.epic.org/privacy/bill_track.html.

Here are other sources for security breach information:

- Identity Theft Resource Center, www.idtheftcenter.org/breaches.pdf
- Adam Shostack's blog, www.emergentchaos.com/archives/cat_breaches.html
- Attrition, www.attrition.org/errata/dataloss.html
- World Privacy Forum, Security Breaches in the Digital Medical Environment (scroll to

section D of testimony),
www.worldprivacyforum.org/testimony/NCVHStestimony_092005.html

DATE MADE PUBLIC	NAME	TYPE OF BREACH	NUMBER
Feb. 15, 2005	ChoicePoint	Bogus accounts established by ID thieves	145,000
Feb. 25 , 2005	Bank of America	Lost backup tape	1,200,000
Feb. 25, 2005	PayMaxx	Exposed online	25,000
March 8, 2005	DSW/Retail Ventures	Hacking	100,000
March 10, 2005	LexisNexis	Passwords compromised	32,000
March 11, 2005	Univ. of CA, Berkeley	Stolen laptop	98,400
March 11, 2005	Boston College	[illegible]ing	120,000
March 12, 2005	NV Dept. of Motor Vehicle	Stolen computer	8,900
March 20, 2005	Northwestern Univ.	Hacking	21,000
March 20, 2005	Univ. of NV., Las Vegas	Hacking	5,000
March 22, 2005	Calif. State Univ., Chico	Hacking	59,000
March 23, 2005	Univ. of CA, San Francisco	Hacking	7,000
March 28, 2005	Univ. of Chicago Hospital	Dishonest insider	unknown
April ?, 2005	Georgia DMV	Dishonest insider	465,000
April 5, 2005	MCI	Stolen laptop	16,500
April 8, 2005	Eastern National	Hacker	15,000
April 8, 2005	San Jose Med. Group	Stolen computer	185,000
April 11, 2005	Tufts University	Hacking	106,000
April 12, 2005	LexisNexis	Passwords compromised	Additional 280,000
April 14, 2005	Polo Ralph Lauren/HSBC	Hacking	180,000
April 14,	Calif. Fastrack	Dishonest Insider	4,500

2005			
April 15, 2005	CA Dept. of Health Services	Stolen laptop	21,600
April 18, 2005	DSW/ Retail Ventures	Hacking	Additional 1,300,000
April 20, 2005	Ameritrade	Lost backup tape	200,000
April 21, 2005	Carnegie Mellon Univ.	Hacking	19,000
April 26, 2005	Mic . State Univ's Wharton Center	Hacking	40,000
April 26, 2005	Christus St. Joseph's Hospital	Stolen computer	19,000
April 28, 2005	Georgia Southern Univ.	Hacking	"tens of thousands"
April 28, 2005	Wachovia, Bank of America, PNC Financial Services Group and Commerce Bancorp	Dishonest insiders	676,000
April 29, 2005	Oklahoma State Univ.	Missing laptop	37,000
Ma/ 2, 2005	Time Warner	Lost backup tapes	600,000
May 4, 2005	CO. Health Dept.	Stolen laptop	1,600 (families)
May 5, 2005	Purdue Univ.	Hacking	11,360
May 7, 2005	Dept. of Justice	Stolen laptop	80,000
May 11, 2005	Stanford Univ.	Hacking	9,900
May 12, 2005	Hinsdale Central High School	Hacking	2,400
May 16, 2005	Westborough Bank	Dishonest insider	750
May 18, 2005	Jackson Comm. College, Michigan	Hacking	8,000
May 18, 2005	Univ. of Iowa	Hacking	30,000
May 19, 2005	Valdosta State Univ., GA	Hacking	40,000
May 20, 2005	Purdue Univ.	Hacking	11,000
May 26, 2005	Duke Univ.	Hacking	5,500
May 27, 2005	Cleveland State Univ.	Stolen laptop **Update 12/24:** CSU found the stolen	[44,420] Not included in total below

		laptop	
May 28, 2005	Merlin Data Services	Bogus acct. set up	9,000
May 30, 2005	Motorola	Computers stolen	unknown
June 6, 2005	CitiFinancial	Lost backup tapes	3,900,000
June 10, 2005	Fed. Deposit Insurance Corp. (FDIC)	Not disclosed	6,000
June 16, 2005	CardSystems	Hacking	40,000,000
June 17, 2005	Kent State Univ.	Stolen laptop	1,400
June 18, 2005	Univ. of Hawaii	Dishonest Insider	150,000
June 22, 2005	Eastman Kodak	Stolen laptop	5,800
June 22, 2005	East Carolina Univ.	Hacking	250
June 25, 2005	Univ. of CT (UCONN)	Hacking	72,000
June 28, 2005	Lucas Cty. Children Services (OH)	Exposed by email	900
June 29, 2005	Bank of America	Stolen laptop	18,000
June 30, 2005	Ohio State Univ. Med. Ctr.	Stolen laptop	15,000
July 1, 2005	Univ. of CA, San Diego	Hacking	3,300
July 6, 2005	City National Bank	Lost backup tapes	unknown
July 7, 2005	Mich. State Univ.	Hacking	27,000
July 19, 2005	Univ. of Southern Calif. (USC)	Hacking	270,000 possibly accessed; "dozens"exposed
July 21, 2005	Univ. of Colorado-Boulder	Hacking	42,000
July 30, 2005	San Diego Co. Employees Retirement Assoc.	Hacking	33,000
July 30, 2005	Calif. State Univ., Dominguez Hills	Hacking	9,613
July 31, 2005	Cal Poly-Pomona	Hacking	31,077
Aug. 2, 2005	Univ. of Colorado	Hacking	36,000

Aug. 9, 2005	Sonoma State Univ.	Hacking	61,709
Aug. 9, 2005	Univ. of Utah	Hacking	100,000
Aug. 10, 2005	Univ. of North Texas	Hacking	39,000
Aug. 17, 2005	Calif. State University, Stanislaus	Hacking	900
Aug. 19, 2005	Univ. of Colorado	Hacking	49,000
Aug. 22, 2005	Air Force	Hacking	33,300
Aug. 27, 2005	Univ. of Florida, Health Sciences Center/ChartOne	Stolen Laptop	3,851
Aug. 30, 2005	J.P. Morgan, Dallas	Stolen Laptop	Unknown
Aug. 30, 2005	Calif. State University, Chancellor's Office	Hacking	154
Sept. 10, 2005	Kent State Univ.	Stolen Computers	100,000
Sept. 15, 2005	Miami Univ.	Exposed Online	21,762
Sept. 16, 2005	ChoicePoint (2nd notice, see 2/15/05 for 145,000)	ID thieves accessed; also misuse of IDs & passwords.	9,903
Sept. 17, 2005	North Fork Bank, NY	Stolen laptop (7/24/05) with mortgage data	9,000
Sept. 19, 2005	Children's Health Council, San Jose CA	Stolen backup tape	5,000 - 6,000
Sept. 22, 2005	City University of New York	Exposed online	350
Sept. 23, 2005	Bank of America	Stolen laptop with info of Visa Buxx users (debit cards)	Not disclosed
Sept. 28, 2005	RBC Dain Rauscher	Illegitimate access to customer data by former employee	100+ customers' records compromised out of 300,000
Sept. 29, 2005	Univ. of Georgia	Hacking	At least 1,600
Oct. 12, 2005	Ohio State Univ. Medical Center	Exposed online. Appointment information including SSN, DOB, address, phone no., medical	2,800

		no., appointment reason, physician.	
Oct. 15, 2005	Montclair State Univ.	Exposed online	9,100
Oct. 21, 2005	Wilcox Memorial Hospital, Hawaii	Lost backup tape	130,000
Nov. 1, 2005	Univ. of Tenn. Medical Center	Stolen laptop	3,800
Nov. 4, 2005	Keck School of Medicine, USC	Stolen computer	50,000
Nov. 5, 2005	Safeway, Hawaii	Stolen laptop	1,400 in Hawaii, perhaps more elsewhere
Nov. 8, 2005	ChoicePoint	Bogus accounts established by ID thieves Total affected now reaches 162,000 (See Feb. 15 & Sept. 16)	17,000 more
Nov. 9, 2005	TransUnion	Stolen computer	3,623
Nov. 11, 2005	Georgia Tech Ofc. of Enrollment Services	Stolen computer, Theft 10/16/05	13,000
Nov. 11, 2005	Scottrade Troy Group	Hacking	Unknown
Nov. 19, 2005	Boeing	Stolen laptop with HR data incl. SSNs and bank account info.	161,000
Dec. 1, 2005	Firstrust Bank	Stolen laptop	100,000
Dec. 1, 2005	Univ. of San Diego	Hacking. Faculty, students and employee tax forms containing SSNs	7,800
Dec. 2, 2005	Cornell Univ.	Hacking. Names, addresses, SSNs, bank names and acct. numbers.	900
Dec. 6, 2005	WA Employment Security Dept.	Stolen laptop. Names, SSNs and earnings of former employees.	530
Dec. 12, 2005	Sam's Club/Wal-Mart	Unknown. Exposed credit card data at gas stations.	Unknown
Dec. 16, 2005	La Salle Bank, ABN AMRO Mortgage Group	Backup tape with residential mortgage customers lost in	[2,000,000] Not included in total below

		shipment by DHL, containing SSNs and account information. **Update 12/20:** DHL found the lost tape	
Dec. 16, 2005	Colorado Tech. Univ.	Email erroneously sent containing names, phone numbers, email addresses, Social Security numbers and class schedules.	1,200
Dec. 20, 2005	Guidance Software, Inc.	Hacking. Customer credit card numbers	3,800
Dec. 22, 2005	Ford Motor Co.	Stolen computer. Names and SSNs of current and former employees.	70,000
Dec. 25, 2005	Iowa State Univ.	Hacking. Credit card information and Social Security numbers.	5,500
Dec. 28, 2005	Marriot International	Lost backup tape. SSNs, credit card data of time-share owners	206,000
Jan. 1, 2006	University of Pittsburgh Medical Center, Squirrel Hill Family Medicine	6 Stolen c[illegible]ers. Names, Social Security numbers, birthdates	700
Jan. 2, 2006	H&R Block	SSNs exposed in 40-digit number string on mailing label	Unknown
Jan. 9, 2006	Atlantis Hotel - Kerzner Int'l	Dishonest insider or hacking. Names, addresses, credit card details, Social Security numbers, driver's licence numbers and/or bank account data.	55,000
Jan. 12, 2006	People's Bank	Lost computer tape containing names, addresses, Social Security numbers, and checking account numbers.	90,000
Jan. 17, 2006	City of San Diego, Water & Sewer Dept.	Dishonest employee accessed customer account files, including SSNs, and committed identity	Unknown

		theft on some individuals.	
Jan. 21, 2006	California Army National Guard	Stolen briefcase with personal information of National Guardsmen including a "seniority roster," Social Security numbers and dates of birth.	"hundreds of officers"
Jan. 23, 2006	Univ. of Notre Dame	Hackers accessed Social Security numbers, credit card information and check images of school donors.	Unknown
Jan. 24, 2006	Univ. of WA Medical Center	Stolen laptops containing names, Social Security numbers, maiden names, birth dates, diagnoses and other personal data.	1,600
TOTAL			**52,188,132**

HOME TOP

AARP Alaska

February 21, 2006

Honorable Ralph Seekins, Chair
Senate Judiciary Committee
Alaska State Capitol, Room 125
Juneau, Alaska 99801-1182

RE: SB222 (Therriault and Guess)–Support

Dear Chair Seekins:

On behalf of the members of AARP in Alaska, we urge you and your colleagues on the Senate Judiciary Committee to support SB 222, authored by your Committee colleagues Senators Gene Therriault and Gretchen Guess and co-sponsored by Senate Minority Leader Johnny Ellis.

The Problem

Identity theft is an important issue to AARP. Identity theft is a serious crime that is both widespread and costly. According to a Federal Trade Commission (FTC) survey released in January 2006, Alaska ranked first among all states in the number of fraud complaints, per 100,000 population, and 26th in the number of identify theft victims made to the ID Theft Clearinghouse. This is not just a problem for the lower 48. There were 421 ID theft complaints made in 2005 from Alaskans to the National Identity Theft Data Clearinghouse.

People whose identities are stolen can spend months or years – and their hard earned money – cleaning up the mess thieves made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans for education, housing or automobiles, or even get arrested for crimes they did not commit. In addition, the almost daily news reports about data breaches and mishandling of consumers' personal identifying information demonstrate how important it is to safeguard the personal information that not only identifies us, but also provides entrée to our most sensitive financial information. The newspaper USA Today reported that in 2005, at least 130 reported breaches exposed more than 55 million people to potential identity theft.

A security freeze lets consumers stop identity thieves from getting credit in their names. The security freeze blocks or freezes access to consumers' credit files. In most instances, businesses will not issue new credit to an applicant when the businesses cannot obtain credit information about the person. If consumers freeze their credit files, it does not prevent them from obtaining new credit. Consumers can simply "thaw" the freeze. Once the business providing the new credit obtains the credit reports and credit scores, the freeze can be renewed.

3601 C Street, Suite 1420 | Anchorage, AK 99503 | toll-free 866-227-7447 | 907-341-2270 fax | toll-free 877-434-7598 TTY
Marie F. Smith, President | William D. Novelli, Chief Executive Officer | www.aarp.org/ak

Federal Action

In December 2003, Congress amended the Fair Credit Reporting Act (FCRA), which provides consumer protections regarding the use, accuracy and privacy of consumer credit reports. Through the enactment of the Fair and Accurate Credit Transactions Act (FACT Act)[1], several important consumer protections regarding identity theft were added to FCRA. One of the identity theft provisions was the "one-call" fraud alert. The fraud alert provision permits a notation to be placed on the credit report of consumers who are or believe they may be victims of identity theft. The notation asks issuers of credit to check with the consumers prior to issuing new credit. The fraud alert does not prevent access to the credit report, nor does it prevent the issuance of new credit. The fraud alert should not be confused with a security freeze.

State Action

Twelve (12) states have enacted security freeze laws.[2] While these laws vary in some ways, they all have a common goal – to provide consumers some control over who can gain access to their credit files. As Alaska develops a security freeze law, there are several issues that should be given special consideration.

Who Can Place A Freeze?

AARP believes that all consumers should be able to place a freeze on their credit files. State and federal laws already provide a number of protections for victims of identity theft. Consumers now need a law that will give them the opportunity to protect themselves. Eight states (CA, CO, CT, LA, ME, NV, NJ, NC) currently permit all consumers to place a security freeze. Four states (IL, TX, VT, WA) have laws that apply only to victims of identity theft. However, it should be noted that in each of these states except Texas, bills have been introduced and are moving forward to expand coverage of the laws to all consumers.

Placing and Lifting a Freeze

Security freeze laws are fairly uniform with regard to how a consumer can request a freeze. All states require the request to be in writing and sent by certified mail. AARP believes that consideration should be given to other methods for requesting a freeze as long as the method is secure and the Consumer Reporting Agencies establish policies and procedures to ensure that they can provide proper verification of the consumer. Such methods as a secure electronic mail connection can significantly reduce the amount of time that will be required to place, remove or temporarily lift a freeze. At the present time, most state laws require the freeze be lifted in no more than three (3) days. New Jersey's law set a "15 minute goal" for temporarily lifting a freeze. If this reduction in time can be achieved, consumers will be able to take advantage of those instant credit offers made by retailers, even if they have placed a freeze on their credit files.

---

[1] Pub. L. No. 108-159 (2003).

[2] California, Colorado, Connecticut, Illinois, Louisiana, Maine, Nevada, New Jersey, North Carolina, Texas, Vermont and Washington.

Fees

The issue of fees has caused some significant variations in state laws. Colorado and New Jersey do not require any consumers to pay a fee to place a freeze on their credit files. All of the other states except Connecticut and Texas permit identity theft victims to place a freeze without paying a fee. Louisiana also permits residents 62 years of age and older to avoid paying to place a freeze. For everyone else, the fees for placing a freeze range from low of $8.00 in Texas to a high of $15.00 in Nevada. There is also significant variation in fees charged depending on whether the temporary lifting of the freeze is global versus applying to a specific creditor.

AARP believes that the amount of the fee charged should be reasonable and supports whatever efforts are made to reduce the number of fees that must be paid by the consumer to have a security freeze. The $5.00 fee proposed in SB 222 is reasonable and affordable.

AARP believes that all consumers should have the choice to place a freeze on their credit files. First, the freeze is the best form of identity theft protection that consumers currently have at their disposal. Even though it is by no means a 100% guarantee of safety, it can provide some piece of mind for consumers. Second, the freeze provides consumers a measure of control over their financial security that is not otherwise available. Finally, while the freeze is not for everyone, it should be available for those who wish to have it.

Concern

We asked AARP's attorney that specializes in Identify Theft to review this bill. The only concern she had was the preemption clause. AARP's position is that the State of Alaska needs to maintain the right to protect our citizens and the preemption provision undermines that right. As you know, currently preemption is unsettled law and is being debated in several courts. Eventually this issue will be settled by the courts. Until that happens, state law should prevail, particularly since federal law provides less protection.

Conclusion

Privacy is of considerable concern to the 84,000 AARP members in Alaska, and surveys that we have conducted across the country show that most do not believe that their personal information is being adequately protected. We are grateful that Senators Therriault, Guess and Ellis have taken the time to consider this important issue and we encourage your Committee to support adoption of this legislation for the citizens of our state. We also welcome the opportunity to work with the authors and support legislation that will protect Alaskans from the devastating crime of identity theft.

AARP recommends an "AYE" vote on SB 222.

Should you have any questions about our position, please feel free to contact me (586-3637) or Patrick Luby, AARP Advocacy Director (907-762-3314).

Thank you for your consideration.

Sincerely,

Marie Darlin

Marie Darlin, Coordinator
AARP Capital City Task Force
415 Willoughby Avenue, Apt. 506
Juneau, AK 99801
586-3637 (voice)
463-3580 (fax)

CC: Vice-Chair Charlie Huggins
Senator Gene Therriault
Senator Hollis French
Senator Gretchen Guess

Consumers Union

February 9, 2006

Re: Support of S 222 and HB 226

Consumers Union, the non-profit independent publisher of *Consumer Reports* ©, appreciates this opportunity to submit its views on providing consumers with tools to protect themselves against identity theft. We support bills S 222 and HB 226, which provide all Alaska consumers with additional identity theft protections such as notice of a data security breach and the option of a security freeze on their credit files at a low or no cost. These bills provide key elements in protecting all Alaska consumers from the cost, stress, and time lost due to identity theft.

Identity theft is a serious and increasingly more common crime in this "information age." According to the Federal Trade Commission, in 2003, nearly 10 million Americans were victims of identity theft, costing businesses and financial institutions nearly $48 billion and consumers $5 billion. When identity thieves open new accounts in a consumer's name, the victim ends up spending, on average, $500 and countless hours cleaning up the damage. The personal costs can be devastating; identity theft can create unimaginable family stress when victims are turned down for mortgages, student loans, and even jobs.

One year ago, consumers nationwide first learned of data security breaches only because of one state's law requiring that its res 'ents be told, and 38 state Attorneys General (including then Attorney General Renke) subsequently demanded that their states' residents be informed as well. The Privacy Rights Clearinghouse, a non-profit, non-partisan privacy education and advocacy organization estimates that over 52 million people have had their personal data put at risk due to security breaches. (See http://privacyrights.org/ar/ChronData Breaches.htm). Since ChoicePoint's February 2005 revelations, nearly half of the nation's states have enacted a notice of security breach law.

Notice of a data security breach helps inform consumers to watch for identity theft more promptly after a breach occurs and leads to better and greater data security. A security freeze gives consumers the personal option to take preventative and proactive steps to stop identity thieves from using stolen personal information to open new credit or other new accounts in consumers' names.

A security freeze allows consumers to control who gains access to the personal information contained in credit files. The security freeze blocks access to new creditors to credit reports and credit scores derived from those reports, until the consumer affirmatively unlocks the file. This would help prevent identity thieves from achieving their ultimate goal – opening up new accounts to accumulate debt in their victims' names, ruining credit reports and credit scores.

To explain how a security freeze works, a consumer initially activates the freeze by placing a request with the credit bureaus. After the freeze has been placed, the consumer can then "thaw" or lift the freeze by providing the credit bureaus with a PIN, allowing specified new creditors into the credit files for a specified period of time. The security freeze helps prevent identity thieves from achieving their ultimate goal – opening up new accounts to accumulate debt in their victims' names, which leads to a ruined credit report and credit score.

A growing number of states have provided consumers with the option of a security freeze. Twelve states now give this right, and most to all consumers can now choose to use the security freeze to prevent identity thieves from opening new accounts in their good names.

We urge you to support strong legislation that provides greater identity theft protections for consumers in Alaska. Both S 222 and HB 226 would provide Alaska's consumers with necessary tools to better protect themselves against identity theft.

Please feel to contact either myself or Gail Hillebrand at 415/431-6747 should you have any questions.

Sincerely,

Michelle Jun
Staff Attorney
Financial Privacy Now
Consumers Union

SENATE COMMITTEE REPORT

DATE: 2/16/06

FURTHER: Rules

DATE TURNED IN TO OFFICE: 3/15/06

Judiciary Committee considered SENATE BILL NO. 222

SB 222 PROTECTION OF PERSONAL INFORMATION

"An Act relating to breaches of security involving personal information, consumer report security freezes, consumer credit monitoring, credit accuracy, protection of social security numbers, disposal of records, factual declarations of innocence after identity theft, filing police reports regarding identity theft, and furnishing consumer credit header information; and amending Rule 60, Alaska Rules of Civil Procedure."

and recommends:

[✓] be **replaced** with _____ **CS** SB 222 (JUD)

[ ] adopt **previous** _____ **CS** _____ (_____)

[ ] attached amendment(s)

[ ] adopt Letter of Intent by _____ Committee

[ ] further referral to _____ Committee

CS Senate Bill:
[ ] Same Title
[✓] New Title

SCS House Bill:
[ ] Same Title
[ ] Technical Title Change
[ ] New Title w/ SCR #_____

NEW FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#
GOV/ALL	2/21/06		✓		5

PREVIOUS FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#

[ ] **APPROPRIATION - no fiscal note**

SIGNATURES AND RECOMMENDATIONS:	DO PASS	DO NOT PASS	NO REC	AMEND
French	X			
Guess	X			
Therriault	X			
CHAIR: Seekins	✓			

SENATE COMMITTEE REPORT
First Committee of Referral

FN
FIN REF ?

DATE: 1/9/06

FURTHER: (Judiciary)

Date of 5-Day Notice: 1/19/06
(in accordance with Uniform Rule 23)

DATE TURNED IN TO OFFICE: 2-15-06

Labor and Commerce Committee considered SENATE BILL NO. 222

SB 222 PROTECTION OF PERSONAL INFORMATION

"An Act relating to breaches of security involving personal information, consumer report security freezes, consumer credit monitoring, credit accuracy, protection of social security numbers, disposal of records, factual declarations of innocence after identity theft, filing police reports regarding identity theft, and furnishing consumer credit header information; and amending Rule 60, Alaska Rules of Civil Procedure."

and recommends:

[ ] be **replaced** with _____ **CS** SB 222 (L&C)

[ ] adopt **previous** _____ **CS** _____ (_____)

[ ] attached amendment(s)

[ ] adopt Letter of Intent by _____ Committee

[ ] further referral to _____ Committee

CS Senate Bill:
[ ] Same Title
[X] New Title

SCS House Bill:
[ ] Same Title
[ ] Technical Title Change
[ ] New Title w/ SCR #____

NEW FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#
DOT	1/24/06		✓		1
DWL	1/23/06		✓		2
DPS	1/23/06			✓	3
ADM	1/24/06			✓	4

PREVIOUS FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#

[ ] **APPROPRIATION - no fiscal note**

	SIGNATURES AND RECOMMENDATIONS:	DO PASS	DO NOT PASS	NO REC	AMEND
Davis	Betty J. Davis	X			
Ellis	Pat Ellis	X			
Seekins	Ralph Seekins	✓			
B. Stevens	Ben Stevens				X
Bunde	CHAIR:	X			

D. Barrans TESTIMONY BEFORE SENATE FINANCE COMMITTEE

DATE: March 23, 3006

SUBJECT: Comments re: CSSB 222(JUD)

Co-Chair Green, Co-Chair Wilken, Members: Bunde,Dyson, Stedman, Hoffman, Olson

Thank you for the opportunity to testify today regarding CSSB 222(JUD). While the Alaska Commission on Postsecondary Education is already in compliance with a number of the information security elements of the bill we do have significant concerns about the provisions relating to the collection and use of social security numbers. The current provisions constitute a potential major impairment of ACPE's ability to efficiently and effectively carry out its administrative responsibilities for state financial aid programs.
Specifically, (page 16, lines 25 to 27) *AS 45 48.400(b) Unless expressly required by federal or state law, a person may not sell, lease, loan, trade, rent, or otherwise disclose an individual's social security number to a third party for any purpose without the individual's written consent.*

Currently ACPE uses the SSN as one of several key identifiers in a multi-point ID protocol when performing statutorily required servicing processes which include: insuring the identify of the applicant, review of applicant credit history, review for relevant selective service status, review for child support delinquency, garnishment of wages and/or PFDs, skip tracing, credit reporting, etc. These matches are made with both federal and state entities as well as with private postsecondary institutions and other non-governmental third parties critical to the process.

Collection of SSNs is absolutely critical to these processes and yet, the act of collecting the SSN is not *expressly* required by law, it is performing the processes that is required.

Current language contained in the state education loan Master Promissory Note (MPN) includes an IMPORTANT NOTICES section which advises applicants that submission of the SSN is required to participate in the loan program. It further advises them, generally, how the SSN will be used as an identifier, when needed and appropriate, throughout the life of the loan. While the promissory note does state: *"Information Sharing I authorize the release of information pertinent to my loans...etc."*, it does not contain an explicit statement relating to release of the SSN. Should this phrasing issue be subject to litigation and the language deemed to be deficient, I cannot estimate what costs could come from a class action. The current MPN has been in use for the past four years.

For the Commission to have to require new MPNs of all current borrowers is estimated to cost in excess of $50,000 in printing, distribution and staff time explaining to borrowers and participating institutions why the existing MPN must be replaced. There would also be the intangible cost to the organization, of putting our customers' confidence in the organization at risk. Since we also operate as a lender under the federal program, should we be unable to comply with federal credit reporting requirements the financial losses to the Alaska Student Loan Corporation could be in the millions. Federal loan volume for the current loan year is estimated to be approximately $27 million and represents slightly less than 40% of our total loan volume.

The other two sections of related concern are 45.48.410 and 45.48.415. While 45.48.410 appears to provide agencies with the ability to create SSN-related "law" through the regulation, as it currently reads, that ability is limited to this single section. Should we attempt to provide all of the requisite authority to support critical administrative processes, I am very concerned that, if subjected to litigation by a disgruntled borrower, the courts would take a strict reading of the statute and disallow any such regulation that was not supported by clear statutory authority.

It is also relevant to note that the legislature has expressly charged ACPE with acting as an enterprise agency, using a business model to generate revenue for the state. However, by prohibiting a state agency from asking for a SSN, but not extending that prohibition to other entities, the proposed language in 45.48.410 not only results in significantly increased cost for ACPE – and associated decreases in ACPE's ability to generate revenue for the state – but also results in ACPE not being able to compete with out-of-state organizations that actively market their loans to Alaska's students, costing those students more, decreasing state revenues, and resulting in an outflow of education loan repayment dollars to other states.

Finally, ACPE's business process is already subject to a variety of federal consumer protection laws including: Fair Debt Collection Practices Act (FDCPA); Telephone Consumer Protection Act (TCPA); Fair Credit Reporting Act (FCRA); Patriot Act (for OFAC compliance); Gramm Leach Bliley (GLB); Fair and Accurate Credit Act (FACT ACT); Alaska Privacy Act; Alaska statutes and regulations governing the education loan programs; Truth in Lending Act as well as a variety of federal and state laws relative to consumer information protection, identity theft, payment processing, debt collection, and related financial information. The additional requirements placed on the agency by this legislation certainly adds complexity to compliance, due to possible conflicts, without adding meaningfully to the protection of our customers.

If it is not possible to altogether exempt ACPE from these referenced requirements, then appropriate amendments are necessary to avoid devastating consequences to our operations, our ability to operate as an enterprise agency, and – most important – our ability to support Alaska's students and institutions of higher education.