Alabama

ALA. CODE §§ 8-38-1—8-38-12
http://alisondb.legislature.state.al.us/alison/CodeOfAlabama/1975/174919.htm

***Year most recently amended*:**
Effective: June 1, 2018,

Scope:

Definition of breach:

The unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach.

Definition of personally identifiable information:

"Sensitive personally identifying Information" is defined as an Alabama resident's first name or first initial and last name in combination with one or more of the following with respect to the same Alabama resident: (1) A non-truncated Social Security number or tax identification number; (2) A non-truncated driver's license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual; (3) A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account; (4) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (5) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; (6) A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	Yes
Medical Information	Yes	**Paper Records**	No
De-identified information	No	**Publicly available information**	No
Encrypted Information*	Yes. Information that is encrypted is not covered, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the personally identifying information readable has also been breached.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

A covered entity includes any person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information. Additionally, third-party agents are also covered if they have been contracted to maintain, store, process, or permitted to access sensitive personally identifying information in connection with providing services to a covered entity.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

After an investigation of some kind- After a good faith and prompt investigation determines that sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates, notice of the breach shall be given.

Is there a "Risk of harm" trigger for notification?

Yes. The personally identifying information acquired by an unauthorized person has to be reasonably likely to cause substantial harm to the individuals to whom the information relates.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. If a federal or state law enforcement agency determines that notice to individuals required under this section would interfere with a criminal investigation or national security, the notice shall be delayed upon the receipt of written request of the law enforcement agency for a period that the law enforcement agency determines is necessary. A law enforcement agency, by a subsequent written request, may revoke the delay as of a specified date or extend the period set forth in the original request made under this section if further delay is necessary.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. For a covered entity, as expeditiously as possible and without unreasonable delay, within 45 days. If a third party ageny has experienced a breach, the agent shall notify the covered entity as expeditiously as possible and without unreasonable delay, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred. After receiving notice from a third-party agent, a covered entity shall provide notice within 45 days if required.

Does the law specify how notification must be given?

Yes. Notice to an affected individual under this section shall be given in writing, sent to the mailing address of the individual in the records of the covered entity, or by email notice sent to the email address of the individual in the records of the covered entity.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The notice must include, at a minimum, all of the following: (1) The date, estimated date, or estimated date range of the breach.(2) A description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach.(3) A general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach.(4) A general description of steps an affected individual can take to protect himself or herself from identity theft.(5) Information that the individual can use to contact the covered entity to inquire about the breach.

Does the law require reporting to the Alabama Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: Exceeds 1,000

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: More than 1,000 individuals at a single time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *An entity subject to or regulated by federal laws, rules, regulations, procedures, or guidance on data breach notification established or enforced by the federal government is exempt from this act as long as the entity does all of the following: (1) Maintains procedures pursuant to those laws, rules, regulations, procedures, or guidance. (2) Provides notice to affected individuals pursuant to those laws, rules, regulations, procedures, or guidance. (3) Timely provides a copy of the notice to the Attorney General when the number of individuals the entity notified exceeds 1,000.*

If Yes, list the Federal laws that are referenced:

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

Up to $500,000 in civil penalties per breach. And, $5,000 per day for each consecutive day the covered entity fails to take reasonable action to comply with the notice provisions here.

Enforcing Agency:

Additional Exceptions:
State law exception- An entity subject to or regulated by state laws, rules, regulations, procedures, or guidance on data breach notification that are established or enforced by state government, and are at least as thorough as the notice requirements provided by this act, is exempt from this act so long as the entity does all of the following: (1) Maintains procedures pursuant to those laws, rules, regulations, procedures, or guidance. (2) Provides notice to affected individuals pursuant to the notice requirements of those laws, rules, regulations, procedures, or guidance. (3) Timely provides a copy of the notice to the Attorney General when the number of individuals the entity notified exceeds 1,000.

Alaska

Alaska Stat. §§ 45.48.010 — 45.48.090
http://www.legis.state.ak.us/basis/folioproxy.asp?url=http://wwwjnu01.legis.state.ak.us/cgi-bin/folioisa.dll/stattx09/query=[JUMP:%27AS4548010%27]/doc/{@1}?firsthit

***Year most recently amended*:**
Effective: July 1, 2009, 2021 Alaska House Bill No. 222 (Rauscher & McCarty)

Scope:

Definition of breach:

"Breach of the security" means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector.

Definition of personally identifiable information:

"Personal information" means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of (A) an individual's name (first name or first initial and his or her last name) and (B) one or more of the following information elements: (i) the individual's social security number; (ii) the individual's driver's license number or state identification card number; (iii) Account number, card number, or debit card number in combination with any required security code or password that would allow access to an individual's financial account; and (iv) passwords, personal identification numbers, or other access codes for financial accounts.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No
Medical Information	No	**Paper Records**	Yes
De-identified information	Yes.	**Publicly available information**	No
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

A "covered person" means a (A) person doing business; (B) governmental agency; or (C) person with more than 10 employees

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

After discovering or being notified of the breach, a covered person must disclose the breach. However, disclosure is not required if, after an appropriate investigation and after written notification to the attorney general, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach.

Is there a "Risk of harm" trigger for notification?

Yes. Disclosure is not required if the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach. The Attorney General must be notified in writing.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. An information collector may delay disclosing the breach if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation. However, the information collector shall disclose the breach to the state resident in the most expeditious time possible and without unreasonable delay after the law enforcement agency informs the information collector in writing that disclosure of the breach will no longer interfere with the investigation.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No time limits. The notification must occur in the most expeditious time possible and without unreasonable delay.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Alaska Attorney General or separate government agency under certain conditions?

If Yes, Number of affected residents required for Agency Reporting:

If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?
Yes.

If Yes, number of affected residents to trigger CRA notification*:* More than 1,000 state residents

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.
No.

If Yes, list the Federal laws that are referenced:

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
Liable to the state for a civil penalty of up to $500 for each state resident who was not notified. Total civil penalty may not exceed $50,000

Enforcing Agency:
Department of Administration

Additional Exceptions:
Cost of providing notice- If the information collector (a covered person) demonstrates that the cost of providing notice would exceed $150,000, that the affected class of state residents to be notified exceeds 300,000, or that the information collector does not have sufficient contact information to provide notice, than notice may be given by (1) email; (2) a conspicuous notification on the website of the covered person; and providing a notice to major statewide media. Exception for employees and agents- the good faith acquisition of personal information by an employee or agent of an information collector for a legitimate purpose of the information collector is not a breach of the security of the information system if the employee or agent does not use the personal information for a purpose unrelated to a legitimate purpose of the information collector and does not make further unauthorized disclosure of the personal information.

Arizona

Ariz. Rev. Stat. §§ 18-551, 18-552
https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/18/00551.htm AND
https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/18/00552.htm

***Year most recently amended*:**
Amended 2022, 2022 Ariz. Legis. Serv. Ch. 81 (H.B. 2146)

Scope:

Definition of breach:

"Breach" or "security system breach" means n unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of unencrypted and unredacted computerized personal information maintained as part of a database of personal information regarding multiple individuals.

Definition of personally identifiable information:

"Personal information" means any of the following: (i) An individual's first name or first initial and last name in combination with one or more specified data elements. (ii) An individual's user name or e-mail address, in combination with a password or security question and answer, that allows access to an online account. "Specified data element" includes: (a) An individual's social security number. (b) The number on an individual's driver license or nonoperating identification license. (c) A private key that is unique to an individual and that is used to authenticate or sign an electronic record. (d) An individual's financial account number or credit or debit card number in combination with any required security code, access code or password that would allow access to the individual's financial account. (e) An individual's health insurance identification number. (f) Information about an individual's medical or mental health treatment or diagnosis by a health care professional. (g) An individual's passport number. (h) An individual's taxpayer identification number or an identity protection personal identification number issued by the United States internal revenue service. (i) Unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No. The breach pertains to unencrypted information only.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

A "person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government or governmental subdivision or agency or any other legal or commercial entity. (b) Does not include the department of public safety, a county sheriff's department, a municipal police department, a prosecution agency or a court.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

After conducting a prompt investigation, the person that owns or licenses the unencrypted and unredeacted computerized data must notify if the investigation results in a determination that there has been a security system breach.

Is there a "Risk of harm" trigger for notification?

No.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notifications required may be delayed if a law enforcement agency advises the person that the notifications will impede a criminal investigation. On being informed by the law enforcement agency that the notifications no longer compromise the investigation, the person shall make the required notifications, as applicable, within forty-five days.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. 45 days.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The notification shall include at least the following: 1. The approximate date of the breach. 2. A brief description of the personal information included in the breach. 3. The toll-free numbers and addresses for the three largest nationwide consumer reporting agencies. 4. The toll-free number, address and website address for the federal trade commission or any federal agency that assists consumers with identity theft matters.

Does the law require reporting to the Arizona Attorney General or separate government agency under certain conditions? Yes.

***If Yes, Number of affected residents required for Agency Reporting**:* More than 1,000
If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

***If Yes, number of affected residents to trigger CRA notification**:* More than 1,000 individuals.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *Does not apply to a person subject to title V of GLB. Does not apply to covered entities or business assocaites under HIPAA. Does not apply to charitable fundraising foundations or nonprofits if they comply with applicable provisions of HIPAA.*

If Yes, list the Federal laws that are referenced: *GLB, HIPAA*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. The person's policy must be consistent with the requirements aforementioned, including the 45 day notification period. If so, they are deemed to be in compliance with the notification requirements.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

AG may impose civil penalties of up to $10,000 per violation. The max civil penalty may not exceed $500,000.

Enforcing Agency:

Punishable by the Attorney General

Additional Exceptions:

Arkansas

Ark. Code. Ann. §§ 4-110-101 — 4-110-108
https://advance.lexis.com/documentpage/?pdmfid=1000516&crid=b7917c28-e4c6-4b3f-b603-9b4281b515c8&nodeid=AAEAAHAAZAAB&nodepath=%2fROOT%2fAAE%2fAAEAAH%2fAAEAAHAAZ%2fAAEAAHAAZAAB&level=4&haschildren=&populated=false&title=4-110-101.+Short+title.&config=00JAA2ZjZiM2VhNS0wNTVlLTQ3NzUtYjQzYy0yYWZmODJiODRmMDYKAFBvZENhdGFsb2fXiYCnsel0plIgqpYkw9PK&pddocfullpath=%2fshared%2fdocument%2fstatutes-legislation%2furn%3acontentItem%3a4WVD-4KB0-R03N-607R-00008-00&ecomp=_g1_kkk&prid=952de607-d805-47a8-bc3e-ca01c506ca27

***Year most recently amended*:**
Amended July, 2019, 2019 Arkansas Laws Act 1030 (H.B. 1943)

Scope:

Definition of breach:

"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and his or her last name in combination with any one (1) or more of the following data elements when either the name or the data element is not encrypted or redacted: (A) Social Security number; (B) Driver's license number or Arkansas identification card number; (C) Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; (D) Medical information; and (E)(i) Biometric data. (ii) As used in this subdivision, "biometric data" means data generated by automatic measurements of an individual's biological characteristics, including without limitation: (a) Fingerprints; (b) Faceprint; (c) A retinal or iris scan; (d) Hand geometry;(e) Voiceprint analysis; (f) Deoxyribonucleic acid (DNA); or (g) Any other unique biological characteristics of an individual if the characteristics are used by the owner or licensee to uniquely authenticate the individual's identity when the individual accesses a system or account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	No.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No. The breach pertains to unencrypted information only.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

"Person or business"- Any person or business that acquires, owns, maintains, or licenses computerized data that includes personal information.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after discovery of the breach. However, if, after a reasonable investigation, the person or buisness determines that there is no reasonable liklohood of harm to customers, notification is not required.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

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

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. Notice may be provided by one (1) of the following methods: (1) Written notice; (2) Electronic mail notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001, as it existed on January 1, 2005; or (3) (A) Substitute notice if the person or business demonstrates that: (i) The cost of providing notice would exceed two hundred fifty thousand dollars ($250,000); (ii) The affected class of persons to be notified exceeds five hundred thousand (500,000); or (iii) The person or business does not have sufficient contact information. (B) Substitute notice shall consist of all of the following: (i) Electronic mail notice when the person or business has an electronic mail address for the subject persons; (ii) Conspicuous posting of the notice on the website of the person or business if the person or business maintains a website; and (iii) Notification by statewide media.

Does the law require reporting to the Arkansas Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting*:* More than 1,000
If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

No.

If Yes, number of affected residents to trigger CRA notification*:*

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

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

If Yes, list the Federal laws that are referenced:

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies affected persons in accordance with its policies in the event of a breach of the security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

Enforcing Agency:

Punishable by the Attorney General

Additional Exceptions:

Good faith exception- Breach of the security of the system does not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure.

California

Cal. Civ. Code § 1798.82 (for businesses) Cal. Civ. Code § 1798.29 (for state agencies)
http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82.
AND
https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29.

***Year most recently amended*:**
January, 2022, 2021 Cal. Legis. Serv. Ch. 527 (A.B. 825) and 2021 Cal. Legis. Serv. Ch. 527 (A.B. 825)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means either of the following: (1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social security number. (B) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (D) Medical information. (E) Health insurance information. (F) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes. (G) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5. (H) Genetic data. (2) A username or email address, in combination with a password or security question and answer that would permit access to an online account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information. Additionally, any agency that owns or licenses computerized data that includes personal information.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after the discovery of the breach.

Is there a "Risk of harm" trigger for notification?

No.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

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

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The security breach notification described in paragraph (1) shall include, at a minimum, the following information: (A) The name and contact information of the reporting person or business subject to this section. (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach. (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice. (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided. (E) A general description of the breach incident, if that information is possible to

determine at the time the notice is provided. (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number. (G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

Does the law require reporting to the California Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: More than 500 California residents as a result of a single breach.

If Yes, does the agency publish breach data?: Yes. *https://oag.ca.gov/privacy/databreach/list*

Does the law require notifying consumer reporting agencies under certain conditions?

No.

If Yes, number of affected residents to trigger CRA notification:

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).1 However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.*

If Yes, list the Federal laws that are referenced: *HIPAA*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

Yes.

Enforcement damages and penalties:

Any customer injured by a violation of this title may bring a civil action to recover damages. Statute specifically authorizes injunctions against businesses violating the statute. Class actions are notbarred.

Enforcing Agency:

Attorney General.

Additional Exceptions:

Colorado

Colo. Rev. Stat. § 6-1-716.

https://advance.lexis.com/documentpage/?pdmfid=1000516&crid=44219357-4e59-432c-981e-6b845607e6e4&nodeid=AAGAABAABAAIAAU&nodepath=%2FROOT%2FAAG%2FAAGAAB%2FAAGAABAAB%2FAAGAABAABAAI%2FAAGAABAABAAIAAU&level=5&haschildren=&populated=false&title=6-1-716.+Notification+of+security+breach.&config=014FJAAyNGJkY2Y4Zi1mNjgyLTRkN2YtYmE4OS03NTYzNzYzOTg0OGEKAFBvZENhdGFsb2d592qv2Kywlf8caKqYROP5&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A61P5-X0P1-DYDC-J4YD-00008-00&ecomp=_g1_9kk&prid=19ae81af-5107-4b79-94ee-47d60fdcdbe6

***Year most recently amended*:**
Amended September, 2018, 2018 Colo. Legis. Serv. Ch. 266 (H.B. 18-1128)

Scope:

Definition of breach:

"Security breach" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity. Good faith acquisition of personal information by an employee or agent of a covered entity for the covered entity's business purposes is not a security breach if the personal information is not used for a purpose unrelated to the lawful operation of the business or is not subject to further unauthorized disclosure.

Definition of personally identifiable information:

"Personal information" means a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: (A) Social security number; student, military, or passport identification number; driver's license number or identification card number; medical information; health insurance identification number; or biometric data; (B) A Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account; or (C) A Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

"Covered entity" means a person, as defined in section 6-1-102(6), that maintains, owns, or licenses personal information in the course of the person's business, vocation, or occupation. "Covered entity" does not include a person acting as a third-party service provider as defined in subsection (1)(i) of this section.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

After conducting a prompt investigation, if it is determined that the likelihood that personal information has been or will be misused, the covered entity shall give notice to the affected Colorado residents.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. Notice must be made in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. No later than 30 days after the date of determination that a security breach occurred.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. In the case of a breach of personal information, notice must include, but need not be limited to, the following information: (I) The date, estimated date, or estimated date range of the security breach; (II) A description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach; (III) Information that the resident can use to contact the covered entity to inquire about the security breach; (IV) The toll-free numbers, addresses, and websites for consumer reporting

agencies; (V) The toll-free number, address, and website for the federal trade commission; and (VI) A statement that the resident can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes. FURTHERMORE, if the investigation determines that the personal information has been misused or is reasonably likely to be misused, then the covered entity shall, in addition to the aforementioned requirements, (I) Direct the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the covered entity and all other online accounts for which the person whose personal information has been breached uses the same username or e-mail address and password or security question or answer. (II) For log-in credentials of an e-mail account furnished by the covered entity, the covered entity shall not comply with this section by providing the security breach notification to that e-mail address, but may instead comply with this section by providing notice through other methods, as defined in subsection (1)(f) of this section, or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an internet protocol address or online location from which the covered entity knows the resident customarily accesses the account.

Does the law require reporting to the Colorado Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: 500
If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: More than 1,000 residents.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *The following subsection does NOT apply to a covered entity who is subject to Title V of the Federal GLB Act: If a covered entity is required to notify more than one thousand Colorado residents of a security breach pursuant to this section, the covered entity shall also notify, in the most expedient time possible and without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by the federal "Fair Credit Reporting Act", 15 U.S.C. sec. 1681a(p), of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified. Nothing in this subsection (2)(d) requires the covered entity to provide to the consumer reporting agency the names or other personal information of security breach notice recipients.*

If Yes, list the Federal laws that are referenced: *GLB*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. (a) Pursuant to this section, a covered entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information and whose procedures are otherwise consistent with the timing requirements of this section is in compliance with the notice requirements of this section if the covered entity notifies affected Colorado residents in accordance with its policies in the event of a security breach; except that notice to the attorney general is still required. (b) A covered entity that is regulated by state or federal law and that maintains procedures for a security breach pursuant to the laws, rules, regulations, guidances, or guidelines established by its state or federal regulator is in compliance with this section; except that notice to the attorney general is still required. In the case of a conflict between the time period for notice to individuals that is required pursuant to this subsection and the applicable state or

federal law or regulation, the law or regulation with the shortest time frame for notice to the individual controls.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
Recover direct economic damages resulting from a violation, or both. The provisions of this section are not exclusive and do not relieve a covered entity subject to this section from compliance with all other applicable provisions of law.

Enforcing Agency:
Punishable by the Attorney General

Additional Exceptions:
Third-party service providers- If a covered entity uses a third-party service provider to maintain computerized data that includes personal information, then the third-party service provider shall give notice to and cooperate with the covered entity in the event of a security breach that compromises such computerized data, including notifying the covered entity of any security breach in the most expedient time possible, and without unreasonable delay following discovery of a security breach, if misuse of personal information about a Colorado resident occurred or is likely to occur.

Connecticut

Conn. Gen. Stat. § 36a-701b
https://www.cga.ct.gov/current/pub/chap_669.htm#sec_36a-701b

***Year most recently amended*:**
Amended October, 2021, 2021 Conn. Legis. Serv. P.A. 21-59 (H.B. 5310)

Scope:

Definition of breach:

"Breach of security" means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data, containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

Definition of personally identifiable information:

"Personal information" means an individual's (A) first name or first initial and last name in combination with any one, or more, of the following data: (i) Social Security number; (ii) taxpayer identification number; (iii) identity protection personal identification number issued by the Internal Revenue Service; (iv) driver's license number, state identification card number, passport number, military identification number or other identification number issued by the government that is commonly used to verify identity; (v) credit or debit card number; (vi) financial account number in combination with any required security code, access code or password that would permit access to such financial account; (vii) medical information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (viii) health insurance policy number or subscriber identification number, or any unique identifier used by a health insurer to identify the individual; or (ix) biometric information consisting of data generated by electronic measurements of an individual's unique physical characteristics used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina or iris image; or (B) user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** No.

What entities are covered?

Any person who owns, licenses or maintains computerized data that includes personal information

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after discovery of the breach. Any person who owns, licenses or maintains computerized data that includes personal information, shall provide notice of any breach of security following the discovery of the breach to any resident of this state whose personal information was breached or is reasonably believed to have been breached.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

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

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. No later than 60 days after the discovery of the breach.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. Any notice to a resident, owner or licensee required by the provisions of this section may be provided by one of the following methods, subject to the provisions of subsection (f) of this section: (1) Written notice; (2) telephone notice; (3) electronic notice, provided such notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001; (4) substitute notice, provided such person demonstrates that the cost of providing notice in accordance with subdivision (1), (2) or (3) of this subsection would exceed two hundred fifty thousand dollars, that the affected class of subject persons to be notified exceeds five hundred thousand persons or that the person does not have sufficient contact information.

Substitute notice shall consist of the following: (A) Electronic mail notice when the person has an electronic mail address for the affected persons; (B) conspicuous posting of the notice on the web site of the person if the person maintains one; and (C) notification to major state-wide media, including newspapers, radio and television. In the event of a breach of login credentials under subparagraph (B) of subdivision (2) of subsection (a) of this section, notice to a resident may be provided in electronic or other form that directs the resident whose personal information was breached or is reasonably believed to have been breached to promptly change any password or security question and answer, as applicable, or to take other appropriate steps to protect the affected online account and all other online accounts for which the resident uses the same user name or electronic mail address and password or security question and answer.

Does the law require reporting to the Connecticut Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: Any breach must be reported to the Attorney General

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

No.

If Yes, number of affected residents to trigger CRA notification:

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *Any person that is subject to and in compliance with the privacy and security standards under the Health Insurance Portability and Accountability Act of 19961 and the Health Information Technology for Economic and Clinical Health Act ("HITECH") shall be deemed to be in compliance with this section, provided that (1) any person required to provide notification to Connecticut residents pursuant to HITECH shall also provide notice to the Attorney General.*

If Yes, list the Federal laws that are referenced: *HIPAA, HITECH*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. Any person that maintains such person's own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies, as applicable, residents of this state, owners and licensees in accordance with such person's policies in the event of a breach of security and in the case of notice to a resident, such person also notifies the Attorney General not later than the time when notice is provided to the resident. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in 15 USC 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided (1) such person notifies, as applicable, such residents of this state, owners, and licensees required to be notified under and in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security, and (2) if notice is given to a resident of this state in accordance with subdivision (1) of this subsection regarding a breach of security, such person also notifies the Attorney General not later than the time when notice is provided to the resident.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
Constitues an unfair trade practice for purposes of section 42-110b and shall be enforced by the Attorney General.

Enforcing Agency:
Punishable by the Attorney General

Additional Exceptions:
Third-party notifications- Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery, if the personal information of a resident of this state was breached or is reasonably believed to have been breached.

Delaware

Del. Code Ann. tit. 6, §§ 12B-100
https://delcode.delaware.gov/title6/c012b/index.html

***Year most recently amended*:**
Amended September, 2018, 2018 Delaware Laws Ch. 425 (H.B. 465)

Scope:

Definition of breach:

"Breach of security" means as follows: a. The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. Good faith acquisition of personal information by an employee or agent of any person for the purposes of such person is not a breach of security, provided that the personal information is not used for an unauthorized purpose or subject to further unauthorized disclosure. b. The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information is not a breach of security to the extent that personal information contained therein is encrypted, unless such unauthorized acquisition includes, or is reasonably believed to include, the encryption key and the person that owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable or useable.

Definition of personally identifiable information:

"Personal information" means a Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to that individual: 1. Social Security number. 2. Driver's license number or state or federal identification card number. 3. Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account. 4. Passport number. 5. A username or email address, in combination with a password or security question and answer that would permit access to an online account. 6. Medical history, medical treatment by a healthcare professional, diagnosis of mental or physical condition by a healthcare professional, or deoxyribonucleic acid profile. 7. Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person. 8. Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes. 9. An individual taxpayer identification number.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

"Person" means an individual; corporation; business trust; estate trust; partnership; limited liability company; association; joint venture; government; governmental subdivision, agency, or instrumentality; public corporation; or any other legal or commercial entity.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Following the determination of a breach, notice must be given UNLESS, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. A law-enforcement agency determines that the notice will impede a criminal investigation and such law-enforcement agency has made a request of the person that the notice be delayed. Any such delayed notice must be made after such law-enforcement agency determines that notice will not compromise the criminal investigation and so notifies the person of such determination. ALSO, when a person is otherwise required to provide notice, could not, through reasonable diligence, identify within 60 days that the personal information of certain residents of this State was included in a breach of security, such person must provide the notice required by this section to such residents as soon as practicable after the determination that the breach of security included the personal information of such residents.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. No later than 60 days after determination of the breach of security.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Delaware Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting*:* Exceeds 500.

If Yes, does the agency publish breach data?: No.

https://attorneygeneral.delaware.gov/fraud/cpu/securitybreachnotification/database/

Does the law require notifying consumer reporting agencies under certain conditions?

No.

If Yes, number of affected residents to trigger CRA notification*:*

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *Both HIPAA and GLB- laws, rules, regulations, guidance, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this chapter if the person notifies affected Delaware residents in accordance with the maintained procedures when a breach of security occurs.*

If Yes, list the Federal laws that are referenced: *HIPAA, GLB*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

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

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

The Attorney General may bring an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both.

Enforcing Agency:

Punishable by the Attorney General

Additional Exceptions:

In the case of a breach of security involving personal information for login credentials of an email account furnished by the person, the person cannot comply with this section by providing the security breach notification to such email address, but may instead comply with this section by providing notice by another method described in § 12B-101(5) of this title or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person knows the resident customarily accesses the account. Additionally, if a breach involves Social Security numbers, credit monitoring services must be provided at no cost to residents

for a period of 1 year. Lastly, a person that maintains computerized data that includes personal information that the person does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of security immediately following determination of the breach of security (third-party service provider notice rule).

Florida

Fla. Stat. § 501.171
http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html

***Year most recently amended*:**
Amended October, 2019, 2019 Fla. Sess. Law Serv. Ch. 2019-32 (H.B. 7047)

Scope:

Definition of breach:

"Breach of security" or "breach" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

Definition of personally identifiable information:

"Personal information" means either of the following: a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: (I) A social security number; (II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; (IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	Yes.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No. The statute specifically excludes encrypted information.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

"Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. This includes a governmental entity.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Provides for a period of investigation. Notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. If a federal, state, or local law enforcement agency determines that notice to individuals required under this subsection would interfere with a criminal investigation, the notice shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period set forth in the original request made under this paragraph to a specified date if further delay is necessary. ADDITIONALLY, a covered entity may receive 15 additional days to provide notice as required if good cause for delay is provided in writing to the Department of Legal Affairs within 30 days after determination of the breach or reason to believe a breach occurred.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. No later than 30 days after the determination of a breach.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The notice to an individual with respect to a breach of security shall include, at a minimum: 1. The date, estimated date, or estimated date range of the breach of security. 2. A description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security. 3.

Information that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual.

Does the law require reporting to the Florida Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting*:* 500 or more individuals of Florida.

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification*:* More than 1,000 individuals at a single time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator is deemed to be in compliance with the notice requirement in this subsection if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security. The covered entity that timely provides a copy of such notice to the department is deemed to be in compliance with the notice of this law.*

If Yes, list the Federal laws that are referenced:

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

Covered entity liable for a civil penalty not to exceed $500,000 as follows: In the amount of $1,000 for each day up to the first 30 days following any violation of subsection (3) or subsection (4) and, thereafter, $50,000 for each subsequent 30-day period or portion thereof for up to 180 days. If the violation continues for more than 180 days, in an amount not to exceed $500,000.

Enforcing Agency:

Violation shall constitute an unfair or deceptive trade practice in any action brought by the Department of Legal Affairs.

Additional Exceptions:

The notice given to the Department of Legal Affairs includes different requirements than the notice given to individuals. The written notice must include: 1. A synopsis of the events surrounding the breach at the time notice is provided.2. The number of individuals in this state who were or potentially have been affected by

the breach.3. Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services.4. A copy of the notice required under subsection (4) or an explanation of the other actions taken pursuant to subsection (4).5. The name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about the breach. Third-party notice- In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred. Upon receiving notice from a third-party agent, a covered entity shall provide notices required under subsections (3) and (4). A third-party agent shall provide a covered entity with all information that the covered entity needs to comply with its notice requirements.

Georgia

Ga. Code §§ 10-1-911—10-1-912
http://ga.elaws.us/law/section10-1-912

***Year most recently amended*:**
Amended May, 2007, 2007 Georgia Laws Act 241 (S.B. 236)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (A) Social security number; (B) Driver's license number or state identification card number; (C) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords; (D) Account passwords or personal identification numbers or other access codes; or (E) Any of the items contained in subparagraphs (A) through (D) of this paragraph when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

"Person" means any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association, or other entity. This includes data collectors and information brokers.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?
Immediately after discovery.

Is there a "Risk of harm" trigger for notification?
No.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?
Yes. The notification required may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation. The notification required by this Code section shall be made after the law enforcement agency determines that it will not compromise the investigation.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?
Yes. If the information broker or data collector maintains computerized data, in the most expedient time possible and without unreasonable delay. If person or business maintains computerized data on behalf of an information broker, within 24 hours following discovery (third-party notice rule).

Does the law specify how notification must be given?
Yes.
If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?
No.

Does the law require reporting to the Georgia Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: More than 10,000 residents at one time.

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?
Yes.

***If Yes, number of affected residents to trigger CRA notification**:* More than 10,000 residents at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

No.

If Yes, list the Federal laws that are referenced:

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. An information broker or data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

Not specified.

Enforcing Agency:

Additional Exceptions:

Substitute notice- if the information broker or data collector demonstrates that the cost of providing notice would exceed $50,000.00, that the affected class of individuals to be notified exceeds 100,000, or that the information broker or data collector does not have sufficient contact information to provide written or electronic notice to such individuals. Substitute notice shall consist of all of the following: (i) E-mail notice, if the information broker or data collector has an e-mail address for the individuals to be notified; (ii) Conspicuous posting of the notice on the information broker's or data collector's website page, if the information broker or data collector maintains one; and (iii) Notification to major state-wide media.

Hawaii

Haw. Rev. Stat. §§ 487N-1—487N-4
http://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487N/HRS_0487N-0001.htm

***Year most recently amended*:**
Amended July, 2008, 2008 Hawaii Laws 1st Sp. Sess. Act 10 (S.B. 2803)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) Driver's license number or Hawaii identification card number; or (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	Yes
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes. A business is defined as a sole proprietorship, partnership, corporation, association, or other group, however organized, and whether or not organized to operate at a profit. The term includes a financial institution

organized, chartered, or holding a license or authorization certificate under the laws of the State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. The term also includes an entity whose business is records destruction. A government agency is defined as any department, division, board, commission, public corporation, or other agency or instrumentality of the State or of any county.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

The disclosure notification shall be made without unreasonable delay, immediately after discovery of the breach.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

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

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The notice shall be clear and conspicuous. The notice shall include a description of the following: (1) The incident in general terms; (2) The type of personal information that was subject to the unauthorized access and acquisition; (3) The general acts of the business or government agency to protect the personal

information from further unauthorized access; (4) A telephone number that the person may call for further information and assistance, if one exists; and (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Does the law require reporting to the Hawaii Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: More than 1,000 persons at one time

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: More than 1,000 persons at one time

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *The following businesses shall be deemed to be in compliance with this section: (1) A financial institution that is subject to the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice published in the Federal Register on March 29, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, or subject to 12 C.F.R. Part 748,1 and any revisions, additions, or substitutions relating to the interagency guidance; and (2) Any health plan or healthcare provider that is subject to and in compliance with the standards for privacy or individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996.*

If Yes, list the Federal laws that are referenced: *HIPAA, federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice,*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

Yes.

Enforcement damages and penalties:

Any business that violates this privision shall be subject to penalties of not more than $2,500 for each violation. Additionally, business shall be liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation. The court may award reasonable attorneys' fees to the prevailing party.

Enforcing Agency:

The attorney general, the executive director of the office of consumer protection, or any injured party may bring action.

Additional Exceptions:

Substitute notice- if the business or government agency demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of subject persons to be notified exceeds two hundred thousand, or if the business or government agency does not have sufficient contact information or consent to satisfy paragraph (1), (2), or (3) of the notice requirement, for only those affected persons without sufficient contact information or consent, or if the business or government agency is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following: (A) Electronic mail notice when the business or government agency has an electronic mail address for the subject persons; (B) Conspicuous posting of the notice on the website page of the business or government agency, if one is maintained; and (C) Notification to major statewide media. Third-party notifications- Any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement. Government reporting requirement- A government agency shall submit a written report to the legislature within twenty days after discovery of a security breach at the government agency that details information relating to the nature of the breach, the number of individuals affected by the breach, a copy of the notice of security breach that was issued, the number of individuals to whom the notice was sent, whether the notice was delayed due to law enforcement considerations, and any procedures that have been implemented to prevent the breach from reoccurring.

Idaho

Idaho Code §§ 28-51-104—28-51-107
https://legislature.idaho.gov/statutesrules/idstat/Title28/T28CH51/

***Year most recently amended*:**
Amended July, 2018, 2015 Idaho Laws Ch. 141 (H.B. 91)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means an Idaho resident's first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:(a) Social security number;(b) Driver's license number or Idaho identification card number; or(c) Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

A city, county or state agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

After an investigation. When it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

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

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Idaho Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: Any breach must be reported to the Attoreny General within 24 hours (after discovery).

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

No.

***If Yes, number of affected residents to trigger CRA notification**:*

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *No specific laws are mentioned. An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance if the individual or the commercial entity complies with the maintained procedures when a breach of the security of the system occurs.*

If Yes, list the Federal laws that are referenced:

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

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

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

Any agency, individual or commercial entity that intentionally fails to give notice in accordance with section 28-51-105, Idaho Code, shall be subject to a fine of not more than twenty-five thousand dollars ($25,000) per breach of the security of the system.

Enforcing Agency:

The primary regulator may bring a civil action to enforce compliance.

Additional Exceptions:

Substitute notice- if the agency, individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed twenty-five thousand dollars ($25,000), or that the number of Idaho residents to be notified exceeds fifty thousand (50,000), or that the agency, individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following: (i) E-mail notice if the agency, individual or the commercial entity has e-mail addresses for the affected Idaho residents; and (ii) Conspicuous posting of the notice on the website page of the agency, individual or the commercial entity if the agency, individual or the commercial entity maintains one; and (iii) Notice to major statewide media. Third-party notice rule- An agency, individual or a commercial entity that maintains computerized data that includes personal information that the agency, individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach if misuse of personal information about an Idaho resident occurred or is reasonably likely to occur.

Illinois

815 Ill. Compt. Stat. §§ 530/1—530/50

http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapAct=815%20ILCS%20530/&ChapterID=67&ChapterName=BUSINESS+TRANSACTIONS&ActName=Personal+Information+Protection+Act.

***Year most recently amended*:**
Amended January, 2020, 2019 Ill. Legis. Serv. P.A. 101-343 (S.B. 1624)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means either of the following: (1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security: (A) Social Security number. (B) Driver's license number or State identification card number. (C) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. (D) Medical information. (E) Health insurance information. (F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. (2) user name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	No.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.

Encrypted Information*	Yes.				

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

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

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

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

Is there a "Risk of harm" trigger for notification?

No.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notification to an Illinois resident required may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation. Furthermore, the disclosure notification shall be made in the most expedient time possible and without unreasonable delay, taking into consideration the measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows: (1) With respect to personal information as defined in Section 5 in paragraph (1) of the definition of "personal information": (A) the toll-free numbers and addresses for consumer reporting agencies; (B) the toll-free number, address, and website address for the Federal Trade Commission; and (C) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. (2) With respect to personal information defined in Section 5 in paragraph (2) of the definition of "personal information", notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

Does the law require reporting to the Illinois Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: More than 500 residents as a result of a single breach (non-State agencies). For State agencies, if they suffer a single breach that deals with more than 250 residents, notice to AG required.

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: If state agency, more than 1,000 persons.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *Yes if: (1) the entity complies with state or federal laws that provide greater protection to personal information than this section; (2) the entity is subject to and in compliance with standards established by §501(b) of GLB Act; or (3) the entity is subject to and in compliance with the privacy and security standards for the protection of electronic health information set by HIPAA.*

If Yes, list the Federal laws that are referenced: *GLB, HIPAA*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. A data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data. A State agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act shall be deemed in compliance with the notification requirements of this Section if the State agency notifies subject persons in accordance with its policies in the event of a breach of the security of the system data or written material.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
Any person, including but not limited to a third party referenced in subsection (c), who violates this Section is subject to a civil penalty of not more than $100 for each individual with respect to whom personal information is disposed of in violation of this Section. A civil penalty may not, however, exceed $50,000 for each instance of improper disposal of materials containing personal information.

Enforcing Agency:
Attorney General.

Additional Exceptions:
Substitute notice- if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required. Third-party notice- Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Indiana

Ind. Code §§ 24-4.9-1-1—24-4.9-5-1
http://iga.in.gov/legislative/laws/2020/ic/titles/024#24-4.9

***Year most recently amended*:**
Amended July, 2009, 2009 Ind. Legis. Serv. P.L. 137-2009 (H.E.A. 1121)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means: (1) a Social Security number that is not encrypted or redacted; or (2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted: (A) A driver's license number. (B) A state identification card number. (C) A credit card number. (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	Yes. The term "breach of the security of data" includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a comput
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes. After discovering or being notified of a breach of the security of data, the data base owner shall disclose the breach to an Indiana resident whose: (2) encrypted personal information was or may have been acquired by an unauthorized person with acces

What entities are covered?

An individual, a corporation, a business trust, an estate, a trust, a partnership, an association, a nonprofit corporation or organization, a cooperative, or any other legal entity that owns or licenses computerized data that includes personal information.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after discovery.

Is there a "Risk of harm" trigger for notification?

Yes- "if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft, or fraud affecting the Indiana resident."

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. Reasonable delay in disclosure is permitted. A delay is reasonable if it is (1) necessary to restore the integrity of the computer system; (2) necessary to discover the scope of the breach; or (3) in response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will: (A) impede a criminal or civil investigation; or (B) jeopardize national security. (b) A person required to make a disclosure or notification under this chapter shall make the disclosure or notification as soon as possible after: (1) delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach; or (2) the attorney general or a law enforcement agency notifies the person that delay will no longer impede a criminal or civil investigation or jeopardize national security.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Indiana Attorney General or separate government agency under certain conditions? Yes.

***If Yes, Number of affected residents required for Agency Reporting**:* Any incident that qualifies as a breach of the security, per this code, is to be disclosed to the attorney general.

If Yes, does the agency publish breach data?: No. *https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/security-breaches/*

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

***If Yes, number of affected residents to trigger CRA notification**:* More than 1,000 consumers

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *This code does not apply to an entity that maintains its own data security procedures as part of an information privacy, security policy, or compliance plan if if the entity's information privacy, security policy, or compliance plan requires the data base owner to maintain reasonable procedures to protect and safeguard from unlawful use or disclosure personal information of Indiana residents that is collected or maintained by the entity and the entity complies with the entity's information privacy, security policy, or compliance plan.*

If Yes, list the Federal laws that are referenced: *(1) the federal USA PATRIOT Act (P.L. 107-56); (2) Executive Order 13224; (3) the federal Driver's Privacy Protection Act (18 U.S.C. 2721 et seq.); (4) the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); (5) the federal Financial Modernization*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

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

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

The attorney general may bring an action under this chapter to obtain any or all of the following: (1) An injunction to enjoin future violations of IC 24-4.9-3. (2) A civil penalty of not more than one hundred fifty thousand dollars ($150,000) per deceptive act. (3) The attorney general's reasonable costs in: (A) the investigation of the deceptive act; and (B) maintaining the action.

Enforcing Agency:

Punishable by the Attorney General

Additional Exceptions:

Substitute notice- If a data base owner required to make a disclosure under this chapter is required to make the disclosure to more than five hundred thousand (500,000) Indiana residents, or if the data base owner required to make a disclosure under this chapter determines that the cost of the disclosure will be more than two hundred fifty thousand dollars ($250,000), the data base owner required to make a disclosure under this chapter may elect to make the disclosure by using both of the following methods: (1) Conspicuous posting of the notice on the web site of the data base owner, if the data base owner maintains a web site. (2) Notice to

major news reporting media in the geographic area where Indiana residents affected by the breach of the security of a system reside. -Unauthorized acquisition of a portable electronic device on which personal information is stored does not trigger breach notification requirements if access to the device is protected by a password that has not been disclosed.

Iowa

Iowa Code §§ 715C.1—715C.2
https://www.legis.iowa.gov/docs/code/715c.pdf

***Year most recently amended*:**
Amended July, 2018, 2018 Ia. Legis. Serv. Ch. 1091 (S.F. 2177)

Scope:

Definition of breach:

"Breach of security" means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. "Breach of security" also means unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or are encrypted, redacted, or otherwise altered by any method or technology but the keys to unencrypt, unredact, or otherwise read the data elements have been obtained through the breach of security: (1) Social security number. (2) Driver's license number or other unique identification number created or collected by a government body. (3) Financial account number, credit card number, or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account. (4) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (5) Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	No.
Medical Information	No.	**Paper Records**	Yes.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

"Person" means an individual; corporation; business trust; estate; trust; partnership; limited liability company; association; joint venture; government; governmental subdivision, agency, or instrumentality; public corporation; or any other legal or commercial entity.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

The law allows for a period of investigation.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The consumer notification requirements of this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that the notification will not compromise the investigation and notifies the person required to give notice in writing.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. Notice pursuant to this section shall include, at a minimum, all of the following: a. A description of the breach of security. b. The approximate date of the breach of security. c. The type of personal information obtained as a result of the breach of security. d. Contact information for consumer reporting agencies. e. Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.

Does the law require reporting to the Iowa Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting*:* More than 500 residents of the state.

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

No.

If Yes, number of affected residents to trigger CRA notification*:*

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *This code does not apply to A person who complies with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this section. This code also does not apply to a person subject to HITECH, HIPAA or Title V of GLB.*

If Yes, list the Federal laws that are referenced: *GLB, HIPAA, HITECH*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. This code does not apply to a person who complies with notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements than that provided by this section pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

The attorney general may seek and obtain an order that a party held to violate this section pay damages to the attorney general on behalf of a person injured by the violation. The attorney general may request and the court may impose a civil penalty not to exceed $40,000 per violation against a person found by the court to have engaged in a method, act, or practice declared unlawful under this section; provided, however, a course of conduct shall not be considered to be separate and different violations merely because the conduct is repeated to more than one person. The court may impose a civil penalty of not more than $5,000 for each day of intentional violation of a preliminary/permanent injunction.

Enforcing Agency:

Punishable by the Attorney General

Additional Exceptions:

Third-party notice- Any person who maintains or otherwise possesses personal information on behalf of another person shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach of security if a consumer's personal information was included in the

information that was breached. -Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, that the affected class of consumers to be notified exceeds three hundred fifty thousand persons, or if the person does not have sufficient contact information to provide notice. Substitute notice shall consist of the following: (1) Electronic mail notice when the person has an electronic mail address for the affected consumers. (2) Conspicuous posting of the notice or a link to the notice on the internet site of the person if the person maintains an internet site. (3) Notification to major statewide media.

Kansas

Kan. Stat. §§ 50-7a01—50-7a04
http://www.kslegislature.org/li/b2021_22/statute/050_000_0000_chapter/050_007a_0000_article/

***Year most recently amended*:**
Amended July, 2016, Laws 2016, ch. 103, § 7

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means a consumer's first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted: (1) Social security number; (2) driver's license number or state identification card number; or (3) financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

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

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

After a reasonable and prompt investigation.

Is there a "Risk of harm" trigger for notification?

Yes- The investigation is used to determine if misuse of the information has occurred or is reasonably likely to occur.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

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

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Kansas Attorney General or separate government agency under certain conditions? No.

If Yes, Number of affected residents required for Agency Reporting:

If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: More than 1,000 consumers at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *A individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this statute.*

If Yes, list the Federal laws that are referenced:

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

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

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

The attorney general is empowered to bring an action in law or equity to address violations of this section and for other relief that may be appropriate.

Enforcing Agency:

Punishable by the Attorney General. -For violations of this section by an insurance company licensed to do business in this state, the insurance commissioner shall have the sole authority to enforce the provisions of this section.

Additional Exceptions:

Substitute notice- if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $100,000, or that the affected class of consumers to be notified exceeds 5,000, or that the individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice can occur via E-mail, conspicuous posting of the notice on the web site page of the individual or the commercial entity, and notification to major statewide media. -Third-party notice- An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the data following discovery of a breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.

Kentucky

Ky. Rev. Stat. § 365.732
https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=43326

***Year most recently amended*:**
Effective: July, 2014,

Scope:

Definition of breach:

"Breach of the security of the system" means unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky. Good-faith acquisition of personally identifiable information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system if the personally identifiable information is not used or subject to further unauthorized disclosure.

Definition of personally identifiable information:

Personally identifiable information" means an individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted: 1. Social Security number; 2. Driver's license number; or 3. Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

"Information holder" means any person or business entity that conducts business in this state.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after discovery.

Is there a "Risk of harm" trigger for notification?

Yes- The breach must lead the information holder to reasonably beleive that identify theft or fraud against any resident has or will occur.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

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

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Kentucky Attorney General or separate government agency under certain conditions? No.

If Yes, Number of affected residents required for Agency Reporting:

If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: More than 1,000 persons at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *This code does not apply to any person who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, or the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.*

If Yes, list the Federal laws that are referenced: *HIPAA, GLB*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
Yes.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
No applicable provision.

Enforcing Agency:

Additional Exceptions:
Substitute Notice- if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the information holder does not have sufficient contact information. Substitute notice shall consist of all of the following: 1. E-mail notice, when the information holder has an e-mail address for the subject persons; 2. Conspicuous posting of the notice on the information holder's Internet Web site page, if the information holder maintains a Web site page; and 3. Notification to major statewide media.

Louisiana

La. Stat. §§ 51:3071—51:3077
http://legis.la.gov/Legis/Law.aspx?d=322027

***Year most recently amended*:**
Amended August, 2018, 2018 La. Sess. Law Serv. Act 382 (S.B. 361)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means the first name or first initial and last name of an individual resident of this state in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted: (i) Social security number. (ii) Driver's license number or state identification card number. (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv) Passport number. (v) Biometric data. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account. (b) "Personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

"Person" means any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity. Agencies that own or license computerized data that includes PII are also covered. "Agency" means the state, a political subdivision of the state, and any officer, agency, board, commission, department or similar body of the state or any political subdivision of the state.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Noification is not required if after a reasonable investigation, the person or buisness determines that there is no reasonable likelihood of harm to the residents of this state.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. If a law enforcement agency determines that the notification required under this Section would impede a criminal investigation, such notification may be delayed until such law enforcement agency determines that the notification will no longer compromise such investigation. Notification can also be delayed due to a determination by the person or agency that measures are necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. Notification, when required, must be made no later than sixty (60) days from the discovery of the breach.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Louisiana Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: Written explanation (as to the reason for a delay in the 60 day notification period) to the attorney general.

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?
No.

***If Yes, number of affected residents to trigger CRA notification**:*

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.
Yes. *A financial institution that is subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this chapter.*

If Yes, list the Federal laws that are referenced: *Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
Yes.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
Yes.

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

Enforcing Agency:
Attorney General

Additional Exceptions:
Rule on the destruction of personal information no longer needed- Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information shall take all reasonable steps to destroy or arrange for the destruction of the records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

Maine

Me. Stat. tit. 10 §§ 1346–1350-B
https://legislature.maine.gov/legis/statutes/10/title10ch210-Bsec0.html

***Year most recently amended*:**
Amended September, 2019, 2019 Me. Legis. Serv. Ch. 512 (S.P. 209) (L.D. 696) (WEST)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

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

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

"Person" means an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity, including agencies of State Government, municipalities, school administrative units, the University of Maine System, the Maine Community College System, Maine Maritime Academy and private colleges and universities. "Person" as used in this chapter may not be construed to require duplicative notice by more than one individual, corporation, trust, estate, cooperative, association or other entity involved in the same transaction.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?
After a prompt investigation.

Is there a "Risk of harm" trigger for notification?
Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?
Yes. If, after the completion of an investigation, notification is required under this section, the notification required by this section may be delayed for no longer than 7 business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?
Yes. No more than 30 days after becoming aware of of a breach of security.

Does the law specify how notification must be given?
Yes.
If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?
No.

Does the law require reporting to the Maine Attorney General or separate government agency under certain conditions? Yes.

***If Yes, Number of affected residents required for Agency Reporting**:* When notice of a breach of the security of the system is required, the person shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the Attorney G

If Yes, does the agency publish breach data?: No.
https://www.maine.gov/ag/consumer/identity_theft/index.shtml

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: More than 1,000 persons at a single time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *A person that complies with federal and state laws is deemed to be in compliance with these requirements as long as the law, rules, regulations or guidelines provide for notification procedures at least as protective as the notification requirements of this section.*

If Yes, list the Federal laws that are referenced: *No federal laws specified.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

A fine of $500 per violation, up to a maximum of $2,500 for each day the person is in violation, but Does not apply to Gov entities. Also, equitable relief, enjoinment from furhter violations.

Enforcing Agency:

Attorney General.

Additional Exceptions:

Substitute notice- if the person maintaining personal information demonstrates that the cost of providing notice would exceed $5,000, that the affected class of individuals to be notified exceeds 1,000 or that the person maintaining personal information does not have sufficient contact information to provide written or electronic notice to those individuals. Substitute notice must consist of all of the following: (1) E-mail notice, if the person has e-mail addresses for the individuals to be notified; (2) Conspicuous posting of the notice on the person's publicly accessible website, if the person maintains one; and (3) Notification to major statewide media. Third party notice- A 3rd-party entity that maintains, on behalf of a person, computerized data that includes personal information that the 3rd-party entity does not own shall notify the person maintaining personal information of a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Maryland

Md. Code Ann., Com. Law §§ 14-3501—14-3508
https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gcl&section=14-3402&enactments=False&archived=False

***Year most recently amended*:**
Amended in 2022. Effective October 1, 2022., 2022 Maryland Laws Ch. 503 (S.B. 643)

Scope:

Definition of breach:

"Breach of the security of a system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business.

Definition of personally identifiable information:

(e)(1) "Personal information" means: (i) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: 1. A Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government; 2. A driver's license number or State identification card number; 3. An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account; 4. Health information, including information about an individual's mental health; 5. A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information; or 6. Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or 7. For purposes of the notifications required under § 14–3504(b)(2), (c), (d), (e), (f), and (g) of this subtitle, genetic information with respect to an individual; (ii) A user name or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account; or (iii) For the purposes of the requirements of this title other than the notifications required under § 14–3504(b)(2), (c), (d), (e), (f), and (g) of this subtitle, genetic information with respect to an individual when the genetic information is not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable, including: 1. Data, regardless of its format, that results from the analysis of a biological sample of the individual or from another source that enables equivalent information to be obtained and that concerns genetic material; 2. Deoxyribonucleic acids; 3. Ribonucleic acids; 4. Genes; 5. Chromosomes; 6. Alleles; 7. Genomes; 8. Alterations or modifications to deoxyribonucleic acids or ribonucleic acids; 9. Single nucleotide polymorphisms; 10. Uninterrupted data that results from the analysis of a biological sample from the individual or other sources; and 11. Information extrapolated, derived, or inferred from item 1, 2, 3, 4, 5, 6, 7, 8, 9, or 10 of this item.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes.

Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

"Business" means a sole proprietorship, partnership, corporation, association, or any other business entity, whether or not organized to operate at a profit. "Business" includes a financial institution organized, chartered, licensed, or otherwise authorized under the laws of this State, any other state, the United States, or any other country, and the parent or subsidiary of a financial institution.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

After a prompt investigation.

Is there a "Risk of harm" trigger for notification?

Yes. The investigation looks to see the liklihood that personal information has been or will be misused.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notification may be delayed (i) If a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or (ii) To determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. For businesses that owns, licenses, or maintains computerized data containing PII- no later than 45 days after the business discovers or is notified of the breach.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The notification shall include: (1) To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired; (2) Contact information for the business making the notification, including the business' address, telephone number, and toll-free telephone number if one is maintained; (3) The toll-free telephone numbers and addresses for the major consumer reporting agencies; and (4) (i) The toll-free telephone numbers, addresses, and website addresses for: 1. The Federal Trade Commission; and 2. The Office of the Attorney General; and (ii) A statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft.

Does the law require reporting to the Maryland Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: Any number.

If Yes, does the agency publish breach data?: Yes.

https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: 1,000 or more individuals.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *A business that complies with the requirements for notification procedures, the protection or security of personal information, or the destruction of personal information under the rules, regulations, procedures, or guidelines established by the primary or functional federal or State regulator of the business shall be deemed to be in compliance with this subtitle. Furthermore, a buisness that is in compliance with HIPAA, GLB, § 216 of the federal Fair and Accurate Credit Transactions Act, the federal Interagency Guidelines Establishing Information Security Standards, and the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or substitutions, shall be deemed to be in compliance.*

If Yes, list the Federal laws that are referenced: *GLB, HIPAA, § 216 of the federal Fair and Accurate Credit Transactions Act, federal Interagency Guidelines Establishing Information Security Standards, the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information a*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

Yes.

Enforcement damages and penalties:
Unfair and deceptive trade practice, subject to the enforcement and penalty provisions of Title 13. Title 13 states: Any person may bring an action to recover for injury or loss sustained by him. Any person who brings an action to recover for injury or loss under this section and who is awarded damages may also seek, and the court may award, reasonable attorney's fees. A merchant who engages in a violation of this title is subject to a fine not exceeding $10,000 for each violation.(b) A merchant who has been found to have engaged in a violation of this title and who subsequently repeats the same violation is subject to a fine not exceeding $25,000 for each subsequent violation.

Enforcing Agency:

Additional Exceptions:
Substitute notice under subsection (e)(4) of this section shall consist of:(1) Electronically mailing the notice to an individual entitled to notification under subsection (b) of this section, if the business has an electronic mail address for the individual to be notified;(2) Conspicuous posting of the notice on the website of the business, if the business maintains a website; and(3) Notification to statewide media major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.

Massachusetts

Mass. Gen. Laws ch. 93H, §§ 1–6
https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H/Section3

***Year most recently amended*:**
Amended January, 2019, 2018 Mass. Legis. Serv. Ch. 444 (H.B. 4806)

Scope:

Definition of breach:

"Breach of security", the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Definition of personally identifiable information:

"Personal information" means a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

Persons and agencies. A person is a natural person, corporation, association, partnership or other legal entity. An agency is any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or any of its branches, or of any political subdivision thereof.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after discovery.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. Notice may be delayed if a law enforcement agency determines that provision of such notice may impede a criminal investigation and has notified the attorney general, in writing, thereof and informs the person or agency of such determination. If notice is delayed due to such determination and as soon as the law enforcement agency determines and informs the person or agency that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable and without unreasonable delay.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The notice to be provided to the resident shall include, but shall not be limited to: (i) the resident's right to obtain a police report; (ii) how a resident may request a security freeze and the necessary information to be provided when requesting the security freeze; (iii) that there shall be no charge for a security freeze; and (iv) mitigation services to be provided pursuant to this chapter; provided, however, that said notice shall not include the nature of the breach of security or unauthorized acquisition or use, or the number of residents of the commonwealth affected by said breach of security or unauthorized access or use. The person or agency that experienced the breach of security shall provide a sample copy of the notice it sent to consumers to the attorney general and the office of consumer affairs and business regulation.

Does the law require reporting to the Massachusetts Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: Any number.

If Yes, does the agency publish breach data?: Yes. *https://www.mass.gov/lists/data-breach-reports*

Does the law require notifying consumer reporting agencies under certain conditions?

Yes

If Yes, number of affected residents to trigger CRA notification*:* If the director of consumer affairs and business regulation identifies relevant consumer reporting agencies as appropriate to notify, the person or agency shall provide notice to the consumer reporting agencies.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *a person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; provided further that the person also notifies the attorney general and the director of the office of consumer affairs and business regulation of the breach as soon as practicable and without unreasonable delay following the breach.*

If Yes, list the Federal laws that are referenced: *No federal laws specified.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

The attorney general may bring an action against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

Enforcing Agency:

Attorney General

Additional Exceptions:

Social Security Numbers- if a breach of security includes a social security number, the person shall contract with a third party to offer to each resident whose social security number was disclosed in the breach of security or is reasonably believed to have been disclosed in the breach of security, credit monitoring services at no cost to said resident for a period of not less than 18 months.

Michigan

Mich. Comp. Laws §§ 445.61, 445.63, 445.65, 445.72

http://www.legislature.mi.gov/(S(psko1q24a5k4bvnk20jovefw))/mileg.aspx?page=getobject&objectname=mcl-445-61

***Year most recently amended*:**
Amended April, 2011, 2010 Mich. Legis. Serv. P.A. 318 (S.B. 149)

Scope:

Definition of breach:

"Breach of the security of a database" or "security breach" means the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals.

Definition of personally identifiable information:

"Personal identifying information" means a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, social security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, any other account password in combination with sufficient information to identify and access the account, automated or electronic signature, biometrics, stock or other security certificate or account number, credit card number, vital record, or medical records or information.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

Both person and agency. Person- "Person" means an individual, partnership, corporation, limited liability company, association, or other legal entity. Agency- "Agency" means a department, board, commission, office,

agency, authority, or other unit of state government of this state. The term includes an institution of higher education of this state. The term does not include a circuit, probate, district, or municipal court.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after discovery of the breach. However, the person or agency is not required to provide notice if the security breach is not likely to cause substantial loss or injury, or result in identity theft with respect to, 1 or more residents.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. A delay is permissible if: (a) A delay is necessary in order for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database, (b) A law enforcement agency determines and advises the agency or person that providing a notice will impede a criminal or civil investigation or jeporadize homeland or national security.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The notice must do the following: (a) For a notice provided under subsection (5)(a) or (b) (written notice or electronic written notice), be written in a clear and conspicuous manner and contain the content required under subdivisions (c) to (g). (b) For a notice provided under subsection (5)(c) (telephone notice), clearly communicate the content required under subdivisions (c) to (g) to the recipient of the telephone call. (c) Describe the security breach in general terms. (d) Describe the type of personal information that is the subject of the unauthorized access or use. (e) If applicable, generally describe what the agency or person providing the notice has done to protect data from further security breaches. (f) Include a telephone number where a notice recipient may obtain assistance or additional information. (g) Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

Does the law require reporting to the Michigan Attorney General or separate government agency under certain conditions? No.

***If Yes, Number of affected residents required for Agency Reporting**:*

If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

***If Yes, number of affected residents to trigger CRA notification**:* More than 1,000 residents.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *A person or agency in compliance with HIPAA is in compliance with this section. Also, a financial institution that is subject to, and has notification procedures in place that are subject to examination by the financial institution's appropriate regulator for compliance is considered to be in compliance with this section.*

If Yes, list the Federal laws that are referenced: *HIPAA, Financial institutions regulated for compliance with the interagency guidance*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

Enforcement damages and penalties:

A person that knowingly fails to provide any notice of a security breach pays a civil fine of $250 for each failure. Aggregate liabiltiy of a person for civil fines for multiple violations from the same security breach shall not exceed $750,000.

Enforcing Agency:

The attorney general or a prosecuting attorney may bring an action to recover a civil fine under this section.

Additional Exceptions:

Written notice sent electronically permitted if: (i) The recipient has expressly consented to receive electronic notice. (ii) The person or agency has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the person or agency reasonably believes that it has the recipient's current electronic mail address. OR (iii) The person or agency conducts its business primarily through internet account transactions or on the internet. Telephone notice requirements- f not otherwise prohibited by state or federal law, notice given by telephone by an individual who represents the person or agency if all of the following are met: (i) The notice is not given in whole or in part by use of a recorded message. (ii) The recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the person or agency also provides notice under subdivision (a) or (b) if the notice by telephone does not result in a live conversation between the individual representing the person or agency and the recipient within 3 business days after the initial attempt to provide telephonic notice. Substitute Notice- if the person or

agency demonstrates that the cost of providing notice under subdivision (a), (b), or (c) will exceed $250,000.00 or that the person or agency has to provide notice to more than 500,000 residents of this state. A person or agency provides substitute notice under this subdivision by doing all of the following: (i) If the person or agency has electronic mail addresses for any of the residents of this state who are entitled to receive the notice, providing electronic notice to those residents. (ii) If the person or agency maintains a website, conspicuously posting the notice on that website. (iii) Notifying major statewide media. A notification under this subparagraph shall include a telephone number or a website address that a person may use to obtain additional assistance and information.

#VALUE!

Minn. Stat §§ 325E.61, 325E.64, 8.31
https://www.revisor.mn.gov/statutes/cite/325E.61

***Year most recently amended*:**
Effective: 2006 and 2007,

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired: (1) Social Security number; (2) driver's license number or Minnesota identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

Any person or business that conducts business in this state, and that owns or licenses data that includes personal information. Also,

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after discovery in the most expedient time possible and without unreasonable delay.

Is there a "Risk of harm" trigger for notification?

No.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notification may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation. Can also be delayed by taking into account the measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data systems.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the #VALUE! Attorney General or separate government agency under certain conditions? No.

If Yes, Number of affected residents required for Agency Reporting:

If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: More than 500 persons at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *This section does not apply to any "financial institution" as defined by United States Code, title 15, section 6809(3).*

If Yes, list the Federal laws that are referenced: *United States Code, title 15, section 6809(3).*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section and section 13.055, subdivision 6, shall be deemed to be in compliance with the notification requirements of this section and section 13.055, subdivision 6, if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No?

Enforcement damages and penalties:

As applicable to government entities: any individual injured by a violation of this chapter may bring action for damages plus costs and reasonable attorney fees.

Enforcing Agency:

Enforced by the Attorney General.

Additional Exceptions:

Substitute notice- if the person or business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice must consist of all of the following: (i) e-mail notice when the person or business has an e-mail address for the subject persons; (ii) conspicuous posting of the notice on the website page of the person or business, if the person or business maintains one; and (iii) notification to major statewide media.

Mississippi

Miss. Code § 75-24-29

https://advance.lexis.com/documentpage/?pdmfid=1000516&crid=31358736-5515-46c0-8ab2-0b3054d5828d&nodeid=ABNAAWAABAAQ&nodepath=%2fROOT%2fABN%2fABNAAW%2fABNAAWAAB%2fABNAAWAABAAQ&level=4&haschildren=&populated=false&title=%C2%A7+75-24-29.+Persons+conducting+business+in+Mississippi+required+to+provide+notice+of+a+breach+of+security+involving+personal+information+to+all+affected+individuals%3b+enforcement.&config=00JABhZDIzMTViZS04NjcxLTQ1MDItOTllOS03MDg0ZTQxYzU4ZTQKAFBvZENhdGFsb2f8inKxYiqNVSihJeNKRlUp&pddocfullpath=%2fshared%2fdocument%2fstatutes-legislation%2furn%3acontentItem%3a627R-MSW3-GXJ9-31CB-00008-00&ecomp=_g1_kkk&prid=4a73830b-21c5-4f5d-87ac-7e382345050e

***Year most recently amended*:**
Amended July, 2021, H.B. No. 277, § 9

Scope:

Definition of breach:

"Breach of security" means unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements: (i) Social security number; (ii) Driver's license number, state identification card number or tribal identification card number; or (iii) An account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account; "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

This section applies to any person who conducts business in this state and who, in the ordinary course of the person's business functions, owns, licenses or maintains personal information of any resident of this state.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

The law permits an investigation. Notification shall not be required if, after an appropriate investigation, the breach will not likely result in harm to the affected individuals.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. Notification can be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation or national security and the law enforcement agency has made a request that the notification be delayed.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes, if the person's primary means of communication with the affected individuals is by electronic means or if the notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USCS 7001.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?
No.

Does the law require reporting to the Mississippi Attorney General or separate government agency under certain conditions? No.

If Yes, Number of affected residents required for Agency Reporting:
If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?
No.

If Yes, number of affected residents to trigger CRA notification:

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.
Yes. *Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or federal functional regulator shall be deemed to be in compliance with the security breach notification requirements of this section.*

If Yes, list the Federal laws that are referenced: *No federal laws specified.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
Yes. Any person who conducts business in this state that maintains its own security breach procedures as part of an information security policy for the treatment of personal information, and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section if the person notifies affected individuals in accordance with the person's policies in the event of a breach of security.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
Failure to comply with the requirements of this section shall constitute an unfair trade practice and shall be enforced by the Attorney General.

Enforcing Agency:
Failure to comply with the requirements of this section shall constitute an unfair trade practice and shall be enforced by the Attorney General.

Additional Exceptions:
Third party notice- Any person who conducts business in this state that maintains computerized data which includes personal information that the person does not own or license shall notify the owner or licensee of the information of any breach of the security of the data as soon as practicable following its discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes. Substitute Notice- permitted if the person demonstrates that the cost

of providing notice would exceed Five Thousand Dollars ($5,000.00), that the affected class of subject persons to be notified exceeds five thousand (5,000) individuals or the person does not have sufficient contact information.

Missouri

Mo. Rev. Stat. § 407.1500
https://revisor.mo.gov/main/OneSection.aspx?section=407.1500&bid=23329&hl=

***Year most recently amended*:**
Effective: August, 2009,

Scope:

Definition of breach:

"Breach of security" or "breach", unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

Definition of personally identifiable information:

"Personal information", an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable: (a) Social Security number; (b) Driver's license number or other unique identification number created or collected by a government body; (c) Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; (d) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (e) Medical information; or (f) Health insurance information.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

"Person", any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, governmental agency, governmental instrumentality, public corporation, or any other legal or commercial entity.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

After an investigation of some kind. Notification is not required if, after an appropriate investigation by the person, the person determines that a risk of identity theft or fraud is not reasonably likely to occur as a result of the breach.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notification may be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security. The law also allows for a period of daley to determien the scope of the breach and restore the reasonable integrity, security, and confidentialtiy of the data system.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Missouri Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: More than one thousand consumers at one time.

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?
Yes.

If Yes, number of affected residents to trigger CRA notification*:* More than one thousand consumers at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.
Yes. *A person that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section if the person notifies affected consumers in accordance with the maintained procedures when a breach occurs. Additionally, financial institutions that are subject to the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, the National Credit Union Administration regulations, or Title V of the Gramm-Leach-Bliley Financial Modernization Act are deemed to be in compliance with this section.*

If Yes, list the Federal laws that are referenced: *Unauthorized Access to Customer Information and Customer Notice, the National Credit Union Administration regulations, or Title V of the Gramm-Leach-Bliley Financial Modernization Act*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
Yes. A person that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the person notifies affected consumers in accordance with its policies in the event of a breach of security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
The attorney general shall have exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section and may seek a civil penalty not to exceed $150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

Enforcing Agency:
Attorney general may bring action for damages.

Additional Exceptions:
Substitute notice included.

Montana

Mont. Code Ann. §§ 30-14-1701—30-14-1705
https://leg.mt.gov/bills/mca/title_0300/chapter_0140/part_0170/section_0040/0300-0140-0170-0040.html

***Year most recently amended*:**
Amended 2015, 2015 Montana Laws Ch. 62 (H.B. 74)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) social security number; (B) driver's license number, state identification card number, or tribal identification card number; (C) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (D) medical record information; (E) a taxpayer identification number; or (F) an identity protection personal identification number issued by the United States internal revenue service. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

Any person or business that owns or licenses computerized data that includes personal information. "Buisness" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or any other country or the parent or the subsidiary of a financial institution.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after discovery. The disclosure must be made without unreasonable delay.

Is there a "Risk of harm" trigger for notification?

Yes. The breach has to meterially compromise the security, confidentiality, or integrity of personal information maintained by the person/business. It has to reasonably cause loss or injury.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notification required may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay in notification.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. If a business discloses a security breach to any individual pursuant to this section and gives a notice to the individual that suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual.

Does the law require reporting to the Montana Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: Any number. Any person or business that is required to issue a notification pursuant to this section shall simultaneously submit an

electronic copy of the notification and a statement providing the date and method of distribution of the notification to th

If Yes, does the agency publish breach data?: Yes. *https://dojmt.gov/consumer/databreach/*

Does the law require notifying consumer reporting agencies under certain conditions?

Yes, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual IF the business discloses a security breach to any individual that suggests, indicates, or implies to the ind

If Yes, number of affected residents to trigger CRA notification:

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

No.

If Yes, list the Federal laws that are referenced:

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and that does not unreasonably delay notice is considered to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the data system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

AG may bring action. Covered entity may be liable for civil penalities not more than $10,000 for each violation, plus additional civil penalities not more than $10,000 per willful violation under Mont. Code 30-14-142.

Enforcing Agency:

Attorney General

Additional Exceptions:

Substitute notice permitted if the person or buisness demonstrates that: (A) the cost of providing notice would exceed $250,000; (B) the affected class of subject persons to be notified exceeds 500,000; or (C) the person or business does not have sufficient contact information.

Nebraska

Neb. Rev. Stat. §§ 87-801—807
http://nebraskalegislature.gov/laws/statutes.php?statute=87-801

***Year most recently amended*:**
Amended 2018, 2018 Nebraska Laws L.B. 757

Scope:

Definition of breach:

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

Definition of personally identifiable information:

Personal information means either of the following: (a) A Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable: (i) Social security number; (ii) Motor vehicle operator's license number or state identification card number; (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account; (iv) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or (v) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or (b) A user name or email address, in combination with a password or security question and answer, that would permit access to an online account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

Both individuals and commercial entities. Commercial entity includes a corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency, or instrumentality, or any other legal entity, whether for profit or not for profit.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

After an investigation to investigate the likelihood that personal information has been or will be used for an unauthorized purpose.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. The law also takes into account time needed to conduct an investigation to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Nebraska Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting*:* Any number. If notice of a breach of security of the system is required by this law, the individual or commercial entity shall also provide notice of the breach to the Attorney General.

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?
No.

***If Yes, number of affected residents to trigger CRA notification**:*

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.
Yes. *An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance if the individual or commercial entity notifies affected Nebraska residents and the Attorney General in accordance with the maintained procedures in the event of a breach of the security of the system.*

If Yes, list the Federal laws that are referenced: *No laws specified.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
Yes. An individual or a commercial entity that maintains its own notice procedures which are part of an information security policy for the treatment of personal information and which are otherwise consistent with the timing requirements here, is deemed to be in compliance with these notice requirements if the individual or the commercial entity notifies affected Nebraska residents and the Attorney General in accordance with its notice procedures in the event of a breach of the security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
The Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation.

Enforcing Agency:
Attorney General

Additional Exceptions:
Substitute notice included. Third party notice- An individual or a commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system.

Nevada

Nev. Rev. Stat. §§ 603A.010—603A.040 AND Nev. Rev. Stat. §§ 603A.210—603A.220
https://www.leg.state.nv.us/NRS/NRS-603A.html

***Year most recently amended*:**
Amended October, 2021, 2021 Nevada Laws Ch. 256 (A.B. 61)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

1. "Personal information" means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: (a) Social security number. (b) Driver's license number, driver authorization card number or identification card number. (c) Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account. (d) A medical identification number or a health insurance identification number. (e) A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account. 2. The term does not include the last four digits of a social security number, the last four digits of a driver's license number, the last four digits of a driver authorization card number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public from federal, state or local governmental records.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

"Data collector" means any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after discovery of the breach.

Is there a "Risk of harm" trigger for notification?

Yes. The breach has to materially compromise the security, confidentiality or integrity of personal information maintained by the data collector.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. Additionally, the notification timing requirement takes into consideration the measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system data.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Nevada Attorney General or separate government agency under certain conditions? No.

If Yes, Number of affected residents required for Agency Reporting:

If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?
Yes.

If Yes, number of affected residents to trigger CRA notification*:* More than 1,000 persons at any one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.
Yes. *If data collector complies with GLB, they are in compliance with the notification requirement of this section.*

If Yes, list the Federal laws that are referenced: *GLB.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
Yes. A data collector that maintains its own notification policies and procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the data collector notifies subject persons in accordance with its policies and procedures in the event of a breach of the security of the system data.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
Only for data collectors.

Enforcement damages and penalties:
Civil action can be brought. Awarded damages may include: the reasonable costs of notification, reasonable attorney's fees and costs and punitive damages when appropriate. The costs of notification include, without limitation, labor, materials, postage and any other costs reasonably related to providing the notification. AG can bring action againstg a person to obtain a temporary or permanent injunction against the violation.

Enforcing Agency:
Attorney General

Additional Exceptions:
Substitute notice included.

New Hampshire

N.H. Rev. Stat. Ann. §§ 359-C:19, C:20, C:21; 358-A:4; 332-I:1—332-I:6N.H. Rev. Stat. Ann. §§ 189:65, 189:66

http://www.gencourt.state.nh.us/rsa/html/XXXI/359-C/359-C-19.htm

***Year most recently amended*:**

Effective: August, 2007,

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or other government identification number. (3) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	Yes. "Government identification numbers" are covered.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

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

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

After an investigation to determine the liklihood that the information has been or will be misused.

Is there a "Risk of harm" trigger for notification?

Yes. There has to be a likelihood that the information has been or will be misused.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

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

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. Notice under this section shall include at a minimum: (a) A description of the incident in general terms. (b) The approximate date of breach. (c) The type of personal information obtained as a result of the security breach. (d) The telephonic contact information of the person subject to this section.

Does the law require reporting to the New Hampshire Attorney General or separate government agency under certain conditions? Yes.

***If Yes, Number of affected residents required for Agency Reporting**:* Any number. Any person engaged in trade or commerce shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office.

If Yes, does the agency publish breach data?: Yes. *https://www.doj.nh.gov/consumer/security-breaches/*

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

***If Yes, number of affected residents to trigger CRA notification**:* More than 1,000 consumers.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

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

If Yes, list the Federal laws that are referenced: *No laws specified.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

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

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

Yes.

Enforcement damages and penalties:

Action can be brought for actual damages and for such equitable relief, including an injunction, as the court deems necessary and proper. Also prevailing plaintiff is awarded costs of the suit and reasonable attorney's fees. DAMAGES can be up to 3 times, but not less than 2 times.

Enforcing Agency:

Attorney General enforces.

Additional Exceptions:

Substitute notice included. Notice to the Attorney General shall include the anticipated date of the notice to the individuals and the approximate number of individuals in this state who will be notified.

New Jersey

N.J. Stat. Ann §§ 56:8-161—56:8-166

https://lis.njleg.state.nj.us/nxt/gateway.dll?f=templates&fn=default.htm&vid=Publish:10.1048/Enu

***Year most recently amended*:**

Amended September, 2019, 2019 NJ Sess. Law Serv. Ch. 95 (SENATE 52)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (4) user name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	Yes.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

Any business or public entity that compiles or maintains computerized records that include personal information. A "business" means a sole proprietorship, partnership, corporation, association, or other entity, however organized and whether or not organized to operate at a profit, including a financial institution

organized, chartered, or holding a license or authorization certificate under the law of this State, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution. "Public entity" includes the State, and any county, municipality, district, public authority, public agency, and any other political subdivision or public body in the State. For the purposes of sections 10 through 15 of P.L.2005, c. 226 (C.56:8-161 through C.56:8-166), public entity does not include the federal government.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after the discovery of a breach. However, disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible.

Is there a "Risk of harm" trigger for notification?

Yes. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the New Jersey Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: Any business or public entity required to disclose a breach of security must report the breach to the Division of State Police in the Department of Law and Public Safety.

If Yes, does the agency publish breach data?: Yes. *https://www.cyber.nj.gov/threat-center/public-data-breaches/*

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: More than 1,000 persons at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

No.

If Yes, list the Federal laws that are referenced:

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. A business or public entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and is otherwise consistent with the requirements of this section, shall be deemed to be in compliance with the notification requirements of this section

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

No applicable provision.

Enforcing Agency:

Division of State Police in the Department of Law and Public Safety

Additional Exceptions:

Substitute notice included. Third party notice also included. Email furnishing by a business- Any business or public entity that furnishes an email account shall not provide notification to the email account that is subject to a security breach. The business or public entity shall provide notice by another method described

New Mexico

N. M. Stat. Ann. §§ 57-12C-1—57-12C-12
https://nmonesource.com/nmos/nmsa/en/item/4423/index.do#!b/57-12C-1

***Year most recently amended*:**
Effective: June, 2017,

Scope:

Definition of breach:

"Security breach" means the unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality or integrity of personal identifying information maintained by a person. "Security breach" does not include the good-faith acquisition of personal identifying information by an employee or agent of a person for a legitimate business purpose of the person; provided that the personal identifying information is not subject to further unauthorized disclosure

Definition of personally identifiable information:

"Personal identifying information": (1) means an individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable: (a) social security number; (b) driver's license number; (c) government-issued identification number; (d) account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account; or (e) biometric data.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes. "Government identification numbers" are covered.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

"Service provider" means any person that receives, stores, maintains, licenses, processes or otherwise is permitted access to personal identifying information through its provision of services directly to a person that is subject to regulation.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

If, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud, notification is not required.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notification required may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation; or as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. No later than 45 days following discovery of the breach.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. Notification shall contain: A. the name and contact information of the notifying person; B. a list of the types of personal identifying information that are reasonably believed to have been the subject of a security breach, if known; C. the date of the security breach, the estimated date of the breach or the range of dates within which the security breach occurred, if known; D. a general description of the security breach incident; E. the toll-free telephone numbers and addresses of the major consumer reporting agencies; F. advice that directs the recipient to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach; and G. advice that informs the recipient of the notification of the recipient's rights pursuant to the federal Fair Credit Reporting Act.

Does the law require reporting to the New Mexico Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: More than 1,000 residents as a result of a single security breach.

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?
Yes.

If Yes, number of affected residents to trigger CRA notification*:* More than 1,000 residents as a result of a single breach.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.
Yes. *The provisions of the Data Breach Notification Act shall not apply to a person subject to the federal Gramm-Leach-Bliley Act or the federal Health Insurance Portability and Accountability Act of 1996.*

If Yes, list the Federal laws that are referenced: *GLB, HIPAA*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
Yes. A person that maintains its own notice procedures as part of an information security policy for the treatment of personal identifying information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
The court may issue an injunction; and award damages for actual costs or losses, including consequential financial losses. If the court determines that the person violated this act knolwingly or recklessly, the court may impose a civil penalty of $25,000 or, in the case of failed notification, $10.00 per instance of failed notification up to a maximum of $150,000.

Enforcing Agency:
Attorney General

Additional Exceptions:
Substitute notice included. State and political subdivisions explicitly exempted- "Nothing in the Data Breach Notification Act shall be interpreted to apply to the state of New Mexico or any of its political subdivisions."

New York

N.Y. Gen. Bus. Law § 899-aa
https://www.nysenate.gov/legislation/laws/GBS/899-AA

***Year most recently amended*:**
Amended October, 2019, 2019 Sess. Law News of N.Y. Ch. 117 (S. 5575-B)

Scope:

Definition of breach:

"Breach of the security of the system" shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business. Good faith access to, or acquisition of, private information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

Definition of personally identifiable information:

"Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person. "Private information" shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired: (1) social security number; (2) driver's license number or non-driver identification card number; (3) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; (4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or (5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or (ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

Any person or business which conducts business in NY and either owns, licenses, or maintains computerized data that includes private information.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Upon discovery of the breach.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. Notice shall include contact information for the person or business making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

Does the law require reporting to the New York Attorney General or separate government agency under certain conditions? Yes.

***If Yes, Number of affected residents required for Agency Reporting**:* Any number of New York residents, the person or buisness shall notify the attorney general, the department of state, and the division of state police.

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

***If Yes, number of affected residents to trigger CRA notification**:* More than 5,000 New york residents.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *If notice of a breach is made to affected persons pursuant to the breach notification requirements of the following laws, nothing in this section requires additional notice to the affected individuals: i. GLB, ii. HIPAA, iii. part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, iv. any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.*

If Yes, list the Federal laws that are referenced: *HIPAA, GLB.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

The court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of $5,000 or up to $20,000 per instance of failed notification, provided that the latter amount shall not exceed $250,000.

Enforcing Agency:

Attorney General

Additional Exceptions:

Determinign whether a breach has occurred: (i). In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person. (ii). In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others: (1) indications that the information is in the physical possession and control of an

unauthorized person, such as a lost or stolen computer or other device containing information; or (2) indications that the information has been downloaded or copied; or (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

North Carolina

N.C. Gen. Stat. §§ 75-61, 75-65
https://www.ncleg.net/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-61.html AND
https://www.ncleg.net/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-65.html

***Year most recently amended*:**
Amended January, 2016, 2015 North Carolina Laws S.L. 2015-193 (H.B. 607)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

--A person's first name or first initial and last name in combination with: (1) Social security or employer taxpayer identification numbers. (2) Drivers license, State identification card, or passport numbers. (3) Checking account numbers. (4) Savings account numbers. (5) Credit card numbers. (6) Debit card numbers. (7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6). (8) Digital signatures. (9) Any other numbers or information that can be used to access a person's financial resources. (10) Biometric data. (11) Fingerprints. For the purposes of this section, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes.
Medical Information	No.	**Paper Records**	Yes.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

"Business".--A sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. Business shall not include any government or governmental subdivision or agency.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after the discovery of a breach.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notice required by this section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security. Additionally, the speed of the notification to the individual takes into consideration the measures necessary to determine contact information, the scope of the breach, and to restore the systems.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The notice shall be clear and conspicuous. The notice shall include all of the following: (1) A description of the incident in general terms. (2) A description of the type of personal information that was subject to the unauthorized access and acquisition. (3) A description of the general acts of the business to protect the personal information from further unauthorized access. (4) A telephone number for the business that the person may call for further information and assistance, if one exists. (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. (6) The toll-free numbers and addresses for the major consumer reporting agencies. (7) The toll-free numbers, addresses, and

Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

Does the law require reporting to the North Carolina Attorney General or separate government agency under certain conditions? Yes.

***If Yes, Number of affected residents required for Agency Reporting**:* Any number. If a business provides notice to an affected person pursuant to this section, the business shall notify the Consumer Protection Division of the Attorney General's Office.

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

***If Yes, number of affected residents to trigger CRA notification**:* More than 1,000 persons at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *Financial institutions that are subject to and in compliance with the Federal Interagency Guidance are deemed to be in compliance with this section.*

If Yes, list the Federal laws that are referenced: *Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

Yes.

Enforcement damages and penalties:

A violation of this section is a violation of G.S. 75-1.1, unfair and deceptive acts or practices.

Enforcing Agency:

Attorney General

Additional Exceptions:

Substitute notice included. Third party notice included.

North Dakota

N.D. Cent. Code §§ 51-30-01—51-20-07
https://www.ndlegis.gov/cencode/t51c30.pdf

***Year most recently amended*:**
Effected: August, 2015,

Scope:

Definition of breach:

"Breach of the security system" means unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable. Good-faith acquisition of personal information by an employee or agent of the person is not a breach of the security of the system, if the personal information is not used or subject to further unauthorized disclosure.

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted: (1) The individual's social security number; (2) The operator's license number assigned to an individual by the department of transportation; (3) A nondriver color photo identification card number assigned to the individual by the department of transportation; (4) The individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts; (5) The individual's date of birth; (6) The maiden name of the individual's mother; (7) Medical information; (8) Health insurance information;(9) An identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or (10) The individual's digitized or other electronic signature.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

Any person that owns or licenses computerized data that includes personal information.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?
Immediately after the discovery of the breach.

Is there a "Risk of harm" trigger for notification?
No.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?
Yes. The notification required by this chapter may be delayed if a law enforcement agencydetermines that the notification will impede a criminal investigation. Additionally, the speed of the notification takes into consideration the measures necessary to determine the scope of the breach and to restore the integrity of the data system.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?
No.

Does the law specify how notification must be given?
Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?
No.

Does the law require reporting to the North Dakota Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: Exceeds 250 individuals.
If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?
No.

If Yes, number of affected residents to trigger CRA notification:

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *A financialinstitution, trust company, or credit union that is subject to, examined for, and in compliance withthe federal interagency guidance on response programs for unauthorized access to customerinformation and customer notice is in compliance with this chapter. A covered entity, businessassociate, or subcontractor subject to breach notification requirements under title 45, Code ofFederal Regulations, subpart D, part 164, is considered to be in compliance with this chapter.*

If Yes, list the Federal laws that are referenced: *a financial institution in compliance and examined for compliance with the federal interagency guidance on response programs for unauthorized access to customerinformation and customer notice. Also, title 45, Code ofFederal Regulations, subpart D, part*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. A person that maintains its own notification proceduresas part of an information security policy for the treatment of personal information and isotherwise consistent with the timing requirements of this chapter is deemed to be in compliancewith the notification requirements of this chapter if the person notifies subject individuals inaccordance with its policies in the event of a breach of security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

AG may bring action.

Enforcing Agency:

Attorney General.

Additional Exceptions:

Ohio

Ohio Rev. Code Ann. §§ 1347.12; 1349.19, 1349.191—1349.192
https://codes.ohio.gov/ohio-revised-code/section-1347.12 AND https://codes.ohio.gov/ohio-revised-code/section-1349.19 AND https://codes.ohio.gov/ohio-revised-code/section-1349.191

***Year most recently amended*:**
Amended September, 2015, 2015 Ohio Laws File 12 (Am. H.B. 141)

Scope:

Definition of breach:

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

Definition of personally identifiable information:

"Personal information" means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: (i) Social security number; (ii) Driver's license number or state identification card number; (iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

Individual or business entity conducting business in Ohio that owns, licenses, is custodian of or stores computerized data that includes personal information.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after the discovery of the breach.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The person may delay the disclosure or notification required if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. No later than 45 days following the discovery or notification of the breach.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Ohio Attorney General or separate government agency under certain conditions? No.

If Yes, Number of affected residents required for Agency Reporting:

If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: More than 1,000 residents in a single occurence of a breach.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *This section does not apply to any person or entity that is a covered entity as defined in 45 C.F.R. 160.103, as amended. Additionally, a financial institution, trust company, or credit union or any affiliate of a financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the requirements of this section.*

If Yes, list the Federal laws that are referenced: *Financial institutions subject to federal laws about customer notifications.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
AG may bring civil action. Appropriate relief includes a temporary restraining order, preliminary or permanent injunction, and civil penalties. Civil penalty is as follows: $1,000 for each day the entity has intentionally or recklessly failed to comply with the applicable section. If the entity has intentionally or recklessly failed to comply for more than 60 days, an additional $5,000 penalty for each day the entity fails to comply. If the entity has failed to comply for more than 90 days, civil penalty of up to $10,000 for each day the entity fails to comply.

Enforcing Agency:
Attorney General.

Additional Exceptions:

Oklahoma

Okla. Stat. tit. 24 § 161—166
http://www.oklegislature.gov/OSSTATUESTITLE.HTML

***Year most recently amended*:**
Effective: November, 2008,

Scope:

Definition of breach:

"Breach of the security of a system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

Definition of personally identifiable information:

"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted: a. social security number, b. driver license number or state identification card number issued in lieu of a driver license, or c. financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

An individual or entity that owns or licenses computerized data that includes personal information of a resident. "Individual" means natural person. "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint

ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?
Immediately after the discovery of the breach.

Is there a "Risk of harm" trigger for notification?
Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?
Yes. Notice required by this section may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?
No.

Does the law specify how notification must be given?
Yes.
If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?
No.

Does the law require reporting to the Oklahoma Attorney General or separate government agency under certain conditions? No.
If Yes, Number of affected residents required for Agency Reporting:
If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?
No.
If Yes, number of affected residents to trigger CRA notification:

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is in compliance here. Also, an entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures, or guidelines established by the primary or functional federal regulator of the entity shall be deemed to be in compliance*

If Yes, list the Federal laws that are referenced: *Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies residents of this state in accordance with its procedures in the event of a breach of security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

AG shall have exclusive authority to bring action and obtain either actual damages for a violation OR a civil penalty not exceeding $150,000 per breah.

Enforcing Agency:

Attorney General

Additional Exceptions:

Substitute notice included. A violation of this act by a state-chartered or state-licensed financial institution shall be enforceable exclusively by the primary state regulator of the financial institution.

Oregon

Or. Rev. Stat. §§ 646A.600–.646A.604, 646A.624–646A.626
https://www.oregonlegislature.gov/bills_laws/ors/ors646A.html

***Year most recently amended*:**
Amended January, 2020, 2019 Oregon Laws Ch. 180 (S.B. 684)

Scope:

Definition of breach:

"Breach of security" means an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains or possesses. "Breach of security" does not include an inadvertent acquisition of personal information by a person or the person's employee or agent if the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.

Definition of personally identifiable information:

"Personal information" means: (A) A consumer's first name or first initial and last name in combination with any one or more of the following data elements, if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired: (i) A consumer's Social Security number; (ii) A consumer's driver license number or state identification card number issued by the Department of Transportation; (iii) A consumer's passport number or other identification number issued by the United States; (iv) A consumer's financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account, or any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account; (v) Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction; (vi) A consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or (vii) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer. (B) A user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification. (C) Any of the data elements or any combination of the data elements described in subparagraph (A) or (B) of this paragraph without the consumer's user name, or the consumer's first name or first initial and last name, if: (i) Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and(ii) The data element or combination of data elements would enable a person to commit identity theft against a consumer.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes.
Medical Information	Yes.	**Paper Records**	No.

De-identified information	Yes.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

"Covered entity" means a person that owns, licenses, maintains, stores, manages, collects, processes, acquires or otherwise possesses personal information in the course of the person's business, vocation, occupation or volunteer activities. "Person" means an individual, private or public corporation, partnership, cooperative, association, estate, limited liability company, organization or other entity, whether or not organized to operate at a profit, or a public body. "Public body" means state government bodies, local government bodies and special government bodies.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after the discovery of the breach.

Is there a "Risk of harm" trigger for notification?

Yes. In order to trigger a notification, the breach of security must materially compromise the security, confidentiality, or integrity of personal information that a person maintains or possesses.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. A covered entity may delay giving the notice only if a law enforcement agency determines that a notification will impede a criminal investigation and if the law enforcement agency requests in writing that the covered entity delay the notification.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. No later than 45 days after discovering or receiving notification of the breach of security.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. Notice under this section must include, at a minimum: (a) A description of the breach of security in general terms; (b) The approximate date of the breach of security; (c) The type of personal information that was subject to the breach of security; (d) Contact information for the covered entity; (e) Contact information for national consumer reporting agencies; and (f) Advice to the consumer to report suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission.

Does the law require reporting to the Oregon Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: Number of consumers to whom the covered entity must send notice to exceeds 250.

If Yes, does the agency publish breach data?: Yes. *https://justice.oregon.gov/consumer/databreach/*

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: More than 1,000 consumers.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *This law does not apply to: i. Personal information that is subject to, and a person that complies with, notification requirements or procedures for a breach of security that the person's primary or functional federal regulator adopts, promulgates or issues in rules, regulations, procedures, guidelines or guidance, if the personal information and the person would otherwise be subject to this act; ii. Personal information that is subject to, and a person that complies with, a state or federal law that provides greater protection to personal information and disclosure requirements at least as thorough as the protections and disclosure requirements provided under this section; iii. Title V of GLB; iv. HIPAA and HITECH Act.*

If Yes, list the Federal laws that are referenced: *GLB, HITECH Act, HIPAA*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

In addition to all other penalties and enforcement provisions by law, any person who violates or who procures, aids or abets in the violation of this section shall be subject to a penalty of not more than $1,000 for every violation. Max penalty for any occurrence shall not exceed $500,000.

Enforcing Agency:

Attorney General.

Additional Exceptions:
Substitute notice included. Third party (vendor) notice included.

Pennsylvania

73 Pa. Cons. Stat. §§ 2301–2308, 2329

https://govt.westlaw.com/pac/Browse/Home/Pennsylvania/UnofficialPurdonsPennsylvaniaStatutes?guid=N9B3F41908C4F11DA86FC8D90DD1949D4&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)

***Year most recently amended*:**
Effective: June, 2006,

Scope:

Definition of breach:

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

Definition of personally identifiable information:

An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: (i) Social Security number. (ii) Driver's license number or a State identification card number issued in lieu of a driver's license. (iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

An entity that maintains, stores or manags computerized data that includes personal information. An "entity" is a State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after the breach.

Is there a "Risk of harm" trigger for notification?

Yes. The breach has to materially compromise the security or confidentiality of personal information, causing the entity to reasonably beleive that loss or injury to a resident has occurred or will occur.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notification required by this act may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Pennsylvania Attorney General or separate government agency under certain conditions? No.

If Yes, Number of affected residents required for Agency Reporting:
If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: More than 1,000 persons at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this act. Additionally, an entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity's primary or functional Federal regulator shall be in compliance with this act.*

If Yes, list the Federal laws that are referenced: *Compliance with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

A violation of this act shall be deemed to be an unfair or deceptive act or practice.

Enforcing Agency:

Attorney General.

Additional Exceptions:

Rhode Island

11 R.I. Gen Laws §§ 11-49.3-2—11-49.3-6
http://webserver.rilin.state.ri.us/Statutes/TITLE11/11-49.3/INDEX.HTM

***Year most recently amended*:**
Effective: July, 2016,

Scope:

Definition of breach:

"Breach of the security of the system" means unauthorized access or acquisition of unencrypted, computerized data information that compromises the security, confidentiality, or integrity of personal information maintained by the municipal agency, state agency, or person. Good-faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system; provided, that the personal information is not used or subject to further unauthorized disclosure.

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name and the data elements are not encrypted or are in hard copy, paper format: (i) Social security number; (ii) Driver's license number, Rhode Island identification card number, or tribal identification number; (iii) Account number, credit, or debit card number, in combination with any required security code, access code, password, or personal identification number, that would permit access to an individual's financial account; (iv) Medical or health insurance information; or (v) E-mail address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

Any municipal agency, state agency, or person that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information. "Municipal agency" means any department, division, agency, commission, board, office, bureau, authority, quasi-public authority, or school, fire, or water district within Rhode Island, other than a state agency, and any other agency that is in any branch of municipal government

and exercises governmental functions other than in an advisory nature. "State agency" means any department, division, agency, commission, board, office, bureau, authority, or quasi-public authority within Rhode Island; either branch of the Rhode Island general assembly or an agency or committee thereof; the judiciary; or any other agency that is in any branch of Rhode Island state government and that exercises governmental functions other than in an advisory nature. "Person" shall include any individual, sole proprietorship, partnership, association, corporation, joint venture, business, legal entity, trust, estate, cooperative, or other commercial entity.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after the discovery of the breach.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notification required by this section may be delayed if a federal, state, or local law enforcement agency determines that the notification will impede a criminal investigation.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. No later than 45 days after confirmation of the breach.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The notification to individuals must include the following information to the extent known: (1) A general and brief description of the incident, including how the security breach occurred and the number of affected individuals; (2) The type of information that was subject to the breach; (3) Date of breach, estimated date of breach, or the date range within which the breach occurred; (4) Date that the breach was discovered; (5) A clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact: (i) The credit reporting agencies; (ii) Remediation service providers; (iii) The attorney general; and (6) A clear and concise description of the consumer's ability to file or obtain a

police report; how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

Does the law require reporting to the Rhode Island Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: More than 500 Rhode Island residents.

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification: More than 500 Rhode Island residents.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *Compliance with this section if the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice is followed by the following: financial institution, trust company, credit union, or its affiliates. Additionally, HIPAA comliance is deemed to be in compliance with this section.*

If Yes, list the Federal laws that are referenced: *HIPAA, Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. The municipal agency, state agency, or person maintains its own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with these timing and notification requirements is compliant with this section. Additionally, The person who maintains a security breach procedure pursuant to procedures established by the primary or functional regulator is also in compliant.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

Each reckless violation of this chapter is a civil violation for which a penalty of not more than one hundred dollars ($100) per record may be adjudged against a defendant. Each knowing and willful violation of this chapter is a civil violation for which a penalty of not more than two hundred dollars ($200) per record may be adjudged against a defendant.

Enforcing Agency:

Attorney General.

Additional Exceptions:

Substitute notice included.

South Carolina

S.C. Code. Ann. 39-1-90
https://www.scstatehouse.gov/code/t39c001.php

***Year most recently amended*:**
Amended July, 2013, 2013 South Carolina Laws Act 15 (H.B. 3248)

Scope:

Definition of breach:

"Breach of the security of the system" means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident. Good faith acquisition of personal identifying information by an employee or agent of the person for the purposes of its business is not a breach of the security of the system if the personal identifying information is not used or subject to further unauthorized disclosure.

Definition of personally identifiable information:

"Personal identifying information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted: (a) social security number; (b) driver's license number or state identification card number issued instead of a driver's license; (c) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or (d) other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information. "Person" includes a natural person or an individual, and an

organization. "Organization" means a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative or association.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?
Immediately after the discovery of the breach.

Is there a "Risk of harm" trigger for notification?
Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?
Yes. The notification required by this section may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it no longer compromises the investigation.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?
No.

Does the law specify how notification must be given?
Yes.
If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?
No.

Does the law require reporting to the South Carolina Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: More than 1,000 persons at one time, notify the Consumer Protection Division of the Department of Consumer Affairs

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?
Yes.

If Yes, number of affected residents to trigger CRA notification*:* More than 1,000 persons at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *Does not apply to those in GLB compliance.*

If Yes, list the Federal laws that are referenced: *GLB, Federal Interagency Guidance*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. A person that maintains its own notification procedures as part of an information security policy for the treatment of personal identifying information and is otherwise consistent with the timing requirements of this section is considered to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

Yes.

Enforcement damages and penalties:

Can recover damages in a case of wilful and knowing violation, can recover actual damages resulting from a violation in case of a negligent violation. A person who knowingly and wilfully violates this section is subject to fine of $1,000 for each resident whose info was accessible by reason of the breach.

Enforcing Agency:

Department of Consumer Affairs.

Additional Exceptions:

Substitute notice included.

South Dakota

S.D. Codified Laws §§ 22-40-19—22-40-26
https://sdlegislature.gov/Statutes/Codified_Laws/2047702

***Year most recently amended*:**
Effective: July, 2018,

Scope:

Definition of breach:

"Breach of system security," the unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder. The term does not include the good faith acquisition of personal or protected information by an employee or agent of the information holder for the purposes of the information holder if the personal or protected information is not used or subject to further unauthorized disclosure.

Definition of personally identifiable information:

"Personal information," a person's first name or first initial and last name, in combination with any one or more of the following data elements: (a) Social security number; (b) Driver license number or other unique identification number created or collected by a government body; (c) Account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person's financial account; (d) Health information as defined in 45 CFR 160.103; or (e) An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes. An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication p	**Passports**	Yes- covers other unique identification numbers created or collected by a government body.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

"Information holder," any person or business that conducts business in this state, and that owns or licenses computerized personal or protected information of residents of this state.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Following discovery, the information holder shall disclose the breach to any resident impacted. But, following an appropriate investigation, if the information holder reasonably determines that the breach will not likely result in harm to the affected person, notice is not required.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. A notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. No later than 60 days from the discovery or notification of the breach of system security.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the South Dakota Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: 250 residents of this state.
If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification*:* Any number.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *Any information holder that is regulated by federal law or regulation, including the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, as amended) or the Gramm Leach Bliley Act (15 U.S.C. § 6801 et seq., as amended) and that maintains procedures for a breach of system security pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional federal regulator is deemed to be in compliance with this chapter if South Dakota residents are properly notified.*

If Yes, list the Federal laws that are referenced: *GLB, HIPAA*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. If an information holder maintains its own notification procedure as part of an information security policy for the treatment of personal or protected information and the policy is otherwise consistent with the timing requirements of this section, the information holder is in compliance with the notification requirements of § 22-40-22 if the information holder notifies each person in accordance with the information holder's policies in the event of a breach of system security.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

The attorney general may bring an action to recover on behalf of the state a civil penalty of not more than $10,000 per day per violation. The attorney general may recover attorney's fees and any costs associated with any action brought under this section.

Enforcing Agency:

Attorney General.

Additional Exceptions:

Tennessee

Tenn. Code Ann. §§ 47-18-2105—47-18-2107
https://advance.lexis.com/documentpage/?pdmfid=1000516&crid=276bded8-ea5d-427c-8661-5cb10d673b62&nodeid=ABVAAUAAVAAH&nodepath=%2fROOT%2fABV%2fABVAAU%2fABVAAUAAV%2fABVAAUAAVAAH&level=4&haschildren=&populated=false&title=47-18-2107.+Release+of+personal+consumer+information.&config=025054JABlOTJjNmIyNi0wYjI0LTRjZGEtYWE5ZC0zNGFhOWNhMjFlNDgKAFBvZENhdGFsb2cDFQ14bX2GfyBTaI9WcPX5&pddocfullpath=%2fshared%2fdocument%2fstatutes-legislation%2furn%3acontentItem%3a4X8K-XB40-R03J-K1K5-00008-00&ecomp=f38_kkk&prid=ae167118-3d03-4a8c-af3c-83c6191bfd5e

***Year most recently amended*:**
Amended September, 2019, 2019 Tennessee Laws Pub. Ch. 459 (H.B. 948)

Scope:

Definition of breach:

"Breach of system security": (A) Means the acquisition of the information set out in subdivision (a)(1)(A)(i) or (a)(1)(A)(ii) by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder: (i) Unencrypted computerized data; or (ii) Encrypted computerized data and the encryption key; and (B) Does not include the good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder if the personal information is not used or subject to further unauthorized disclosure.

Definition of personally identifiable information:

"Personal information": (A) Means an individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements: (i) Social security number; (ii) Driver license number; or (iii) Account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

"Information holder" means any person or business that conducts business in this state, or any agency of this state or any of its political subdivisions, that owns or licenses computerized personal information of residents of this state.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?
Immediately after the discovery of the breach.

Is there a "Risk of harm" trigger for notification?
No.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?
Yes. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?
Yes. No later than 45 days from the discovery or notification of the breach.

Does the law specify how notification must be given?
Yes.
If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?
No.

Does the law require reporting to the Tennessee Attorney General or separate government agency under certain conditions? No.

If Yes, Number of affected residents required for Agency Reporting:
If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?
Yes.

If Yes, number of affected residents to trigger CRA notification: More than 1,000 persons at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.
Yes. *This section does not apply to information holders subject to GLB or HIPAA.*
If Yes, list the Federal laws that are referenced: *GLB, HIPAA*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
Yes. If an information holder maintains its own notification procedures as part of an information security policy for the treatment of personal information and if the policy is otherwise consistent with the timing requirements of this section, the information holder is in compliance with the notification requirements of this section, as long as the information holder notifies subject persons in accordance with its policies in the event of a breach of system security.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
Yes.

Enforcement damages and penalties:
Can recover damages and to enjoin the information holder from furhter action in violation of this section. Whichever of the following is greater: $10,000; $5,000 per day for each day that a person's identity has been assumed; or ten times the amount obtained or attempted to be obtained by the person using the identity theft. Any knowing or willful violation of the terms of an injunction or order issued pursuant to this section shall be punishable by a civil penalty of not more than $5,000 for each and every violation.

Enforcing Agency:
Attorney General

Additional Exceptions:
Substitute notice included.

Texas

Tex. Bus. & Com. Code §§ 521.002, 521.053, 521.151
https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm#521.002

***Year most recently amended*:**
Amended September 2021, 2021 Tex. Sess. Law Serv. Ch. 496 (H.B. 3746) (VERNON'S)

Scope:

Definition of breach:

"Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.

Definition of personally identifiable information:

"Sensitive personal information" means, subject to Subsection (b): (A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: (i) social security number; (ii) driver's license number or government-issued identification number; or (iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (B) information that identifies an individual and relates to: (i) the physical or mental health or condition of the individual; (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	Yes. Covers governmnet-issued identification numbers.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?
Immediately after the discovery of the breach.

Is there a "Risk of harm" trigger for notification?
No.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?
Yes. A person may delay providing required notice at the request of a law enforcement agency that determines that the notification will impede a criminal investigation.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?
Yes. Not later than the 60th day after the date on which the person determines that the breach occurred.

Does the law specify how notification must be given?
Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?
No.

Does the law require reporting to the Texas Attorney General or separate government agency under certain conditions? Yes.

***If Yes, Number of affected residents required for Agency Reporting**:* At least 250 residents of this state.

If Yes, does the agency publish breach data?: Yes.
https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage

Does the law require notifying consumer reporting agencies under certain conditions?
Yes.

***If Yes, number of affected residents to trigger CRA notification**:* More than 10,000 persons at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.
No.

If Yes, list the Federal laws that are referenced:

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
Yes. A person who maintains the person's own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
A person who violates this chapter is liable to this state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. Additionally, a person who fails to take reasonable action to comply with Section 521.053(b) is liable to this state for a civil penalty of not more than $100 for each individual to whom notification is due under that subsection for each consecutive day that the person fails to take reasonable action to comply with that subsection. Civil penalties under this section may not exceed $250,000 for all individuals to whom notification is due after a single breach.

Enforcing Agency:
Attorney General.

Additional Exceptions:
Notice provided to the AG shall include: (1) a detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach; (2) the number of residents of this state affected by the breach at the time of notification; (3) the number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification; (4) the measures taken by the person regarding the breach; (5) any measures the person intends to take regarding the breach after the notification under this subsection; and (6) information regarding whether law enforcement is engaged in investigating the breach.

Utah

Utah Code Ann. §§ 13-44-101—13-44-301
https://le.utah.gov/xcode/Title13/Chapter44/13-44.html?v=C13-44_1800010118000101

***Year most recently amended*:**
Amended May, 2019, 2019 Utah Laws Ch. 348 (S.B. 193)

Scope:

Definition of breach:

"Breach of system security" means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.

Definition of personally identifiable information:

"Personal information" means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable: (i) Social Security number; (ii) (A) financial account number, or credit or debit card number; and (B) any required security code, access code, or password that would permit access to the person's account; or (iii) driver license number or state identification card number.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

A person who owns or licenses computerized data that includes personal information concerning a Utah resident.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	No.	**Local government agencies?**	No.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

After an investigation to determine the liklihood that personal information has been or will be misused for identity theft or fraud pruposes.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. A person may delay providing notification under Subsection (1) at the request of a law enforcement agency that determines that notification may impede a criminal investigation.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

No.

Does the law require reporting to the Utah Attorney General or separate government agency under certain conditions? No.

If Yes, Number of affected residents required for Agency Reporting:

If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?

No.

If Yes, number of affected residents to trigger CRA notification:

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *A person who is regulated by state or federal law and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with this part if the person notifies each affected Utah resident in accordance with the other applicable law in the event of a breach. Additionally, this chapter does not apply to a financial institution or an affiliate, as defined in 15 U.S.C. Sec. 6809, of a financial institution.*

If Yes, list the Federal laws that are referenced: *No federal laws specified.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
Yes. If a person maintains the person's own notification procedures as part of an information security policy for the treatment of personal information the person is considered to be in compliance with this chapter's notification requirements if the procedures are otherwise consistent with this chapter's timing requirements and the person notifies each affected Utah resident in accordance with the person's information security policy in the event of a breach.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
A person who violates this chapter's provisions is subject to a civil penalty of:(a) no greater than $2,500 for a violation or series of violations concerning a specific consumer; and(b) no greater than $100,000 in the aggregate for related violations concerning more than one consumer. In addition to the penalties above, the AG may seek injunctive relief to prevent future violations of this chapter; and attorneys fees and costs.

Enforcing Agency:
Attorney General

Additional Exceptions:

Vermont

Vt. Stat. Ann. tit. 9, §§ 2430, 2435
https://legislature.vermont.gov/statutes/chapter/09/062

***Year most recently amended*:**
Amended July, 2020, 2020 Vermont Laws No. 89 (S. 110)

Scope:

Definition of breach:

"Security breach" means unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information or login credentials maintained by a data collector.

Definition of personally identifiable information:

"Personally identifiable information" means a consumer's first name or first initial and last name in combination with one or more of the following digital data elements, when the data elements are not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons: (i) a Social Security number; (ii) a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction; (iii) a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords; (iv) a password, personal identification number, or other access code for a financial account; (v) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; (vi) genetic information; and (vii)(I) health records or records of a wellness program or similar program of health promotion or disease prevention; (II) a health care professional's medical diagnosis or treatment of the consumer; or (III) a health insurance policy number.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes.
Medical Information	Yes.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

Any data collector that owns or licenses computerized personally identifiable information or login credentials. "Data collector" means a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after the discovery or notification to the data collector of the breach.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notice to a consumer required by this subsection shall be delayed upon request of a law enforcement agency.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. Not later than 45 days after the discovery or notification

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The notice to a consumer required in subdivision (1) of this subsection shall be clear and conspicuous. A notice to a consumer of a security breach involving personally identifiable information shall include a description of each of the following, if known to the data collector: (A) the incident in general terms; (B) the type of personally identifiable information that was subject to the security breach; (C) the general acts of the data collector to protect the personally identifiable information from further security breach; (D) a telephone number, toll-free if available, that the consumer may call for further information and assistance; (E) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and (F) the approximate date of the security breach.

Does the law require reporting to the Vermont Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting*:* Any number of residents.

If Yes, does the agency publish breach data?: Yes. *https://ago.vermont.gov/data-security-breaches/*

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification*:* More than 1,000 consumers at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *Exceptions for HIPAA and Federal Interagency Guidance, and financial institutions regulated by the Department of Financial Regulation.*

If Yes, list the Federal laws that are referenced: *The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, HIPAA, and a financial institution regulated by the Department of Financial Regulation.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

A person who violates a provision of this section commits an unfair and deceptive act in commerce. AG or Dept. of Finance may investigate, prosecute, and obtain remedies for violations.

Enforcing Agency:

Attorney General.

Additional Exceptions:

Virginia

Va. Code Ann. §§ 18.2—186.6; 32.1-127.1:05
https://law.lis.virginia.gov/vacode/title18.2/chapter6/section18.2-186.6/

***Year most recently amended*:**
Amended July, 2020, 2020 Virginia Laws Ch. 264 (H.B. 1334)

Scope:

Definition of breach:

"Breach of the security of the system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

Definition of personally identifiable information:

"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: 1. Social security number; 2. Driver's license number or state identification card number issued in lieu of a driver's license number; 3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; 4. Passport number; or 5. Military identification number.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	Yes.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

"Individual" means a natural person. "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint

ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?
Immediately after the discovery of the breach.

Is there a "Risk of harm" trigger for notification?
Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?
Yes. Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?
No.

Does the law specify how notification must be given?
Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?
Yes. Notice required by this section shall include a description of the following: (1) The incident in general terms; (2) The type of personal information that was subject to the unauthorized access and acquisition; (3) The general acts of the individual or entity to protect the personal information from further unauthorized access; (4) A telephone number that the person may call for further information and assistance, if one exists; and (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Does the law require reporting to the Virginia Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting*:* More than 1,000 persons at one time.

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification*:* More than 1,000 persons at one time.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *Entities regulated by GLB Act or entities that comply with notification requirements pursuant to rules or regulations established by entity's primary state or federal regulator.*

If Yes, list the Federal laws that are referenced: *GLB*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information that are consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if it notifies residents of the Commonwealth in accordance with its procedures in the event of a breach of the security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

Yes.

Enforcement damages and penalties:

Recover direct economic damages. AG may impose a civil penalty not to exceed $150,000 per breach of the security of the system that are discovered in a single investigation.

Enforcing Agency:

Attorney General.

Additional Exceptions:

Washington

Wash. Rev. Code §§ 19.255.005—19.255.020; 42.56.590
https://apps.leg.wa.gov/RCW/default.aspx?cite=19.255.010

***Year most recently amended*:**
Amended March, 2020, 2019 Wash. Legis. Serv. Ch. 241 (S.H.B. 1071)

Scope:

Definition of breach:

"Breach of the security of the system" means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

Definition of personally identifiable information:

"Personal information" means: (a)(i) An individual's first name or first initial and last name in combination with any one or more of the following data elements: (A) Social security number; (B) Driver's license number or Washington identification card number; (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account; (D) Full date of birth; (E) Private key that is unique to an individual and that is used to authenticate or sign an electronic record; (F) Student, military, or passport identification number; (G) Health insurance policy number or health insurance identification number; (H) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or (I) Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual; (ii) User name or email address in combination with a password or security questions and answers that would permit access to an online account; and (iii) Any of the data elements or any combination of the data elements described in (a)(i) of this subsection without the consumer's first name or first initial and last name if: (A) Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and (B) The data element or combination of data elements would enable a person to commit identity theft against a consumer.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	Yes.
Medical Information	Yes.	**Paper Records**	Yes.
De-identified information	Yes.	**Publicly available information**	No.

Encrypted Information*	Yes.				

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

Any person or business that conducts business in this state and that owns or licenses data that includes personal information. Additionally, 42.56.590 covers any agency that owns or licenses data that includes personal information. These entities are data owners or licensees.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after the discovery of the breach. However, notice is not required is there is no risk of harm.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. The notification required by this section may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Yes. No more than 30 calendar days after the breach was discovered.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	No.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. Any entity that is required to issue notification pursuant to this section shall meet all of the following requirements:(a) The notification must be written in plain language; and(b) The notification must include, at a minimum, the following information: (i) The name and contact information of the reporting person or

business subject to this section; (ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; (iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and (iv) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

Does the law require reporting to the Washington Attorney General or separate government agency under certain conditions? Yes.

If Yes, Number of affected residents required for Agency Reporting: More than 500 residents of a single breach. An entity that is required to issue a notification pursuant to this section to more than five hundred Washington residents as a result of a single breach shall notify the attorney general of the breach no more t

If Yes, does the agency publish breach data?: Yes. *https://www.atg.wa.gov/data-breach-notifications*

Does the law require notifying consumer reporting agencies under certain conditions?

No.

If Yes, number of affected residents to trigger CRA notification:

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *A covered entity under the federal health insurance portability and accountability act is deemed to have complied with the requirements of this chapter with respect to protected health information if it has complied with section 13402 of the federal health information technology for economic and clinical health act. Additionally, a financial institution under the authority of the office of the comptroller of the currency, the federal deposit insurance corporation, the national credit union administration, or the federal reserve system is deemed to have complied with the requirements of this chapter with respect to "sensitive customer information" as defined in the interagency guidelines establishing information security standards if the institution provides proper notice.*

If Yes, list the Federal laws that are referenced: *HIPAA, Federal Interagency Guidelines*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. A person, business, or agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

Yes.

Enforcement damages and penalties:

Can recover damages.

Enforcing Agency:

Attorney General.

Additional Exceptions:

West Virginia

W. Va. Code §§ 46A-2A-101—46A-2A-105
http://www.wvlegislature.gov/WVCODE/Code.cfm?chap=46a&art=2A#2A

***Year most recently amended*:**
Effective: June, 2008,

Scope:

Definition of breach:

"Breach of the security of a system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of this state. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

Definition of personally identifiable information:

"Personal information" means the first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted: (A) Social security number; (B) Driver's license number or state identification card number issued in lieu of a driver's license; or (C) Financial account number, or credit card, or debit card number in combination with any required security code, access code or password that would permit access to a resident's financial accounts.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	No.	**Passports**	No.
Medical Information	No.	**Paper Records**	No.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	Yes.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?*** Yes.

What entities are covered?

An individual or entity that owns or licenses computerized data that includes personal information. "Individual" means a natural person. "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint

ventures, governments, governmental subdivisions, agencies or instrumentalities, or any other legal entity, whether for profit or not for profit.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Immediately after the discovery of the breach.

Is there a "Risk of harm" trigger for notification?

Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Yes. Notice required by this section may be delayed if a law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

No.

Does the law specify how notification must be given?

Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?

Yes. The notice shall include: (1) To the extent possible, a description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person, including social security numbers, driver's licenses or state identification numbers and financial data; (2) A telephone number or website address that the individual may use to contact the entity or the agent of the entity and from whom the individual may learn: (A) What types of information the entity maintained about that individual or about individuals in general; and (B) Whether or not the entity maintained information about that individual. (3) The toll-free contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a fraud alert or security freeze.

Does the law require reporting to the West Virginia Attorney General or separate government agency under certain conditions? No.

If Yes, Number of affected residents required for Agency Reporting:

If Yes, does the agency publish breach data?: No.

Does the law require notifying consumer reporting agencies under certain conditions?

Yes.

If Yes, number of affected residents to trigger CRA notification*:* more than 1,000 persons of a breach of security.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

Yes. *This subsection shall not apply to an entity who is subject to Title V of the Gramm Leach Bliley Act. A financial institution that responds in accordance with the notification guidelines prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this article. Lastly, an entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures or guidelines established by the entity's primary or functional regulator shall be in compliance with this article.*

If Yes, list the Federal laws that are referenced: *GLB.*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Yes. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies residents of this state in accordance with its procedures in the event of a breach of security of the system.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

No.

Enforcement damages and penalties:

The Attorney General shall have exclusive authority to bring action. No civil penalty may be assessed in an action unless the court finds that the defendant has engaged in a course of repeated and willful violations of this article. No civil penalty shall exceed $150,000 per breach of security of the system or series of breaches of a similar nature that are discovered in a single investigation.

Enforcing Agency:

Attorney General.

Additional Exceptions:

Wisconsin

Wis. Stat. § 134.98
https://docs.legis.wisconsin.gov/statutes/statutes/134/98

***Year most recently amended*:**
Effective: March, 2008,

Scope:

Definition of breach:

Acquisition by a person whom the entity that maintains, licenses, or stores personal information in WI and is not authorized to acquire the personal information.

Definition of personally identifiable information:

"Personal information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: 1. The individual's social security number. 2. The individual's driver's license number or state identification number. 3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account. 4. The individual's deoxyribonucleic acid profile, as defined in s. 939.74(2d)(a). 5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information	Yes.	**Passports**	No.
Medical Information	No.	**Paper Records**	Yes.
De-identified information	No.	**Publicly available information**	No.
Encrypted Information*	No.		

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

"Entity" means a person, other than an individual, that does any of the following: a. Conducts business in this state and maintains personal information in the ordinary course of business. b. Licenses personal information in this state.c. Maintains for a resident of this state a depository account as defined in s. 815.18(2)(e). d. Lends money to a resident of this state. 2. "Entity" includes all of the following: a. The state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the constitution or any law, including the legislature and the courts. b. A city, village, town, or county.

Does the law cover:

Businesses and individuals?	Yes.	**State government agencies?**	Yes.	**Local government agencies?**	Yes.

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?
Immediately after the discovery of the breach.

Is there a "Risk of harm" trigger for notification?
Yes.

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?
Yes. A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required under sub. (2) for any period of time and the notification process required under sub. (2) shall begin at the end of that time period.

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?
Yes. Not to exceed 45 days after the entity learns of the acquisition of personal information.

Does the law specify how notification must be given?
Yes.

If yes, Does the law permit notification by:

Email:	Yes.	**Physical mail:**	Yes.	**Fax or "other":**	Yes.

Does the law specify what must be included in the notice, and if so, what must the notice include?
Yes. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.

Does the law require reporting to the Wisconsin Attorney General or separate government agency under certain conditions? No.

If Yes, Number of affected residents required for Agency Reporting:

If Yes, does the agency publish breach data?: Yes.

https://datcp.wi.gov/pages/programs_services/databreaches.aspx

Does the law require notifying consumer reporting agencies under certain conditions?
Yes.

If Yes, number of affected residents to trigger CRA notification: 1,000 or more individuals as the result of a single incident.

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.
Yes. *Exempt if in compliance with GLB or HHS Privacy Rule.*

If Yes, list the Federal laws that are referenced: *HHS Privacy Rule, GLB*

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:
No.

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?
No.

Enforcement damages and penalties:
No applicable provision.

Enforcing Agency:
Attorney General

Additional Exceptions:

Wyoming

Wyo. Stat. Ann. §§ 40-12-501—40-12-509.
https://wyoleg.gov/statutes/compress/title40.pdf

***Year most recently amended*:**

Scope:

Definition of breach:

Definition of personally identifiable information:

Does the definition of "Personally Identifiable Information" or "Breach" cover:

Biometric information		**Passports**	
Medical Information		**Paper Records**	
De-identified information		**Publicly available information**	
Encrypted Information*			

**** If encrypted information is covered, does it only cover encrypted information if the decryption key was or is likely to have been exposed?***

What entities are covered?

Does the law cover:

Businesses and individuals?		**State government agencies?**		**Local government agencies?**	

Notice Requirements:

Does the notification requirement trigger *immediately after discovery of the breach* or *after an investigation of some kind*?

Is there a "Risk of harm" trigger for notification?

Are there permitted delays for notification, and if so, under what conditions can a party delay notification?

Are there *time limits for notification* once it is required, and if so, how many days are permitted for notification?

Does the law specify how notification must be given?

If yes, Does the law permit notification by:

Email:		**Physical mail:**		**Fax or "other":**	

Does the law specify what must be included in the notice, and if so, what must the notice include?

Does the law require reporting to the Wyoming Attorney General or separate government agency under certain conditions?

If Yes, Number of affected residents required for Agency Reporting:

If Yes, does the agency publish breach data?:

Does the law require notifying consumer reporting agencies under certain conditions?

If Yes, number of affected residents to trigger CRA notification:

Does the law include an exception to the notification requirements if the entity *is complying with other laws (HIPPA, GLB, etc)*, and if so, notes on that exception.

If Yes, list the Federal laws that are referenced:

Does the law include an exception to the notification requirements if the *entity maintains their own notification procedures* which meet a certain threshold:

Enforcement

Does the law include a private right of action for individuals when the entity violates the notification requirements?

Enforcement damages and penalties:
AG may bring an action in law or equity to ensure compliance, to recover damages, or both.

Enforcing Agency:

Additional Exceptions: