Bloomberg Law | Privacy & Data Security

PRACTICAL GUIDANCE OVERVIEW: State Laws Requiring Data Security Practices

By Melissa Krasnow, Partner, VLP Law Group LLP, where she advises clients in the financial services, health and life sciences and technology areas on domestic and cross-border privacy, data security, big data, artificial intelligence and governance matters, technology transactions and mergers and acquisitions.

The information presented here is for general informational purposes only and should not be construed as specific legal advice. The information is also summary in nature.

INTRODUCTION

A number of states have laws requiring private sector businesses to implement data security practices when handling personal information (see Bloomberg Law Tracker), often specifying that businesses "implement and maintain reasonable security procedures and practices" (or similar language). Eleven of those states go a step further by requiring businesses to incorporate data security provisions into vendor agreements.

This overview provides a summary of these contract requirements, as well as the types of personal information covered by those 11 state laws. Because this overview does not cover all of the exceptions to these state security procedures laws, any state laws at issue should be reviewed regarding any exceptions.

ALABAMA

A. CONTRACT REQUIREMENTS

The Alabama security procedures law describes contract requirements generally, as an example of reasonable security measures. The Alabama security procedures law requires each covered entity (as defined in Section 2(2) of Ala. S.B. 318) and third-party agent (as defined in Section 2(7) of Ala. S.B. 318), subject to certain requirements, to implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security (as defined in Section 2(1) of Ala. S.B. 318). Section 3(a) of Ala. S.B. 318.

Reasonable security measures means security measures practicable for the covered entity to implement and maintain, including consideration of.... [r]etention of service providers, if any, that are contractually required to maintain appropriate safeguards for sensitive personally identifying information. Section 3(b)(4) of Ala. S.B. 318.

B. INFORMATION COVERED

The Alabama security procedures law covers and defines sensitive personally identifying information as an Alabama resident's first name or first initial and last name together with any of the following:

- a non-truncated social security number or tax identification number;
- 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 (as defined in Section 2(5) of Ala. S.B. 318);

- a financial account number, including a bank account number, credit card number, or debit card number, together 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;
- any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
- an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or
- a user name or email address, together with a password or security question and answer that would permit access to an online account affiliated with the covered entity (as defined in Section 2(2) of Ala. S.B. 318) that is reasonably likely to contain or is used to obtain sensitive personally identifying information. Section 2(6)(a) of Ala. S.B. 318.

Sensitive personally identifying information does not include either:

- information about an individual which has been lawfully made public by a federal, state, or local government record or a widely distributed media; or
- information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable, including encryption of the data, document, or device containing the sensitive personally identifying information, 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 or useable has been breached (as defined in Section 2(1) of Ala. S.B. 318) together with the information. Section 2(6)(b) of Ala. S.B. 318.

CALIFORNIA

A. CONTRACT REQUIREMENTS

The California security procedures law describes contract requirements and California guidance references a third party organization's controls regarding the California security procedures law. Also, the California Consumer Privacy Act of 2018 references the California security procedures law. A business that owns, licenses, or maintains (as defined in Cal. Civ. Code § 1798.81.5(a)(2)) personal information about a California resident must implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Cal. Civ. Code § 1798.81.5(b).

A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party that is not subject to Cal. Civ. Code § 1798.81.5(b) must require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Cal. Civ. Code § 1798.81.5(c).

The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet and the failure to implement all such controls that apply to an organization's environment constitutes a lack of reasonable security. California Data Breach Report 2012-2015, California Attorney General (February 2016).

An example of contract language for such business with respect to such nonaffiliated third party is as follows: nonaffiliated third party shall implement and maintain information security controls, as defined by the 20 controls in the Center for Internet Security's Critical Security Controls, that apply to such nonaffiliated third party and its environment.

California Consumer Privacy Act of 2018. The California Consumer Privacy Act of 2018 references the California security procedures law. Under the California Consumer Privacy Act of 2018, after satisfying certain procedural requirements, a consumer can bring a civil action in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater, among other things, regarding their nonencrypted or nonredacted personal information (as defined in the California security procedures law but excluding a username or email address together with a password or security question and answer that would permit access to an online account) that is subject to an unauthorized access and exfiltration, theft or disclosure as a result of a business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. Section 1798.150 of the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.150).

B. Information Covered

The California security procedures law covers and defines personal information as:

- an individual's first name or first initial and his or her last name together with any of the following data elements, when either the name or the data elements are not encrypted or redacted:
  - Social security number;
  - driver's license number or California identification card number;
  - account number, credit or debit card number, together with any required security code, access code, or password that would permit access to an individual's financial account;
  - medical information (as defined in Cal. Civ. Code § 1798.81.5(d)(2)); or
  - health insurance information (as defined in Cal. Civ. Code § 1798.81.5(d)(3) ; or
- a username or email address together with a password or security question and answer that would permit access to an online account. Cal. Civ. Code § 1798.81.5(d)(1).

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Cal. Civ. Code § 1798.81.5(d)(4).

COLORADO

A. Contract Requirements

The Colorado security procedures law references third-party service provider contracts and requirements: unless a covered entity (as defined in Colo. Rev. Stat. §6-1-713(2)) agrees to provide its own security protection, a covered entity must require that a third-party service provider (meaning an entity that has been contracted to maintain, store, or process personal identifying information on behalf of a covered entity) to which it discloses information to implement and maintain reasonable security procedures and practices that are:

- appropriate to the nature of the personal identifying information disclosed to the third-party service provider; and
- reasonably designed to help protect the personal identifying information from unauthorized access, use, modification, disclosure, or destruction. Colo. Rev. Stat. §6-1-713.5(2).

The Colorado security procedures law distinguishes that a disclosure of personal identifying information does not include disclosure of information to a third party under circumstances where the covered entity retains the primary responsibility for implementing and maintaining reasonable security procedures and practices appropriate to the nature of the personal identifying information and the covered entity implements and maintains technical controls that are reasonably designed to:

- help protect the personal identifying information from unauthorized access, use, modification, disclosure, or destruction; or
- effectively eliminate the third party's ability to access the personal identifying information, notwithstanding the third party's physical possession of the personal identifying information. Colo. Rev. Stat. §6-1-713.5(3).

A covered entity that maintains, owns, or licenses personal identifying information of an individual residing in Colorado must implement and maintain reasonable security procedures and practices appropriate to the nature of the personal identifying information and the nature and size of the business and its operations, to protect the personal identifying information from unauthorized access, use, modification, disclosure, or destruction. Colo. Rev. Stat. §6-1-713.5(1).

B. INFORMATION COVERED

The Colorado security procedures law covers and defines personal identifying information as:

- a social security number;
- a personal identification number;
- a password;
- a pass code;
- an official state or government-issued driver's license or identification card number;
- a government passport number;
- biometric data, as defined in Section 6-1-716(1)(a);
- an employer, student, or military identification number; or
- a financial transaction device, as defined in Colo. Rev. Stat. §18-5-701(3).

Colo. Rev. Stat. §6-1-713(2).

ILLINOIS

A. CONTRACT REQUIREMENTS

The Illinois security procedures law specifies contract requirements. A contract for the disclosure of personal information concerning an Illinois resident that is maintained by a data collector (as defined in 815 ILCS 530/5) must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. 815 ILCS 530/45(b).

A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident must implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. 815 ILCS 530/45(a).

B. INFORMATION COVERED

The Illinois security procedures law covers and defines personal information as:

- an individual's first name or first last name together with any of the following data elements, when either the name or the data elements are not 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 (as defined in 815 ILCS 530/5):
    - social security number;
    - driver's license number or State identification card number;
    - account number or credit or debit card number, or an account number or credit card number together with any required security code, access code, or password that would permit access to an individual's financial account;
    - medical information (as defined in 815 ILCS 530/5);
    - health insurance information (as defined in 815 ILCS 530/5); or
    - 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; or
- username or email address, together 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. 815 ILCS 530/5.

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

MARYLAND

A. CONTRACT REQUIREMENTS

The Maryland security procedures law specifies contract requirements. A business (as defined in Md. Code Ann., Com. Law § 14-3501(b)) that uses a nonaffiliated third party as a service provider to perform services for the business and discloses personal information about an individual residing in Maryland under a written contract with the third party must require by contract that the third party implement and maintain reasonable security procedures and practices that:

- are appropriate to the nature of the personal information disclosed to the nonaffiliated third party; and
- are reasonably designed to help protect the personal information from unauthorized access, use, modification, disclosure, or destruction. Md. Code Ann., Com. Law § 14-3503(b)(1).

The foregoing requirement applies to a written contract entered into on or after January 1, 2009. Md. Code Ann., Com. Law § 14-3503(b)(2).

A business that owns or licenses personal information of an individual residing in Maryland must implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations to protect personal information from unauthorized access, use, modification, or disclosure. Md. Code Ann., Com. Law § 14-3503(a).

B. INFORMATION COVERED

The Maryland security procedures law covers and defines personal information as:

- an individual's first name or first initial and last name together with any of the following data elements, when the name or the data elements are not encrypted (as defined in Md. Code Ann., Com. Law § 14-3501(c)), redacted, or otherwise protected by another method that renders the information unreadable or unusable:
    - a social security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government;
    - a driver's license number or State identification card number;
    - an account number, a credit card number, or a debit card number, together with any required security code, access code, or password, that permits access to an individual's financial account;
    - health information (as defined in Md. Code Ann., Com. Law § 14-3501(d), including information about an individual's mental health;
    - a health insurance policy or certificate number or health insurance subscriber identification number, together 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
    - 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
- a user name or e-mail address together with a password or security question and answer that permits access to an individual's e-mail account. Md. Code Ann., Com. Law § 14-3501(e)(1).

Personal information does not include:

- publicly available information that is lawfully made available to the general public from federal, State, or local government records;
- information that an individual has consented to have publicly disseminated or listed; or
- information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act. Md. Code Ann., Com. Law § 14-3501(e)(2).

MASSACHUSETTS

A. CONTRACT REQUIREMENTS

The Massachusetts security procedures law describes contract requirements as part of a written comprehensive information security program. The Massachusetts security procedures law requires every person (as defined in Mass. Regs. Code tit. 201, § 17.02) that owns or licenses (as defined in Mass. Regs. Code tit. 201, § 17.02) personal information about a Massachusetts resident to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

- the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;

- the amount of resources available to such person;
- the amount of stored data; and
- the need for security and confidentiality of both consumer and employee information. Mass. Regs. Code tit. 201, § 17.03(1).

Such safeguards contained must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated. Id.

Every comprehensive information security program must require oversight of service providers by:

- taking reasonable steps to select and retain third-party service providers (as defined in Mass. Regs. Code tit. 201, § 17.02) that are capable of maintaining appropriate security measures to protect such personal information consistent with Mass. Regs. Code tit. 201, § 17.00 et seq. and any applicable federal regulations; and
- requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information. Mass. Regs. Code tit. 201, § 17.03(2)(f).

An example of specific contract language for such person with respect to such third-party service provider is as follows: third-party service provider shall implement and maintain appropriate security measures to protect personal information consistent with Mass. Regs. Code tit. 201, § 17.00 et seq.: Standards for the Protection of Personal Information of Residents of the Commonwealth and all applicable federal laws, regulations and guidance. An example of broader contract language for such person with respect to such third-party service provider is as follows: third-party service provider shall comply with Mass. Regs. Code tit. 201, § 17.00 et seq.: Standards for the Protection of Personal Information of Residents of the Commonwealth and all applicable federal laws, regulations and guidance, including without limitation, implementing and maintaining appropriate security measures to protect personal information consistent with Mass. Regs. Code tit. 201, § 17.00 et seq.: Standards for the Protection of Personal Information of Residents of the Commonwealth and all applicable federal laws, regulations and guidance.

B. Information Covered

The Massachusetts security procedures law covers and defines personal information as a Massachusetts resident's first name and last name or first initial and last name together with any of the following data elements that relate to such resident:

- social security number;
- driver's license number or state-issued identification card number; or
- 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. Mass. Regs. Code tit. 201, § 17.02.

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

NEBRASKA

A. Contract requirements

The Nebraska security procedures law specifies contract requirements. An individual or commercial entity (as defined in Neb. Rev. Stat. § 87-802(2)) that discloses computerized data that includes personal information about a Nebraska resident to a nonaffiliated, third-party service provider must require by contract that the service provider implement and maintain reasonable security procedures and practices that:

- are appropriate to the nature of the personal information disclosed to the service provider; and
- are reasonably designed to help protect the personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure. Neb. Rev. Stat. § 87-808(2)(a).

The foregoing requirement applies to a contract renewed or entered into on or after July 19, 2018. Neb. Rev. Stat. § 87-808(2)(b).

An individual or a commercial entity that conducts business in Nebraska and owns, licenses, or maintains computerized data that includes personal information about a Nebraska resident must implement and maintain reasonable security procedures and practices that are appropriate to the nature and sensitivity of the personal information owned, licensed, or maintained and the nature and size of, and the resources available to, the business and its operations, including safeguards that protect the personal information when the individual or commercial entity disposes of the personal information, to protect personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure. Neb. Rev. Stat. § 87-808(1).

B. Information covered

The Nebraska security procedures law covers and defines personal information as:

- a Nebraska resident's first name or first initial and last name together with any of the following data elements that relate to the resident if either the name or the data elements are not encrypted (as defined in Neb. Rev. Stat. § 87-802(3)), redacted Neb. Rev. Stat. § 87-802(6)), or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:
    - Social security number;
    - motor vehicle operator's license number or state identification card number;
    - account number or credit or debit card number, together with any required security code, access code, or password that would permit access to a resident's financial account;
    - unique electronic identification number or routing code, together with any required security code, access code, or password; or
    - unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or
- a user name or email address, together with a password or security question and answer, that would permit access to an online account. Neb. Rev. Stat. § 87-802(5).

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

NEVADA

A. Contract requirements

The Nevada security procedures law specifies contract requirements. A contract for the disclosure of the personal information of a Nevada resident which is maintained by a data collector (as defined in Nev. Rev. Stat. § 603A.030) must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure. Nev. Rev. Stat. § 603A.210(2).

A data collector that maintains records which contain personal information of a Nevada resident must implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure. Nev. Rev. Stat. § 603A.210(1).

B. Information covered

The Nevada security procedures law covers and defines personal information as a natural person's first name or first initial and last name together with any of the following data elements, when the name and data elements are not encrypted:

- Social security number;
- driver's license number, driver authorization card number or identification card number;
- account number, credit card number or debit card number, together with any required security code, access code or password that would permit access to the person's financial account;
- a medical identification number or a health insurance identification number; or
- a user name, unique identifier or electronic mail address together with a password, access code or security question and answer that would permit access to an online account. Nev. Rev. Stat. § 603A.040(1).

Personal information 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. Nev. Rev. Stat. § 603A.040(2).

NEW MEXICO

A. Contract requirements

The New Mexico security procedures law specifies contract requirements. A person that discloses personal identifying information of a New Mexico resident pursuant to a contract with a service provider (as defined in N.M. Stat. § 57-12C-2(E)) must require by contract that the service provider implement and maintain reasonable security procedures and practices appropriate to the nature of the personal identifying information and to protect it from unauthorized access, destruction, use, modification or disclosure. N.M. Stat. § 57-12C-5.

A person that owns or licenses personal identifying information of a New Mexico resident must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure. N.M. Stat. § 57-12C-4.

B. INFORMATION COVERED

The New Mexico security procedures law covers and defines personal identifying information as an individual's first name or first initial and last name together with any of the following data elements that relate to the individual, when the data elements are not protected through encryption (as defined in N.M. Stat. § 57-12C-2(B)) or redaction or otherwise rendered unreadable or unusable:

- social security number;
- driver's license number;
- government-issued identification number;
- account number, credit card number or debit card number together with any required security code, access code or password that would permit access to a person's financial account; or
- biometric data (as defined in N.M. Stat. § 57-12C-2(A)). N.M. Stat. § 57-12C-2(C)(1).

Personal identifying information does not mean information that is lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public. N.M. Stat. § 57-12C-2(C)(2).

OREGON

A. CONTRACT REQUIREMENTS

The Oregon security procedures law describes contract requirements generally, as part of an information security program. Under the Oregon security procedures law, a person (as defined in Or. Rev. Stat. § 646A.602(10)) that owns, maintains or otherwise possesses, or has control over or access to, data that includes personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the personal information. Or. Rev. Stat. § 646A.622(1).

A person complies with Or. Rev. Stat. § 646A.622(1) if the person.... [i]mplements an information security program that includes….[a]dministrative safeguards such as:.... [s]electing service providers that are capable of maintaining appropriate safeguards and practices, and requiring the service providers by contract to maintain the safeguards and practices.... Or. Rev. Stat. § 646A.622(2)(d)(A)(v).

B. INFORMATION COVERED

The Oregon security procedures law covers and defines personal information as a consumer's (as defined in Or. Rev. Stat. § 646A.602(2)) first name or first initial and last name together with any of the following data elements, if encryption (as defined in ORS § 646A.602(6)), redaction (as defined in Or. Rev. Stat. § 646A.602(15)) or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired:

- a consumer's social security number;
- a consumer's driver license number or state identification card number issued by the Department of Transportation;
- a consumer's passport number or other identification number issued by the United States;
- a consumer's financial account number, credit card number or debit card number, together 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 (as defined in Or. Rev. Stat. § 646A.602(10)) reasonably knows or should know would permit access to the consumer's financial account;

- 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;
- a consumer's health insurance policy number or health insurance subscriber identification number together with any other unique identifier that a health insurer uses to identify the consumer; and
- 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. Rev. Stat. § 646A.602(11)(a)(A).

Personal information also includes any of the data elements or any combination of the data elements described in Or. Rev. Stat. § 646A.602(11)(a)(A) without the consumer's first name or first initial and last name if:

- encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and
- the data element or combination of data elements would enable a person to commit identity theft against a consumer. Or. Rev. Stat. § 646A.602(11)(a)(B).

Personal information does not include information in a federal, state or local government record, other than a social security number, that is lawfully made available to the public. Or. Rev. Stat. § 646A.602(11)(b).

RHODE ISLAND

A. CONTRACT REQUIREMENTS

The Rhode Island security procedures law specifies contract requirements. A municipal agency, state agency, or person (as defined in R.I. Gen. Laws § 11-49.3-3(a)(7)) who or that discloses personal information about a Rhode Island resident to a nonaffiliated third party must require by written contract that the third party implement and maintain reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure. R.I. Gen. Laws § 11-49.3-2(b). The foregoing requirement applies to contracts entered into after June 26, 2016. Id.

A municipal agency, state agency, or person who or that stores, collects, processes, maintains, acquires, uses, owns, or licenses personal information about a Rhode Island resident must implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of such information. R.I. Gen. Laws § 11-49.3-2(a).

B. INFORMATION COVERED

The Rhode Island security procedures law covers and defines personal information as an individual's first name or first initial and last name together with any of the following data elements, when the name and the data elements are not encrypted (as defined in R.I. Gen. Laws § 11-49.3-3(a)(2)) or are in hard copy, paper format:

- social security number;
- driver's license number, Rhode Island identification card number, or tribal identification number;
- account number, credit, or debit card number, together with any required security code, access code, password, or personal identification number, that would permit access to an individual's financial account;
- medical or health insurance information (as defined in R.I. Gen. Laws § 11-49.3-3(a)(4) or R.I. Gen. Laws § 11-49.3-3(a)(3)); or
- 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. R.I. Gen. Laws § 11-49.3-3(a)(8).

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. R.I. Gen. Laws § 11-49.3-3(b).