LIABILITY AND CYBER SECURITY ISSUES FOR EMERGENCY COMMUNICATIONS AND RESPONSE

iCERT
Industry Council for Emergency Response Technologies

FOREWORD

This report on matters of liability and cyber security in emergency response technologies is brought to you by iCERT, in collaboration with our Outside General Counsel from the law firm of Shulman Rogers, and in cooperation with the University of Houston's Department of Computer Science, with support from the U.S. Department of Homeland Security, Cyber Security Division. It is published to provide iCERT's member companies and other stakeholders with pertinent and timely information on issues of general accountability and cyber assurances for commercial enterprises as they look to provide emergency communications services to public agencies.

This report covers issues under such topic areas as: technology failures and how a company can be held liable if 911 communications fail; cyber security liability concerns for emergency call centers and their service providers; and, utilization of 911 funds and how states are spending fees collected from consumers for 911 services.

To address these critical issues, this publication draws on legal and regulatory issues associated with emergency response technologies; and relevant rulings, court decisions and burgeoning practices of the agencies, legislatures and regulating bodies with authority over these public safety services. While the understandings provided in this report should not be construed as client-based legal advice, they will offer industry stakeholders a level of insight into important guiding and undergirding matters that affect our industry, as well as the nature of a company's engagement as a service provider to public safety agencies.

We trust that you will find value in the pages that follow.

George Rice
Executive Director
iCERT

911 Call Center Liabilities and Protections Arising from Technical Failures and Cyber-attacks

In recent years, 911 call centers have become more frequent targets of cyber-attacks and ransomware incursions. These assaults on the nation's emergency calling and response systems have the potential to cause widespread harm if not managed proactively and with a keen focus on continual prevention.

SecuLore Solutions, an iCERT member company, tracks cyber-attacks on public safety infrastructure and has identified in a little more than a year 184 publicized incidents impacting America's state/county/city networks that either impaired or had the potential to impair public safety response. Of this list, 33 were identified as directly impacting 911 systems in a broad range of states, including Arkansas, California, District of Columbia, Florida, Illinois, Maryland, North Carolina, Ohio, Tennessee, Texas and Virginia. A more recent attack was on March 24 of this year in Baltimore, Maryland.

As the March 24 ransomware attack against Baltimore's 911 system shows, hackers are increasingly targeting public safety services in the hopes that their importance to the community will increase the chances of a payout. In the Baltimore attack, the hackers appear to have been continuously monitoring and probing the 911 systems. When a technician inadvertently changed and left open a security setting, the attackers quickly detected the vulnerability, accessed the systems and shut down the automated call dispatching function.[1] Since human error will always be a risk, these systems should be routinely backed up and tested for recovery.

This article discusses a few specific circumstances in which 911 call centers may become liable from technical failures or cyber-attacks as well as protections against such liabilities.

Similarly, there are many ways in which liability can arise and be protected against in our modern world. This article discusses a few specific circumstances in which 911 call centers may become liable from technical failures or cyber-attacks, as well as protections against such liabilities. Potential liabilities from technical failures and protections are discussed first with an emphasis on the SAFETY Act and the Public Duty Doctrine. Potential liabilities from cyber-attacks and protections are then discussed with an emphasis on the Cybersecurity Information Sharing Act, notice requirements and insurance.

TECHNOLOGY FAILURES

A. FEDERAL LAW: SAFETY ACT

Following the attacks of September 11, 2001, Congress passed the Homeland Security Act of 2002, containing an oft-overlooked provision known as the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act).[2] "The purpose of the SAFETY Act was to encourage the development and deployment of anti-terrorism products and services by granting various risk management protections."[3] "Through a process of designation and certification by the Department of Homeland Security (DHS), the act provides liability protection to technologies and services that might go undeveloped or whose development may be delayed because of the seller's inability to obtain liability insurance to insure against losses to sellers of such technologies and services."[4]

"The purpose of the SAFETY Act was to encourage the development and deployment of anti-terrorism products and services by granting various risk management protections."

The SAFETY Act created two levels of liability protections for claims arising from injury, loss of life, or damage to property or business resulting from an act of terrorism where Qualified Anti-Terrorism Technologies (QATTs) have been deployed in defense against, response to or recovery from such an act.[5]

The first level of protection referred to as "Designation" caps a Sellers'[6] liability for "Designated Technologies" at an amount determined by the U.S. Department of Homeland Security. In addition to limiting liability, Designation also provides:

1) Exclusive jurisdiction in federal court for suits against sellers of a technology arising from acts of terrorism; a bar against punitive damages and prejudgment interest;
2) A limitation on non-economic damages; and
3) Liability only in proportion to the responsibility of the seller.[7]

The SAFETY Act sets the following criteria for Designation:

1) Prior United States Government use or demonstrated substantial utility and effectiveness.
2) Availability of the technology for immediate deployment in public and private settings.
3) Existence of extraordinarily large or unquantifiable potential third-party liability risk exposure to the Seller or other provider of the technology.
4) Substantial likelihood that the technology will not be deployed unless SAFETY Act risk management protections are extended.
5) Magnitude of risk exposure to the public if the technology is not deployed.
6) Evaluation of scientific studies that can be feasibly conducted to assess the capability of the technology to substantially reduce risks of harm.
7) Effectiveness of the technology in facilitating the defense against acts of terrorism.[8]

The second level of protection, referred to as Certification, encompasses all of the benefits of Designation, as well as potential immunity[9] from liability by way of the Government Contractor Defense.[10] Certification is awarded upon a showing that a QATT:

1) Performs as intended.
2) Conforms to the Seller's specifications.
3) Is safe for use as intended.

Outside the context of an actual terror attack, obtaining Designation and/or Certification pursuant to the SAFETY Act may serve as a stamp of approval from the federal government as to the effectiveness of the service provided, and may potentially serve as "significant evidence of commercial reasonableness in legal proceedings not associated with an act of terrorism."[11] For further information about obtaining Designation or Certification, consult an attorney.

B. STATE LAW

1. Statutory Protections

Most, although not all, states and U.S. territories have statutory provisions providing liability and immunity for call center providers of telecommunications. While a limited number of states provide absolute immunity, most carve out exceptions. Depending on the jurisdiction, immunity is unavailable under one or a combination of the following circumstances: willful or wanton misconduct, gross negligence, intentional misconduct and/or failure to use ordinary care. For a complete list of the each state's available statutory liabilities and protections, see **Appendix A (pg. 13, State Liabilities and Protections)**.

2. Public Duty Doctrine

A related protection is recognized in many jurisdictions as the Public Duty Doctrine. This arises from the principal that the government owes a duty to the public at large rather than any specific individual. Therefore, the government (and those acting on behalf of the government) cannot be held liable for injuries to any one specific individual. The following states recognize the Public Duty Doctrine in its entirety: Alabama, Arizona, California, Connecticut, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Maine, Maryland, Minnesota, Mississippi, Montana, Nevada, New Hampshire, New York, North Carolina, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Virginia, Washington, West Virginia, District of Columbia, Guam and the U.S. Virgin Islands. Some states have modified the Doctrine, including Georgia (the public duty doctrine does not apply outside of police protection services), Michigan (gross negligence can overcome public duty doctrine), Missouri (the doctrine will not apply where defendant public employees act in bad faith or with malice), New Jersey (applicable aspect of Doctrine appears in 911 immunity statute, which provides same protections as public duty doctrine), Ohio (doctrine does not apply to situations involving wanton or reckless conduct) and Utah (does not apply to affirmative acts that harm plaintiff). On the other hand, the following jurisdictions do not recognize the Public Duty Doctrine: Alaska, Colorado, Illinois, Louisiana, Massachusetts, Nebraska, New Mexico, North Dakota, Oregon, Vermont, Wisconsin and Wyoming. For a complete list of how each state has addressed the Public Duty Doctrine, see **Appendix B (pg. 39, State Public Duty Doctrines)**.

For example, the Supreme Court of Illinois recently abolished the Public Duty Doctrine in Coleman v. East Joliet Fire Protection District.[12] In this case, a 58-year-old woman called 911 because she was having difficulty breathing. EMS responders did not reach the woman until 41 minutes after her 911 call due to several mistakes made by the dispatchers. She was found unresponsive and pronounced dead at the hospital. The Supreme Court based its ruling on a determination that "the public policy behind the judicially created public duty rule and its special duty exception have largely been supplanted by the legislature's enactment of statutory immunities, rendering the public duty rule and its special duty exception obsolete."[13] The Court went on to state that, "the underlying purposes of the public duty rule are better served by application of conventional tort principles and the immunity protection afforded by statutes than by a rule that precludes a finding of a duty on the basis of the defendant's status as a public entity." [14]

The Supreme Court based its ruling on a determination that "the public policy behind the judicially created public duty rule and its special duty exception have largely been supplanted by the legislature's enactment of statutory immunities, rendering the public duty rule and its special duty exception obsolete."

3. Case Examples

Cook v. City of Dallas

Plaintiffs filed suit against T-Mobile, MetroPCS, Samsung Electronics Co. and Samsung Telecommunications America in the U. S. District Court for the Northern District of Texas seeking to hold the telecommunications companies liable owing to their supposed failure to provide tracking technology that would have more quickly enabled the location of a woman who was murdered while on the phone with 911. On appeal, the U. S. Court of Appeals for the Fifth Circuit ruled[15] that any defect in the phone or providers' services were not the proximate cause of death and therefore, the telecommunications defendants were entitled to immunity under Texas law. However, the Court held that plaintiffs could have overcome the immunity if they demonstrated that the telecommunications companies' acts or omissions (1) proximately caused their injuries and (2) the acts or omissions constituted gross negligence, recklessness or intentional misconduct.

Alex v. T-Mobile

In a case currently pending in the U. S. District Court for the Northern District of Texas (3:12-cv-1532), two parents have filed suit against T-Mobile and MetroPCS arising out of the death of their six-month-old child. The child's babysitter made several unsuccessful attempts[16] to reach 911 using a cell phone after the baby had difficulty breathing after rolling off a bed. The babysitter was unable to reach Dallas emergency dispatch due to it being clogged with "ghost calls."[17] Ultimately, the mother returned home in response to the babysitter's call for help. However, by the time the baby finally reached the emergency room, he was pronounced dead. Causes of action brought by parents include among others: strict liability, negligence and gross negligence, breach of express and implied warranties, Deceptive Trade Practices Act violations and misrepresentation. Taking heed of the Court's ruling in Cook, the plaintiffs have attempted to overcome the statutory immunity by alleging that: 1) the defendants' actions proximately caused the death;[18] and 2) the acts were grossly negligent or reckless.

Wendell v. Verizon

In litigation in the U. S. District Court for the Southern District of Mississippi,[19] plaintiffs sued Verizon claiming their 911 calls did not go through when they, along with their child, were held hostage. Their 911 calls failed to connect with the correct Public Safety Answering Point (PSAP) because, although the call was made in Vicksburg-Warren County, Mississippi, they were rerouted to Tallulah, Louisiana. The Court ordered that the case remain in private arbitration in accordance with the parties' agreement in the contract. The case ultimately settled in arbitration for an unknown amount.

Consult with an attorney for information regarding liabilities form and protections for technology failures.

A. FEDERAL LAW: CYBERSECURITY INFORMATION SHARING ACT

Sharing information about cyber-attacks can be vital to ensuring a quick response. However, many companies hesitate or refuse to share information due to concerns of invading their customers' privacy and/or facing civil liability if that privacy is breached. To address these concerns and encourage companies to share information in an effort to combat cyber-attacks, on December 18, 2015,[20] President Obama signed into law the Cybersecurity Act of 2015, Title I of which is entitled the Cybersecurity Information Sharing Act, or CISA. CISA was designed to establish a voluntary cybersecurity information sharing process that encourages public and private sector entities to share cyber-threat indicators and defensive measures while protecting privacy and civil liberties.[21] Accordingly, CISA provides that, "notwithstanding any other provision of law, a non-federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-federal entity or the Federal Government a cyber-threat indicator or defensive measure."[22] CISA further provides protection from liability against any private entity for the sharing or receipt of a cyber-threat indicator or defensive measure provided the information is shared or received in accordance with the provisions of the Act.

For example, CISA requires that, prior to sharing a cyber-threat indicator under the auspices of the Act, a non-Federal entity must:

> Review such cyber-threat indicator to assess whether such cyber-threat indicator contains any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or
>
> Implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.[23]

CISA further provides protection from liability against any private entity for the sharing or receipt of a cyber-threat indicator or defensive measure provided the information is shared or received in accordance with the provisions of the Act.

Because the dictates of the Act are optional, it also exempts entities from liability "for choosing not to engage in the voluntary activities" authorized by the Act.[24]

As required by the Act, within 180 days of enactment, DOJ and DHS issued guidelines for sharing information with the federal government. These guidelines consisted of four documents: 1) the Operational Procedures; 2) the Non-Federal Entity Sharing Guidance;[25] 3) the Federal Entity Sharing Guidance; and 4) the Privacy and Civil Liberties Guidelines. The Non-Federal Entity Sharing Guidance contains the following:

1) Distinctions between the types of information that qualify as a cyber-threat under the Act and the types of information protected by otherwise applicable privacy laws;
2) Examples of information that would contain cyber-threat indicators that a private entity could share with the federal government;
3) Examples of defensive measures that a private entity could share under CISA;
4) Examples of how private entities must share cyber-threat indicators and defensive measures with the federal government to take advantage of the liability protection made available by the statute.[26]

For additional information regarding compliance with the Act and the protections afforded therein, consult with an attorney.

B. STATE LAW: NOTICE REQUIREMENT

Forty-eight states[27], the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information[28] involving personal identifiable information. Security breach laws typically have provisions regarding who must comply with the law, definitions of "personal information," what constitutes a breach, and requirements for notice and exemptions.[29] For a summary of state notice requirements, see **Appendix C (pg. 44, Summaries of State Notice Statutes)**.

Personal identifiable information is generally defined as an individual's first name or first initial and last name plus one or more of the following: (i) Social Security number; (ii) driver's license number or state-issued ID card number; (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information. Personal information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media. The majority of states have adopted a broader definition of personal information. Additionally, a breach of security is generally recognized as the unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality or integrity of personal information.

Most states follow the basic tenet that companies must immediately disclose a data breach to customers, usually in writing. The specifics vary from state to state in some of the following areas:

1) Notification guidelines—how soon notification is required
2) Penalty for failure to disclose—availability of civil or criminal penalties
3) Private right of action—the existence (or lack thereof) for consumers
4) Exemptions—what types of breaches are exempted from reporting[30]

For the operative sections of the notice requirement statutes enacted by the states and territories, see **Appendix D (pg. 48, State Notice Statutes).**

With cyber-attacks and security breaches becoming increasingly prevalent, more and more businesses are considering cyberinsurance coverage to protect against eventualities insufficiently covered, if at all, by general insurance policies.

C. CYBER INSURANCE

With cyber-attacks and security breaches becoming increasingly prevalent, more and more businesses are considering cyberinsurance coverage to protect against eventualities insufficiently covered, if at all, by general insurance policies. Cyberinsurance addresses a variety of liabilities, including those associated with first-party costs (i.e. notification of clients of a breach or remedying electronic damage) as well as third-party costs like lawsuits or other claims against the insured. Cyberinsurance policies vary not only by insurer but also based on the type of business being insured.

The cost of cyberinsurance varies depending on what is covered, exclusions and other factors described here and ranges from tens of dollars per person to tens of thousands of dollars for organizations. Although the cost of this kind of insurance may make sense when compared to the liabilities that result from breach, cyberinsurance is still not a substitute for good computer and network security practices. It merits mention that failing to meet certain minimum-security practices in place may preclude an entity from obtaining coverage.

[1]Kevin Rector, *Baltimore 911 dispatch system hacked, investigation underway, officials confirm*, The Baltimore Sun, (March 27, 2018), available at http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-911-hacked-20180327-story.html.

[2]Codified at 6 U.S.C. §§ 441-444.

[3]Dismas N. Locaria, Brian M. Zimmet and Jason R. Wool, *The SAFETY Act: Providing Critical Liability Protections for Cyber and Physical Security Efforts*, Venable LLP on Cybersecurity Law (April 2014), available at https://www.venable.com/files/Publication/6c0b031e-c2c5-4029-9ac7-13cb1d8c0d07/Presentation/PublicationAttachment/e81d24a3-fc57-4ece-8e1f-179418baf994/The_SAFETY_Act_Providing_Critical_Liability_Protections_for_Cyber_and_Physical_Securi.pdf

[4]Carlene V. McIntyre and Faith Tabafunda, *An Overview of the SAFETY Act—Liability Protection for Anti-Terrorism Technologies*, 20-SUM AIR & SPACE LAW 1 (Summer 2005).

[5]Locaria, et al. supra note 2; DHS Science and Technology Directorate, *Research and Development Partnerships – SAFETY Act for Liability Protection*, available at https://www.dhs.gov/sites/default/files/publications/Safety%20Act%20for%20Liability%20Protection_0.pdf

[6]"Parties covered under the SAFETY Act are referred to as 'Sellers' and can include any person, firm, or other entity that provides a QATT to customer(s) and to whom a Designation has been issued.

[7]Locaria, et al. *supra* note 2.

[8]6 U.S.C. § 441.

[9]The rebuttal presumption that the government contractor defense applies "shall only be overcome by clear and convincing evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Department during the course of the consideration of such Technology under this section." 6 C.F.R. § 25.8.

[10]The Government Contract Defense finds its origins in the U.S. Supreme Court case *Boyle v. United Technologies Corp.*, 487 U.S. 500 (1988). In *Boyle*, the Supreme Court concluded that where a government contractor manufacturers a product in accordance with government specifications, it is shielded from liability arising from the use of said product. However, it bears mention that "DHS limits the defense to that which existed on the day of the SAFETY Act's enactment (November 25, 2002), meaning that future judicial developments in the government contractor defense would not apply." Locaria, et al. *supra* note 2.

[11]Locaria¸ et al. *supra* note 2.

[12]46 N.E.3d 741 (Ill. 2016)

[13]*Id.* at 757

[14]*Id.* at 757-58.

[15]*Cook v. City of Dallas*, No. 16-10105, 2017 WL 1191573 (5th Cir. Mar. 29, 2017).

[16]According to the Complaint, the babysitter placed three 911 calls from the cell phone being placed on hold for 55 seconds, 8 minutes and 40 seconds and 31 minutes and 35 seconds respectively.

[17]From the Complaint: "T-Mobile's 911 service and technology caused calls to be, phantomlike, placed on hold, resulting in hundreds of unanswered calls."

[18]In *Cook*, the caller was murdered by a third party, whereas in *Alex*, the allegation is that the baby died as a direct result of the failure to receive medical attention promptly following an accident.

[19]*Wendell et al. v. Verizon Communications, Inc., et al.*, No. 5:16-cv-00050-DCB-MTP.

[20]6 U.S.C. §1501 – 1510.

[21]81 FR 39061.

[22]6 U.S.C. § 1501(c)(1).

[23]6 U.S.C. § 1503(d)(2).

[24]6 U.S.C. § 1507(i).

[25]U.S. DEPT OF HOMELAND SEC. & U.S. DEPT OF JUSTICE, GUIDANCE TO ASSIST NON-FEDERAL ENTITIES TO SHARE CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH FEDERAL ENTITIES UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015, https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_(Sec%20105(a)).pdf

[26]Ari Schwartz, et al., *Automating Threat Sharing: How Companies Can Best Ensure Liability Protection When Sharing Cyber Threat Information with Other Companies or Organizations*, 50 U. Mich. J.L. Reform 887, 909 (2017).

[27]Alabama and South Dakota do not have laws requiring consumer notification of security breaches involving personal information.

[28]http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[29]Id.

[30]https://www.csoonline.com/article/2122493/compliance/cso-disclosure-series---data-breach-notification-laws--state-by-state.html

SHULMAN ROGERS | GANDAL PORDY ECKER

By the Shulman Rogers law firm's Cyber Security and Emergency Response Group with primary contact Mark Maier, MMaier@ShulmanRogers.Com, 301-231-0945.

iCERT Industry Council for Emergency Response Technologies

Appendix A
State Liabilities and Protections

State	Statute	Key provisions and protections	Liability
Alabama	Ala. Code 1975 § 11-98-9 § 11-98-9. Technical proprietary information.	Notwithstanding any other provision of the law, no district, political subdivision, voice communication provider, or its employees, directors, officers, or agents shall be liable for any damages in a civil action or subject to criminal prosecution resulting from death, injury, or loss to persons or property incurred by any person in connection with establishing, developing, implementing, maintaining, operating, and otherwise providing 911 service in compliance with the requirements established by the FCC or other state or federal requirement, except in the case of willful or wanton misconduct.	Willful & Wanton
Alaska	AS § 29.35.133 Immunity for 911 systems	(a) . . . "except for intentional acts of misconduct or gross negligence, a service supplier, local exchange telephone company, or wireless telephone company and their employees and agents are also immune from tort liability that might otherwise be incurred in the course of installing, training, maintaining, or providing enhanced 911 systems or transmitting or receiving calls on the system. (b) An individual, telephone company, or employee of a telephone company who operates or maintains an emergency 911 service is not liable for civil damages in a tort action as a result of an act, omission, failure of service, or incorrect information done or given in good faith."	Intentional; Gross Negligence

Arizona	ARS § 12-713. Providers of emergency services; civil liability	In the provision of 911 services, a person, a provider as defined in § 42-5251 or a public entity or any employee of the public entity is not liable for damages in any civil action for injuries, death or loss to a person or property that are incurred by any person with respect to all decisions made and actions or omissions taken that are based on good faith implementation except in the cases of wanton or wilful misconduct, regardless of technology platform including a public safety radio communications network, that receives, develops, collects or processes information for the service's location information databases, relays, transfers, operates, maintains or provides emergency notification services or system capabilities, or provides emergency communications or services for ambulances, police and fire departments or other public safety entities.	Willful & Wanton
Arkansas	§ 12-10-318. Emergency telephone service charges--Imposition--Special election--Liability	(d)(1) Notwithstanding any other provision of the law, in no event shall any commercial mobile radio, voice over internet protocol service, or nontraditional service provider, or its officers, employees, assigns, or agents be liable for civil damages or criminal liability in connection with the development, design, installation, operation, maintenance, performance, or provision of 911 service. (2) Nor shall any commercial mobile radio, voice over internet protocol, or nontraditional service provider, its officers, employees, assigns, or agents be liable for civil damages or be criminally liable in connection with the release of subscriber information to any governmental entity as required under the provisions of this subchapter.	Not Liable

California	CA HLTH & S § 1799.107	(a) .... a qualified immunity from liability shall be provided for public entities and emergency rescue personnel providing emergency services. (b) Except as provided in Article 1 (commencing with Section 17000) of Chapter 1 of Division 9 of the Vehicle Code, neither a public entity nor emergency rescue personnel shall be liable for any injury caused by an action taken by the emergency rescue personnel acting within the scope of their employment to provide emergency services, unless the action taken was performed in bad faith or in a grossly negligent manner. (c) For purposes of this section, it shall be presumed that the action taken when providing emergency services was performed in good faith and without gross negligence. This presumption shall be one affecting the burden of proof. (d) For purposes of this section, "emergency rescue personnel" means any person who is an officer, employee, or member of a fire department or fire protection or firefighting agency of the federal government, the State of California, a city, county, city and county, district, or other public or municipal corporation or political subdivision of this state, or of a private fire department, whether that person is a volunteer or partly paid or fully paid, while he or she is actually engaged in providing emergency services as defined by subdivision (e). (e) For purposes of this section, "emergency services" includes, but is not limited to, first aid and medical services, rescue procedures and transportation, or other related activities necessary to insure the health or safety of a person in imminent peril.	Bad Faith; Gross Negligence

Colorado	C.R.S.A. § 29-11-105. Immunity of providers	"....In addition, no basic emergency service provider or service supplier or any employee or agent thereof shall be liable for any damages in a civil action for injuries, death, or loss to person or property incurred as a result of any act or omission of such provider, service supplier, employee, or agent in connection with developing, adopting, implementing, maintaining, enhancing, or operating an emergency telephone service unless such damage or injury was intentionally caused by or resulted from gross negligence of the provider, supplier, employee, or agent."	Intentional; Gross Negligence
Connecticut	C.G.S.A. § 28-28a, § 28-28a. Provision of subscriber information: Permitted purposes; confidentiality; agreement. Immunity from liability	(d) No telephone company, certified telecommunications provider, provider of wireless telecommunications service, as defined in section 28-30b, pursuant to a license issued by the Federal Communications Commission, provider of prepaid wireless telecommunications service, voice over Internet protocol service provider or the officers, directors, employees, vendors or agents of any such company or provider shall be liable to any person or entity for release of the information specified in this section or for any failure of equipment or procedure in connection with the enhanced 9-1-1 service, an emergency notification system, or the next generation 9-1-1 telecommunication system established under sections 28-25 to 28-29b, inclusive.	Not Liable

Delaware	16 Del. C. § 10008 Limitation of Liability	No person involved in the provision of E-911 or 911 service who in good faith receives, develops, collects or processes information for the enhanced 911 data bases, relays, transfers, operates, maintains or provides enhanced 911 services or system capabilities, or provides emergency telephone and radio communications for ambulance, police and fire departments, shall be liable for damages in any civil action for any act or omission that results in death, injury or loss to person or property unless such action or inaction constitutes gross negligence or an intentional tort. This section shall be construed to include 911 service that utilizes in whole or in part Internet Protocol or other next generation 911 technologies.	intentional; Gross Negligence
D.C.	N/A	N/A	N/A
Florida	Title XXVII, § 365.172(12) Emergency communications number "E911"	[A] local exchange carrier, voice communications services provider, or other service provider that provides 911 or E911 service on a retail or wholesale basis is not liable for damages resulting from or in connection with 911 or E911 service, or for identification of the telephone number, or address, or name associated with any person accessing 911 or E911 service, unless the carrier or provider acted with malicious purpose or in a manner exhibiting wanton and willful disregard of the rights, safety, or property of a person when providing such services. A carrier or provider is not liable for damages to any person resulting from or in connection with the carrier's or provider's provision of any lawful assistance to any investigative or law enforcement officer of the United States, this state, or a political subdivision	Willful & Wanton

		thereof, or of any other state or political subdivision thereof, in connection with any lawful investigation or other law enforcement activity by such law enforcement officer.	
Georgia	Ga. Code Ann., § 46-5-131. Civil Liability	(a) Whether participating in a state-wide emergency 9-1-1 system or an emergency 9-1-1 system serving one or more local governments, neither the state nor any local government of the state nor any emergency 9-1-1 system provider or service supplier or its employees, directors, officers, and agents, except in cases of wanton and willful misconduct or bad faith, shall be liable for death or injury to any person or for damage to property as a result of either developing, adopting, establishing, participating in, implementing, maintaining, or carrying out duties involved in operating the emergency 9-1-1 system or in the identification of the telephone number, address, or name associated with any person accessing an emergency 9-1-1 system.	Willful & Wanton
Guam	N/A	N/A	N/A

Hawaii	HRS § 138-9. Limitation of liability	(a) Notwithstanding any law to the contrary, in no event shall any communications service provider, reseller, independent, third-party accounting firms, consultants, or other third party retained by the State under section 138-2, or their respective employees, directors, officers, assigns, affiliates, or agents, except in cases of gross negligence or wanton and wilful misconduct, be liable for any civil damages or criminal liability resulting from death or injury to a person or from damage to property incurred by any person in connection with any act or omission in developing, designing, adopting, establishing, installing, participating in, implementing, maintaining, or providing access to enhanced 911 or any other communications service intended to help persons obtain emergency assistance. In addition, no communications service provider, reseller, independent, third-party accounting firms, consultants, or other third party retained by the State under section 138-2, or their respective employees, directors, officers, assigns, affiliates, or agents shall be liable for civil damages or criminal liability in connection with the release of customer information to any governmental entity, including any public safety answering point, as required under this chapter. (b) In no event shall any public safety answering point, or its employees, assigns, or agents, or emergency response personnel, except in cases of gross negligence or wanton and wilful misconduct, be liable for any civil damages or criminal liability resulting from death or injury to the person or from damage to property incurred by any person in connection with any act or omission in the development, installation,	Gross Negligence; Willful & Wanton

		maintenance, operation, or provision of enhanced 911 service.	
Idaho	I.C. § 31-4812. Immunity and conditions of liability in providing emergency communications service	(2) A telecommunications provider making available emergency communications systems or services, and its employees and agents, shall not be liable in tort to any person for damages alleged to have been caused by the design, development, installation, maintenance or provision of consolidated emergency communications systems or services, unless such entities or persons act with malice or criminal intent, or commit reckless, willful and wanton conduct.	Willful & Wanton
Illinois	50 ILCS 750/15.1; § 15.1. Public body; exemption from civil liability for developing or operating emergency telephone system.	(a) In no event shall a public agency, the Commission, the Statewide 9-1-1 Advisory Board, the Administrator, the Department of State Police, public safety agency, public safety answering point, emergency telephone system board, or unit of local government assuming the duties of an emergency telephone system board, or carrier, or its officers, employees, assigns, or agents be liable for any civil damages or criminal liability that directly or indirectly results from, or is caused by, any act or omission in the development, design, installation, operation, maintenance, performance, or provision of 9-1-1 service required by this Act, unless the act or omission constitutes gross negligence, recklessness, or intentional misconduct.	Gross Negligence; Reckless; Intentional

Indiana	IC 36-8-16.7-43 Immunity	Sec. 43. Notwithstanding any other law: (1) the board; (2) a PSAP; (3) a political subdivision; (4) a provider; (5) an employee, director, officer, or agent of a PSAP, a political subdivision, or a provider; or (6) an employee or member of the board, the board chair, the executive director, or an employee, agent, or representative of the board chair;is not liable for damages in a civil action or subject to criminal prosecution resulting from death, injury, or loss to persons or property incurred by any person in connection with establishing, developing, implementing, maintaining, operating, and providing 911 service, except in the case of willful or wanton misconduct.	Willful & Wanton
Iowa	I.C.A. § 670.4 Claims exempted	1. The liability imposed by section 670.2 shall have no application to any claim enumerated in this section. As to any such claim, a municipality shall be liable only to the extent liability may be imposed by the express statute dealing with such claims and, in the absence of such express statute, the municipality shall be immune from liability. k. A claim based upon or arising out of an act or omission in connection with an emergency response including but not limited to acts or omissions in connection with emergency response communications services.	Not Liable
Kansas	K.S.A. 12-5376. Limitation on liability	(a) Except as provided by the Kansas tort claims act, and except for failure to use ordinary care, or for intentional acts, the LCPA and each provider, and their employees and agents, and each seller, and their employees and agents, shall not be liable for the payment of damages resulting directly or indirectly from the total or partial failure of any transmission to an emergency communication service or for damages resulting from the	Failure to Use Ordinary Care; Intentional

		performance of installing, maintaining or providing 911 service.	
Kentucky	KRS 65.7637 Limitations of liability for CMRS providers and service suppliers	Notwithstanding any other provision of law, no CMRS provider or service supplier, nor their employees, directors, officers, or agents, except in cases of negligence, or wanton or willful misconduct, or bad faith, shall be liable for any damages in a civil action or subject to criminal prosecution resulting from death or injury to any person or from damage to property incurred by any person in connection with developing, adopting, establishing, participating in, implementing, maintaining, or providing access to a CMRS system for the purposes of providing wireless 911 service or E911 service in compliance with the wireless E911 service requirements established by the FCC order and any rules and regulations which are or may be adopted by the Federal Communications Commission in carrying out the FCC orders: in connection with the quality of the service; in connection with ensuring that any 911 call goes through properly; or in connection with providing access to CMRS service in connection with providing wireless 911 service or E911 service.	Willful & Wanton; Negligence

Louisiana	LSA-R.S. 33:9108. Indemnification of board members; limitation of liability	B. No district, sheriff, service provider, nor any wireless service supplier which meets the requirements of R.S. 33:9109(F)(1) and (2), nor their respective officers, directors, employees, or agents shall be liable to any person for civil damages resulting from, arising out of, or due to any act or omission in the development, design, installation, operation, maintenance, performance, or provision of 911 services, except when said damages are a result of willful or wanton misconduct or gross negligence on their respective part.	Gross Negligence; Willful & Wanton
Maine	25 M.R.S.A. § 2930. Immunity	1. Governmental entity. Subject to all the limitations and exceptions provided under the Maine Tort Claims Act, Title 14, chapter 741,1 a government entity is immune from tort liability for property damages, bodily injury or death resulting from acts or omissions occurring in developing, establishing, implementing, maintaining or operating the E-9-1-1 system. 2. Telecommunications providers. A telecommunications provider assisting in the implementation and operation of the statewide E-9-1-1 system, including, but not limited to, the development, establishment and maintenance of the E-9-1-1 system, is subject to tort liability: A. For property damages, bodily injury or death resulting from any defect in the E-9-1-1 system or inadequacy in the provision of E-9-1-1 service caused by the telecommunications provider's negligent acts or omissions in developing, establishing, implementing, maintaining or operating the E-9-1-1 system, up to a maximum amount for any and all claims arising out of a single occurrence not to exceed $300,000 or the dollar amount that appears in Title 14, section 8105, subsection 1, whichever is greater; and B. For property damages, bodily injury or	Intentional; Willful; Reckless

		death resulting from any defect in the E-9-1-1 system or inadequacy in the provision of E-9-1-1 service caused by the telecommunications provider's intentional, willful or reckless acts or omissions in developing, establishing, implementing, maintaining or operating the E-9-1-1 system, without limitation on the amount.	
Maryland	N/A --> Caselaw--> Apply "special duty" requirement	Police dispatcher employed by county who received anonymous call concerning location of unnamed girl did not, by her statement that dispatch system would "send someone out," act to protect or assist a specific group of individuals like that girl and thus did not owe a special duty to her, precluding liability in negligence action brought by girl's father in connection with girl's death from hypothermia in location where anonymous caller had left her; rather, dispatcher provided general public service under statutes requiring counties to have in operation an enhanced 911 emergency telephone system. Muthukumarana v. Montgomery County, 2002, 805 A.2d 372, 370 Md. 447.	

Massachusetts	N/A	N/A	N/A
Michigan	MCLA 484.1604. Civil liability	Sec. 604. Except for pro rata charges for the service during a period when the service may be fully or partially inoperative, a service supplier, public agency, PSAP, or an officer, agent, or employee of any service supplier, public agency, or PSAP, or an owner or lessee of a pay station telephone shall not be liable for civil damages to any person as a result of an act or omission on the part of the service supplier, public agency, PSAP, or an officer, agent, or employee of any service supplier, public agency, or PSAP, or an owner or lessee in complying with any provision of this act, unless the act or omission amounts to a criminal act or to gross negligence or willful and wanton misconduct.	Criminal Act; Gross Negligence; Willful & Wanton
Minnesota	M.S.A. § 403.07 403.07. Standards established; data privacy	(c) A wire-line telecommunications service provider, its employees, or its agents are not liable to any person for civil damages resulting from or caused by any act or omission in the development, design, installation, operation, maintenance, performance, or provision of enhanced 911 telecommunications service, except for willful or wanton misconduct.	Willful & Wanton

Mississippi	MS ST § 19-5-361. Limitation of liability for 911 suppliers	Any Emergency 911 service supplier, Emergency 911 Voice over Internet Protocol service supplier, and Emergency 911 CMRS provider operating within the State of Mississippi, its employees, directors, officers, agents and subcontractors, shall be entitled to receive the limitations of liability as provided to the state, or any agency or local government of the state, pursuant to Section 11-46-15, Mississippi Code of 1972. **11-46-15:** (1) In any claim or suit for damages against a governmental entity or its employee brought under the provisions of this chapter, the liability shall not exceed the following for all claims arising out of a single occurrence for all damages permitted under this chapter:(a) For claims or causes of action arising from acts or omissions occurring on or after July 1, 1993, but before July 1, 1997, the sum of Fifty Thousand Dollars ($50,000.00);(b) For claims or causes of action arising from acts or omissions occurring on or after July 1, 1997, but before July 1, 2001, the sum of Two Hundred Fifty Thousand Dollars ($250,000.00);(c) For claims or causes of action arising from acts or omissions occurring on or after July 1, 2001, the sum of Five Hundred Thousand Dollars ($500,000.00).	Limited Liability - See Statute
Missouri	VAMS 190.307. No civil liability for operation of emergency system, giving or following emergency instructions, exceptions	1. No public agency or public safety agency, nor any officer, agent or employee of any public agency, shall be liable for any civil damages as a result of any act or omission except willful and wanton misconduct or gross negligence, in connection with developing, adopting, operating or implementing any plan or system required by sections 190.300 to 190.340.	Gross Negligence; Willful & Wanton

Montana	MCA 27-1-735. Emergency communications systems--lawful release of information	(2) A local exchange telephone company registered as a Montana telecommunications service provider, as provided in 69-3-805, or a provider of commercial mobile service, as defined in 47 U.S.C. 332(d)(1), that provides emergency communications systems and related services and its employees and agents are not liable in tort to any person for damages alleged to have been caused by the design, development, installation, maintenance, or provision of emergency communications systems or related services unless the acts or omissions of the entities or persons constitute gross negligence or willful or wanton misconduct. This subsection does not provide immunity from liability in a products liability action.	Gross Negligence; Willful & Wanton
Nebraska	Neb. Rev. St. § 86-441. 911 service; immunity from liability	In contracting for such 911 service and in providing such 911 service, except for failure to use reasonable care or for intentional acts, each governing body, public safety agency, and service supplier and their employees and agents shall be immune from liability or the payment for any damages in the performance of installing, maintaining, or providing 911 service.	Failure to Use Reasonable Care; Intentional Acts
Nevada	NRS 707.500. Enhanced 911 service: Immunity from liability for certain entities providing service through public safety answering point in certain circumstances	1. A telephone company, person providing wireless or commercial mobile radio service, public safety answering point, or manufacturer supplying equipment to a telephone company or public safety answering point, or any agent thereof, is not liable to any person who uses an enhanced 911 service for: (a) The release of the telephone number and street address of the telephone used to place the 911 telephone call, including telephone numbers which are not published, if the release was made in good faith; (b) The failure of any equipment or procedure in connection	Failure to Act in Good Faith

		with the provision of an enhanced 911 service; or (c) Any act, or the omission of any act, committed in good faith, while providing, or while in training to provide, services through a public safety answering point.	
New Hampshire	N.H. Rev. Stat. § 508:12-a. Limitation of Liability.	III. (a) No person or corporation shall be liable in any suit for civil damages who, in good faith and without willful or wanton negligence receives, develops, collects, provides, or processes information for the enhanced 911 database or the statewide emergency notification system (ENS) database, relays or transfers enhanced 911 services, transmits ENS messages and notifications to the public, or provides emergency telephone and radio communications for ambulance, police and fire departments.	Willful & Wanton
New Jersey	N.J.S.A. 52:17C-10. Forwarding information about 9-1-1 caller to jurisdictional public safety answering points by telephone company; immunity from liability	d. No telephone company, person providing commercial mobile radio service as defined in 47 U.S.C.s. 332(d), public safety answering point, or manufacturer supplying equipment to a telephone company, wireless telephone company, or PSAP, or any employee, director, officer, or agent of any such entity, shall be liable to any person for civil damages, or subject to criminal prosecution resulting from or caused by any act, failure or omission in the development, design, installation, operation, maintenance, performance or provisioning of any hardware, software, or any other aspect of delivering enhanced 9-1-1 service, wireless 9-1-1 service or wireless enhanced 9-1-1 service. This	Malicious purpose; Willful & Wanton

		limitation of liability is inapplicable if such failure resulted from a malicious purpose or a wanton and willful disregard for the safety of persons or property.	
New Mexico	N.M.S.A. 1978, § 63-9D-10. Immunity	Enhanced 911 systems are within the governmental powers and authorities of the local governing body or state agency in the provision of services for the public health, welfare and safety. In contracting for such services or the provisioning of an enhanced 911 system, except for intentional acts, the local governing body, public agency, equipment supplier, communications service provider and their officers, directors, vendors, employees and agents are not liable for damages resulting from installing, maintaining or providing enhanced 911 systems or transmitting 911 calls.	Intentional
New York	N/A	N/A	N/A

North Carolina	N.C.G.S.A. § 143B-1413. Limitation of liability	(a) Except in cases of wanton or willful misconduct, a communications service provider, and a 911 system provider or next generation 911 system provider, and their employees, directors, officers, vendors, and agents are not liable for any damages in a civil action resulting from death or injury to any person or from damage to property incurred by any person in connection with developing, adopting, implementing, maintaining, or operating the 911 system or in complying with emergency-related information requests from State or local government officials. This section does not apply to actions arising out of the operation or ownership of a motor vehicle.	Willful; Wanton
North Dakota	NDCC § 57-40.6-08. Emergency services communication system, automated notification system, or emergency instructions--Liability	1. A public agency, public safety agency, assessed communications service provider, prepaid wireless service provider or seller, or person that provides access to an emergency services communication system or an automated notification system, or any officer, agent, or employee of any public agency, public safety agency, assessed communications service provider, prepaid wireless service provider or seller, or person is not liable for any civil damages as a result of any act or omission except willful and wanton misconduct or gross negligence in connection with developing, adopting, operating, or implementing any plan or system as provided under this chapter.	Gross Negligence; Willful & Wanton
Ohio	R.C. § 128.32 (Formerly cited as OH ST §§ 4931.49, 5507.32) Liability; improper use of system; disclosure	(C) Except for willful or wanton misconduct, a telephone company, and any other installer, maintainer, or provider, through the sale or otherwise, of customer premises equipment, and their respective officers, directors, employees, agents, and suppliers are not liable in damages in a civil action for injuries, death, or loss to persons or property incurred by any person resulting from any	Willful & Wanton

		of the following: (1) Such an entity's or its officers', directors', employees', agents', or suppliers' participation in or acts or omissions in connection with participating in or developing, maintaining, or operating a 9-1-1 system;	
Oklahoma	63 Okl. St. Ann. § 2817. Liability	C. A service provider of telecommunications or other communication services involved in providing nine-one-one emergency telephone service or nine-one-one wireless emergency telephone service shall not be liable for any claim, damage, or loss arising from the provision of nine-one-one emergency telephone service or nine-one-one wireless emergency telephone service unless the act or omission proximately causing the claim, damage, or loss constitutes gross negligence, recklessness, or intentional misconduct.	Gross Negligence; Reckless; Intentional
Oregon	O.R.S. § 403.110 (Formerly cited as OR ST § 401.715) Liability of 9-1-1 providers	(1) A provider or a 9-1-1 jurisdiction or the employees or agents of a provider or a 9-1-1 jurisdiction may be held civilly liable for the installation, performance, provision or maintenance of a 9-1-1 emergency reporting system or enhanced 9-1-1 telephone service if the provider or the 9-1-1 jurisdiction or the employees or agents of the provider or the 9-1-1 jurisdiction act with willful or wanton conduct.	Willful & Wanton
Pennsylvania	35 Pa. C.S.A. § 5311.25. Limitation of liability	A local exchange carrier, Internet service provider, manufacturer or provider of MLTS, MLTS manager, MLTS operator or 911 service provider shall not be liable for civil damages or penalties as a result of any act or omission, except willful or wanton misconduct, in connection with	Willful & Wanton

		developing, adopting, operating or implementing any plan or system required under this chapter.	
Puerto Rico	25 L.P.R.A. § 172p. Immunities	(b) None of the following shall be liable for the death or injuries to persons or damage to property, except in cases of gross negligence, improper conduct or bad faith: (1) The Government of Puerto Rico and its employees and the municipalities and their employees in the execution of their duties and activities. (2) The emergency and disaster management agencies or entities and their employees in the execution of their duties and activities. (3) Any volunteer who renders emergency management services.	Gross Negligence; Improper Conduct; Bad Faith
Rhode Island	Gen. Laws 1956, § 39-21.1-5. Establishment of 9-1-1 service	(h) The state of Rhode Island and Providence Plantations, the E 9-1-1 Uniform Emergency Telephone System Authority, local public service answering points, E 9-1-1 service providers, including telephone common carriers and telecommunication services providers and their respective employees, directors, officers, representatives or agents shall not be liable to any person for civil damages resulting from or caused by any act or omission in the development, design, installation, operation, maintenance, performance or provision of E 9-1-1 service, except to the extent due directly to its willful misconduct or gross negligence. Also, no provider of E 9-1-1 service, including a telecommunication services provider shall be liable to any person who uses E 9-1-1 service, for the release of subscriber information, including but not limited to, billing	Willful; Gross Negligence

		information required under this act, to any public safety answering point or to the state of Rhode Island or the E 9-1-1 Uniform Emergency Telephone System Authority.	
South Carolina	Code 1976 § 23-47-70. Liability.	(A) A local government or public safety agency, as defined in Section 23-47-10, or state government entity, their officers, agents, or employees, together with any person following their instructions in rendering services, are not liable for civil damages as a result of an act or omission under this chapter, including, but not limited to, developing, adopting, operating, or implementing a plan or system pursuant to the South Carolina Tort Claims Act, Section 15-78-60(5) or 15-78-60(19).	Not Liable
South Dakota	SDCL §34-45-17. Immunity from liability	The 911 emergency reporting system provided by this chapter is within the governmental powers and authority of the governing body or public agency. In contracting for the 911 emergency reporting system or the provisioning of the 911 service, except for willful or wanton negligence or intentional acts, the board, the governing body, the public agency, the service provider, the prepaid wireless service provider, the prepaid wireless service seller, and the service supplier, their employees and agents, are immune from liability for a failure in the use or operation of the 911 system. The	Willful & Wanton; Intentional

		immunity provided by this section does not extend to the installation or maintenance of the 911 system.	
Tennessee	T.C.A. § 7-86-320. IP-enabled services; immunity	(d)(1) Emergency communications districts shall be immune from suit or liability for civil claims arising from the actions or omission of emergency communications district personnel in processing emergency calls, except that claims for recklessness or intentional misconduct in processing emergency calls shall be permitted, but damages for such claims shall not exceed actual damages or the maximum award that may be awarded per claimant by the Tennessee claims commission.	Intentional; Reckless
Texas	V.T.C.A., Health & Safety Code § 771.053. Statewide Limitation on Liability of Service Providers and Certain Public Officers	(a) A service provider of communications service involved in providing 9-1-1 service, a manufacturer of equipment used in providing 9-1-1 service, a developer of software used in providing 9-1-1 service, a third party or other entity involved in providing 9-1-1 service, or an officer, director, or employee of the service provider, manufacturer, developer, third party, or other entity involved in providing 9-1-1 service is not liable for any claim, damage, or loss arising from the provision of 9-1-1 service unless the act or omission proximately causing the claim, damage, or loss constitutes gross negligence, recklessness, or intentional misconduct.	Gross Negligence; Reckless; Intentional

Utah	U.C.A. 1953 § 69-2-503. Liabilities of Providers	(2) A provider of local exchange service, radio communications service, voice over Internet protocol service, or telephone terminal equipment needed to implement or enhance 911 emergency service, and their employees and agents, are not liable for any damages in a civil action for injuries, death, or loss to person or property incurred as a result of any act or omission of the provider, employee, or agent, in connection with developing, adopting, implementing, maintaining, enhancing, or operating a 911 emergency service, except for damages or injury intentionally caused by or resulting from gross negligence of the provider or person.	Intentional; Gross Negligence
Vermont	30 VSA § 7060. Limitation of liability	No person shall be liable in any suit for civil damages who in good faith receives, develops, collects, or processes information for the Enhanced 911 database or develops, designs, adopts, establishes, installs, participates in, implements, maintains, or provides access to telephone, mobile, or IP-enabled service for the purpose of helping persons obtain emergency assistance in accordance with this chapter unless such action constitutes gross negligence or an intentional tort. In addition, no provider of telephone, mobile, or other IP-enabled service or a provider's respective employees, directors, officers, assigns, affiliates, or agents shall be liable for civil damages in connection with the release of customer information to any governmental entity, including any public safety answering point, as required under this chapter.	Intentional; Gross Negligence
Virgin islands	23 V.I.C. § 1078 Telephone company exempt from liability for providing ANI or ALI information	(c) A common carrier, its employees, agents, contractors, and affiliates shall not be held liable for any acts in the operation, administration, or maintenance of a 911 service, unless such acts are	Willful

		found to be of willful intent as defined in title 1, section 41, of the Virgin Islands Code.	
Virginia	VA Code Ann. § 44-146.23. Immunity from liability	A. Neither the Commonwealth, nor any political subdivision thereof, nor federal agencies, nor other public or private agencies, nor, except in cases of willful misconduct, public or private employees, nor representatives of any of them, engaged in any emergency services activities, while complying with or attempting to comply with this chapter or any rule, regulation, or executive order promulgated pursuant to the provisions of this chapter, shall be liable for the death of, or any injury to, persons or damage to property as a result of such activities.	Willful
Washington	West's RCWA 38.52.550. Emergency communications systems and information--Immunity from civil liability	A telecommunications company, radio communications service company, or interconnected voice over internet protocol service company, providing emergency communications systems or services or a business or individual providing database information to enhanced 911 emergency communications personnel is not liable for civil damages caused by an act or omission of the company, business, or individual in the: (2) Design, development, installation, maintenance, or provision of consolidated enhanced 911 emergency communications systems or services other than an act or omission constituting gross negligence or wanton or willful misconduct.	Gross Negligence; Willful & Wanton
West Virginia	W. Va. Code, § 24-6-8. Limitation of liability	A public agency or a telephone company participating in an emergency telephone system or a county which has established an enhanced emergency telephone system, and any officer, agent or employee of the public agency, telephone company or county is not liable for damages in a civil action for injuries,	Willful or Wanton

		death or loss to persons or property arising from any act or omission, except willful or wanton misconduct, in connection with developing, adopting or approving any final plan or any agreement made pursuant to this article, or otherwise bringing into operation or participating in the operation of an emergency telephone system or an enhanced emergency telephone system pursuant to this article.	
Wisconsin	W.S.A. 256.35. Statewide emergency services number	(7) Liability exemption. All of the following shall not be liable to any person who uses an emergency number system created under this section or makes an emergency telephone call initially routed to a wireless public safety answering point, as defined in sub. (3m)(a)7., 2015 stats.: (a) A telecommunications utility. (b) A wireless provider, as defined in s. 256.35(3m)(a)6., 2015 stats. (c) A local government, as defined in s. 256.35(3m)(a)4., 2015 stats. (d) A person that supplies any service, product, equipment, or database, including any related emergency notification service or process, that is used for or in conjunction with the installation, implementation, operation, or maintenance of the emergency number system and that is used by a public safety answering point.	No Liability

Wyoming	WS 1977 § 16-9-108. Immunity for providers	No basic emergency service provider or service supplier and no employee or agent thereof shall be liable to any person or entity for infringement or invasion of the right of privacy of any person caused or claimed to have been caused, directly or indirectly, by any act or omission in connection with the installation, operation, maintenance, removal, presence, condition, occasion or use of emergency service features, automatic number identification or automatic location identification services and the equipment associated therewith, including the identification of the telephone number, address or name associated with the telephone used by the person accessing 911 service, wireless automatic number identification, wireless automatic location identification service or text to 911 service. A governmental entity, public safety agency, local exchange access company, telephone exchange access company or wireless carrier that provides access to an emergency system or any officers, agents or employees thereof is not liable as a result of any act or omission except willful and wanton misconduct or gross negligence in connection with developing, adopting, operating or implementing emergency telephone service, enhanced wireless 911 service, text to 911 service or any 911 system.	Gross Negligence; Willful & Wanton

Appendix B
State Public Duty Doctrines

State	Public Duty Doctrine	Explanation/Source
Alabama	Yes	Applied and recognized in *Alabama Dept. of Corrections v. Thompson*, 855 So.2d 1016 (Ala. 2006).
Alaska	No	"To allow the public duty doctrine to disturb this equality would create immunity where the legislature has not." *Adams v. State*, 555 P.2d 235 (Alaska 1979).
Arizona	Yes	Originally not recognized (*Ryan v. State* (1982); superseded by statute to re-enact public duty doctrine (*See* Glazer v. State, 237 Ariz. 160, 347 P.3d 1141 (Ariz. 2015).
Arkansas	N/A (No Caselaw)	N/A
California	Yes	Recognized in Caselaw. See *Williams v. State*, 34 Cal.3d 186, 64 P.2d 137 (Ca. 1983); *Tapia v. State*, 2009 WL 2603105 (Cal. App. 2009).
Colorado	No	"Accordingly, we reject the public duty rule in Colorado." *Leake v. Cain*, 720 P.2d 152, 55 USLW 2013 (Colo. 1986).
Connecticut	Yes	"[W]here [it] said that since certain public officials were engaged upon a governmental duty ... so long as they act in good faith, in the exercise of an honest judgment, and not in the abuse of their discretion, or maliciously or wantonly, they cannot be held liable." *Gordon v. Bridgeport Housing Authority*, 208 Conn. 161, 165–66, 544 A.2d 1185 (1988).
Delaware	Yes	Recognized by Delaware. *See Laws v. Handy*, 2017 WL 3127783 at 4* (Del. Super. July 21, 2017).
Florida	Yes	*Pollock v. Fla. Dep't of Highway Patrol,* 882 So.2d 928, 932–33 (Fla. 2004).
Georgia	Yes	Does not apply outside of police protection services (*Hamilton v. Cannon*, 482 S.E. 2d 370 (Ga. 1997)).
Hawaii	Yes	Limited Caselaw; only 2 cases (*Ruf v. Honolulu Police Dept*, 89 Hawai'i 315 (1999); *Concerned Citizens of Palolo v. Korean Buddhist Dae Won Sa Temple of Hawai'i*, 107 Hawai'i 226 (2005)).
Idaho	Yes (Limited Caselaw)	Recognized by *Rees v. State, Dept. of Health and Welfare*, 143 Idaho 10, 15-16, 137 P.3d 397, 402-403 (Idaho 2006).
Illinois	No	Abolished by *Coleman v. East Joliet Fire Protection Dist.*, 46 N.E.3d 741, 2016 IL 117952 (Ill. 2016).

Indiana	Yes	Footnote 5 of *Minks v. Pena*, 709 N.E.2d 379 (Ind. App 2003): "Moreover, we do not believe that it is our place to follow in the footsteps of the supreme judicial court of Massachusetts towards the abolition of the public duty rule which has so recently been applied by our supreme court in *Mullin*. See *Jean W. v. Commonwealth*, 414 Mass. 496, 610 N.E.2d 305 (1993)."
Iowa	Yes	"We conclude the public-duty doctrine remains good law after our adoption of sections of the Restatement (Third) of Torts." *Estate of Gottschalk by Gottschalk v. Pomeroy Development, Inc*., 893 N.W.2d 579 (Iowa 2017).
Kansas	Yes	See *Potts v. Board of County Com'rs of Leavenworth County*, 39 Kan. App.2d 711, 76 P.3d 988 (Kan. App. 2008).
Kentucky	Yes	"Often referred to as the public duty doctrine, absent a special relationship to the victim, public officials have a duty to the public at large, not to individual crime victims" *Gibson v. Hicks*, 2012 WL 3047209 (Ky. App. 2012).
Louisiana	No	"The public duty doctrine has never been adopted by this Court, and we have criticized and rejected it as a categorical rule" … "instead of a traditional public duty doctrine in Louisiana, the legislature adopted La. R.S. 9:2798.1, which exempts public entities from liability for their employees' discretionary or policy-making acts" Hardy v. Bowie, 744 So.2d 606 (La. 1999).
Maine	Yes (Limited Caselaw)	Limited Caselaw; "It is settled law in this state that, when the employees of a municipal corporation are engaged in what may be called a governmental function, or public duty, the municipal corporation is not liable for their acts of negligence." *Bouchard v. City of Auburn*, 133 Me. 439, 179 A. 718 (Me. 1935).
Maryland	Yes	*Ashburn v. Anne Arundel County*, 510 A.2d 1078 (Md. 1986).
Massachusetts	No	"By recognizing that the public duty rule is incompatible with the Act, we align ourselves with most jurisdictions that have squarely considered the issue. While a sizeable number of jurisdictions still adhere to the public duty rule...the trend has been to abolish the rule" *Jean W. v. Com*., 414 Mass. 496, 610 N.E.2d 305 (Mass. 1993).

Michigan	Yes	
Minnesota	Yes	*Ariola v. City of Stillwater*, 2014 WL 5419809 (Minn. 2014).
Mississippi	Yes	Limited Caselaw, but Mississippi recognizes the Public Duty Doctrine. See *Dean v. Walker*, 743 F.Supp.2d 605 (S.D. Miss 2010).
Missouri	Yes	Missouri recognizes Public Duty Doctrine. The public duty doctrine will not apply where defendant public employees act "in bad faith or with malice." *Jackson v. City of Wentzville*, 844 S.W.2d 585, 588 (Mo. App. 1993).
Montana	Yes	See *Gonzales v. City of Bozeman*, 352 Mont. 145, 217 P.3d 487 (Mont. 2009)
Nebraska	No	"In *Maple v. City of Omaha*, 222 Neb. 293, 384 N.W.2d 254 (1986), we concluded that the 'public duty doctrine' had no place in Nebraska law." *Drake v. Drake*, 260 Neb. 530, 618 N.W.2d 650 (Ne. 2000).
Nevada	Yes	See *Coty v. Washoe County*, 108 Nev. 757, 839 P.2d 97 (Nev. 1992).
New Hampshire	Yes	See *Hartman v. Town of Hooksett*, 125 N.H. 34480 A.2d 12 (N.H. 1984)
New Jersey	Yes (modified version in statute)	Section of 9–1–1 immunity statute shielding 9–1–1 operators from liability when providing assistance to an investigative or law enforcement officer provides immunity to 9–1–1 operators for acts or omissions in rendering assistance to ongoing law enforcement investigations and activities. N.J.S.A. 52:17C–10(e); *Wilson ex rel. Manzano v. City of Jersey City*, 39 A.3d 177 (N.J. 2012).
New Mexico	No	The distinction between "public duty" and "private duty" or "special duty" is no less arbitrary and no less a vestige of the doctrine of sovereign immunity than are the "governmental-proprietary" and "discretionary-ministerial" distinctions abolished by Section 41–4–2(B) of the Tort Claims Act. *Schear v. Board of County Com'rs of Bernalillo County*, 101 N.M. 671, 687 P.2d 728 (N.M. 1984).
New York	Yes	See Valdez v. City of New York, 18 N.Y.3d 69, 960 N.E.2d 356 (N.Y. 2011)
North Carolina	Yes	*Braswell v. Braswell*, 330 N.C. 363, 410 S.E.2d 897 (NC 1991)
North Dakota	No	"We reject the City's invitation to adopt the public duty doctrine because it is incompatible with North Dakota law" Ficek v. Morken, 685 N.W.2d 98, 2004 ND

		158 (N.D. 2004).
Ohio	Yes	"While we agree that Ohio's common-law public-duty doctrine remains viable, we conclude that it does not apply to situations involving wanton or reckless conduct." *Estate of Graves v. Circleville*, 179 Ohio App.3d 479, 902 N.E.2d 535 (Ohio App. 2008).
Oklahoma	N/A (No Caselaw)	N/A
Oregon	No	"To the extent that *Svenson v. Brix*, 156 Or. 236, 64 P.2d 830 (1937), relies on the public duty doctrine, we consider it to have been overruled by the enactment of ORS 30.265(1)." *Brennen v. City of Eugene*, 285 Or. 40, 591 P.2d 719 (Or. 1979).
Pennsylvania	Yes	See *Casteel v. Tinkey*, 151 A.3d 261 (Pa. 2016)
Rhode Island	Yes	See *Torres v. Damicis*, 853 A.2d 1233 (R.I. 2004).
South Carolina	Yes	See *Tanner v. Florence County Treasurer*, 336 S.C. 552, 561, 521 S.E.2d 153, 158 (1999).
South Dakota	Yes	South Dakota has specifically refused to abrogate the public duty doctrine. *See Gleason v. Peters*, 1997 SD 102, ¶ 9, 568 N.W.2d 482, 484 (S.D. 2012).
Tennessee	Yes	*Ezell v. Cockrell*, 902 S.W.2d 394 (Tenn. 1995)
Texas	Yes (Limited Caselaw)	See *Fernandez v. City of El Paso*, 876 S.W.2d 370 (Tex. App. 1993).
Utah	Yes	"...we take this opportunity to clarify the public duty doctrine. First, we decline to abrogate the doctrine, as several other states have done, and retain the public duty doctrine as part of Utah's common law. Second, we overturn in part Webb v. University of Utah, 2005 UT 80, 125 P.3d 906, and hold that the public duty doctrine applies only to the omissions of a governmental actor. The doctrine does not immunize the State from liability for affirmative acts that harm a plaintiff. Third, we clarify that the public duty doctrine is limited to situations where a plaintiff seeks to impose liability for a duty to protect the general public from external harms." *Cope v. Utah Valley State College*, 342 P.3d 243, 313 Ed. Law Rep. 364 (Utah 2014).
Vermont	No	"We decline to adopt the confusing and inconsistent public duty doctrine as a means of limiting the liability of government employees who are already protected to some extent by the doctrine of qualified official immunity, or as a means of addressing the discrepancy between the statutory protection

		afforded to state and municipal employees in Vermont." *Hudson v. Town of East Montpelier*, 161 Vt. 168 638 A.2d 561 (Vt. 1993).
Virginia	Yes	See *Burdette v. Marks*, 244 Va. 309421 S.E.2d 419 (Va. 1992).
Washington	Yes	Under the public duty doctrine, no liability may be imposed for a public official's negligent conduct unless it is shown that "the duty breached was owed to the injured person as an individual and was not merely the breach of an obligation owed to the public in general (i.e., a duty to all is a duty to no one)." *Taylor v Stevens County*, 111 Wash.2d at 163, 759 P.2d 447 (Wash 1988).
West Virginia	Yes	See *Randall v. Fairmont City Police Dept.*, 186 W.Va. 336, 346, 412 S.E.2d 737, 747 (1991). *See also Parkulo v. West Virginia Board of Probation and Parole*, 199 W.Va. 161, 483 S.E.2d 507 (1996).
Wisconsin	No	"[T]here is no distinction to be drawn between a 'public duty' and a 'special duty.'" *Coffey v. City of Milwaukee*, 74 Wis.2d 526247 N.W.2d 132 (Wis. 1976).
Wyoming	No	"The public-duty/special-duty rule was in essence a form of sovereign immunity and viable when sovereign immunity was the rule. The legislature has abolished sovereign immunity in this area. The public duty only rule, if it ever was recognized in Wyoming, is no longer viable." *DeWald v. State*, 719 P.2d 643 (Wyo. 1986).
District of Columbia	Yes	See *Platt v. District of Columbia*, 467 A.2d 149, 151 (D.C.1983)
Guam	Yes	See *Shim v. Vert Const. Co.*, Civ. No. 91–00019A; 1991 WL 255832 ((D. Guam App. Div. 1991)
Puerto Rico	N/A (No Caselaw)	N/A
Virgin Islands	Yes	See *Perez v. Government of the Virgin Islands*, 847 F.2d 104, 107 (3d Cir. 1988). In Perez, the Third Circuit found that the public duty doctrine was the law of the Virgin Islands in a situation where a "duty [arose] under legislative enactments or administrative regulations.

Appendix C
Summary of State Notice Statutes

State	Notice Requirement?	Statute
Alabama	No	N/A
Alaska	Yes	Alaska Stat. § 45.48.010 et seq.
Arizona	Yes	Ariz. Rev. Stat. § 18-545
Arkansas	Yes	Ark. Code §§ 4-110-101 et seq.
California	Yes	Cal. Civ. Code §§ 1798.29, 1798.8*2*
Colorado	Yes	Colo. Rev. Stat. § 6-1-716
Connecticut	Yes	Conn. Gen Stat. §§ 36a-701b, 4e-70
Delaware	Yes	Del. Code tit. 6, § 12B-101 et seq.
Florida	Yes	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)
Georgia	Yes	Ga. Code §§ 10-1-910, -911, -912; § 46-5-214
Hawaii	Yes	Haw. Rev. Stat. § 487N-1 et seq.
Idaho	Yes	Idaho Stat. §§ 28-51-104 to -107
Illinois	Yes	815 ILCS §§ 530/1 to 530/25

Indiana	Yes	Ind. Code §§ 4-1-11 *et seq.*, 24-4.9 *et seq.*
Iowa	Yes	Iowa Code §§ 715C.1, 715C.2
Kansas	Yes	Kan. Stat. § 50-7a01 et seq.
Kentucky	Yes	KRS § 365.732, KRS §§ 61.931 to 61.934
Louisiana	Yes	La. Rev. Stat. §§ 51:3071 et seq.
Maine	Yes	Me. Rev. Stat. tit. 10 § 1346 et seq.
Maryland	Yes	Md. Code Com. Law §§ 14-3501 et seq., Md. State Govt. Code §§ 10-1301 to -1308
Massachusetts	Yes	Mass. Gen. Laws § 93H-1 et seq.
Michigan	Yes	Mich. Comp. Laws §§ 445.63, 445.72
Minnesota	Yes	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	Yes	Miss. Code § 75-24-29
Missouri	Yes	Mo. Rev. Stat. § 407.1500
Montana	Yes	Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 *et seq.*, 33-19-321
Nebraska	Yes	Neb. Rev. Stat. §§ 87-801 et seq.
Nevada	Yes	Nev. Rev. Stat. §§ 603A.010 *et seq.*, 242.183

New Hampshire	Yes	N.H. Rev. Stat. §§ 359-C:19 et seq.
New Jersey	Yes	N.J. Stat. § 56:8-161 et seq.
New Mexico	Yes	2017 H.B. 15, Chap. 36 (effective 6/16/2017)
New York	Yes	N.Y. Gen. Bus. Law § 899-AA, N.Y. State Tech. Law 208
North Carolina	Yes	N.C. Gen. Stat §§ 75-61, 75-65
North Dakota	Yes	N.D. Cent. Code §§ 51-30-01 et seq.
Ohio	Yes	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Yes	Okla. Stat. §§ 74-3113.1, 24-161 to -166
Oregon	Yes	Oregon Rev. Stat. §§ 646A.600 to .628
Pennsylvania	Yes	73 Pa. Stat. §§ 2301 *et seq.*
Rhode Island	Yes	R.I. Gen. Laws §§ 11-49.3-1 et seq.
South Carolina	Yes	S.C. Code § 39-1-90
South Dakota	No	N/A
Tennessee	Yes	Tenn. Code §§ 47-18-2107; 8-4-119
Texas	Yes	Tex. Bus. & Com. Code §§ 521.002, 521.053

Utah	Yes	Utah Code §§ 13-44-101 et seq.
Vermont	Yes	Vt. Stat. tit. 9 §§ 2430, 2435
Virginia	Yes	Va. Code §§ 18.2-186.6, 32.1-127.1:05
Washington	Yes	Wash. Rev. Code §§ 19.255.010, 42.56.590
West Virginia	Yes	W.V. Code §§ 46A-2A-101 et seq.
Wisconsin	Yes	Wis. Stat. § 134.98
Wyoming	Yes	Wyo. Stat. §§ 40-12-501 et seq.
District of Columbia	Yes	D.C. Code §§ 28- 3851 et seq.
Guam	Yes	9 GCA §§ 48-10 et seq.
Puerto Rico	Yes	10 Laws of Puerto Rico §§ 4051 et seq.
Virgin Islands	Yes	V.I. Code tit. 14, §§ 2208, 2209

Appendix D
State Notice Statutes

I. ALABAMA:

N/A

II. ALASKA

Sec. 45.48.010. Disclosure of breach of security.

(a) If a covered person owns or licenses personal information in any form that includes personal information on a state resident, and a breach of the security of the information system that contains personal information occurs, the covered person shall, after discovering or being notified of the breach, disclose the breach to each state resident whose personal information was subject to the breach.

(b) An information collector shall make the disclosure required by (a) of this section in the most expeditious time possible and without unreasonable delay, except as provided in AS 45.48.020 and as necessary to determine the scope of the breach and restore the reasonable integrity of the information system.

(c) Notwithstanding (a) of this section, disclosure is not required if, after an appropriate investigation and after written notification to the attorney general of this state, 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 determination shall be documented in writing, and the documentation shall be maintained for five years. The notification required by this subsection may not be considered a public record open to inspection by the public.

Sec. 45.48.020. Allowable delay in notification.

An information collector may delay disclosing the breach under AS 45.48.010 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.

Sec. 45.48.030. Methods of notice.

An information collector shall make the disclosure required by AS 45.48.010

(1) by a written document sent to the most recent address the information collector has for the state resident;

(2) by electronic means if the information collector's primary method of communication with the state resident is by electronic means or if making the disclosure by the electronic means is consistent with the provisions regarding electronic records and signatures required for notices legally required to be in writing under 15 U.S.C. 7001 et seq. (Electronic Signatures in Global and National Commerce Act); or

(3) if the information collector 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, by

(A) electronic mail if the information collector has an electronic mail address for the state resident;

(B) conspicuously posting the disclosure on the Internet website of the information collector if the information collector maintains an Internet website; and

(C) providing a notice to major statewide media.

Sec. 45.48.040. Notification of certain other agencies.

(a) If an information collector is required by AS 45.48.010 to notify more than 1,000 state residents of a breach, the information collector shall also notify without unreasonable delay all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis and provide the agencies with the timing, distribution, and content of the notices to state residents.

(b) This section may not be construed to require the information collector to provide the consumer reporting agencies identified under (a) of this section with the names or other personal information of the state residents whose personal information was subject to the breach.

(c) This section does not apply to an information collector who is subject to the Gramm-Leach-Bliley Financial Modernization Act.

(d) In this section, "consumer credit reporting agency that compiles and maintains files on consumers on a nationwide basis" has the meaning given to "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" in 15 U.S.C. 1681a(p).

Sec. 45.48.050. Exception for employees and agents.

In AS 45.48.010_- 45.48.090, 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.

Sec. 45.48.060. Waivers.

A waiver of AS 45.48.010 - 45.48.090 is void and unenforceable.

Sec. 45.48.070. Treatment of certain breaches.

(a) If a breach of the security of the information system containing personal information on a state resident that is maintained by an information recipient occurs, the information recipient is not required to comply with AS 45.48.010 - 45.48.030. However, immediately after the information recipient discovers the breach, the information recipient shall notify the information distributor who owns the personal information or who licensed the use of the personal information to the information recipient about the breach and cooperate with the information distributor as necessary to allow the information distributor to comply with (b) of this section. In this subsection,

"cooperate" means sharing with the information distributor information relevant to the breach, except for confidential business information or trade secrets.

(b) If an information recipient notifies an information distributor of a breach under (a) of this section, the information distributor shall comply with AS 45.48.010 - 45.48.030 as if the breach occurred to the information system maintained by the information distributor.

Sec. 45.48.080. Violations.

(a) If an information collector who is a governmental agency violates AS 45.48.010 - 45.48.090 with regard to the personal information of a state resident, the information collector

(1) is liable to the state for a civil penalty of up to $500 for each state resident who was not notified under AS 45.48.010 - 45.48.090, but the total civil penalty may not exceed $50,000; and

(2) may be enjoined from further violations.

(b) If an information collector who is not a governmental agency violates AS 45.48.010 - 45.48.090 with regard to the personal information of a state resident, the violation is an unfair or deceptive act or practice under AS 45.50.471 - 45.50.561. However,

(1) the information collector is not subject to the civil penalties imposed under AS 45.50.551 but is liable to the state for a civil penalty of up to $500 for each state resident who was not notified under AS 45.48.010_- 45.48.090, except that the total civil penalty may not exceed $50,000; and

(2) damages that may be awarded against the information collector under

(A) AS 45.50.531 are limited to actual economic damages that do not exceed $500; and

(B) AS 45.50.537 are limited to actual economic damages.

(c) The Department of Administration may enforce (a) of this section against a governmental agency. The procedure for review of an order or action of the department under this subsection is the same as the procedure provided by AS 44.62 (Administrative Procedure Act), except that the office of administrative hearings (AS 44.64.010) shall conduct the hearings in contested cases and the decision may be appealed under AS 44.64.030 (c).

Sec. 45.48.090. Definitions.

In AS 45.48.010 - 45.48.090,

(1) "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; in this paragraph, "acquisition" includes acquisition by

(A) photocopying, facsimile, or other paper-based method;

(B) a device, including a computer, that can read, write, or store information that is represented in numerical form; or

(C) a method not identified by (A) or (B) of this paragraph;

(2) "covered person" means a

(A) person doing business;

(B) governmental agency; or

(C) person with more than 10 employees;

(3) "governmental agency" means a state or local governmental agency, except for an agency of the judicial branch;

(4) "information collector" means a covered person who owns or licenses personal information in any form if the personal information includes personal information on a state resident;

(5) "information distributor" means a person who is an information collector and who owns or licenses personal information to an information recipient;

(6) "information recipient" means a person who is an information collector but who does not own or have the right to license to another information collector the personal information received by the person from an information distributor;

(7) "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; in this subparagraph, "individual's name" means a combination of an individual's

(i) first name or first initial; and

(ii) 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) except as provided in (iv) of this subparagraph, the individual's account number, credit card number, or debit card number;

(iv) if an account can only be accessed with a personal code, the number in (iii) of this subparagraph and the personal code; in this sub-subparagraph, "personal code" means a security code, an access code, a personal identification number, or a password;

(v) passwords, personal identification numbers, or other access codes for financial accounts.

III. ARIZONA

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

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

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

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

1. Written notice.

2. Electronic notice if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in the electronic signatures in global and national commerce act (P.L. 106-229; 114 Stat. 464; 15 United States Code section 7001).

3. Telephonic notice.

4. Substitute notice if the person demonstrates that the cost of providing notice pursuant to paragraph 1, 2 or 3 of this subsection would exceed fifty thousand dollars or that the affected class of subject individuals to be notified exceeds one hundred thousand persons, or the person does not have sufficient contact information. Substitute notice shall consist of all of the following:

(a) Electronic mail notice if the person has electronic mail addresses for the individuals subject to the notice.

(b) Conspicuous posting of the notice on the website of the person if the person maintains one.

(c) Notification to major statewide media.

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

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

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

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

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

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

1. A person subject to title V of the Gramm-Leach-Bliley act (P.L. 106-102; 113 Stat. 1338; 15 United States Code sections 6801 through 6809).

2. Covered entities and business associates as defined under regulations implementing the health insurance portability and accountability act of 1996, 45 Code of Federal Regulations section 160.103 (2003).

K. The department of public safety, a county sheriff's department, a municipal police department, a prosecution agency and a court shall create and maintain an information security policy that includes notification procedures for a breach of the security system of the department of public safety, the county sheriff's department, the municipal police department, the prosecuting agency or the court.

L. For the purposes of this section:

1. "Breach", "breach of the security of the system", "breach of the security system" or "security breach" means an unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information maintained by a person as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual. Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security system if the personal information is not used for a purpose unrelated to the person or subject to further wilful unauthorized disclosure.

2. "Court" means the supreme court, court of appeals, superior court, courts inferior to the superior court and justice courts.

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

4. "Individual" means a person that is a resident of this state as determined by a principal mailing address in this state as reflected in the records of the person conducting business in this state at the time of the breach.

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

6. "Personal information":

(a) Means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not encrypted, redacted or secured by any other method rendering the element unreadable or unusable:

(i) The individual's social security number.

(ii) The individual's number on a driver license issued pursuant to section 28-3166 or number on a nonoperating identification license issued pursuant to section 28-3165.

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

(b) Does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

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

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

IV. ARKANSAS

§ 4-110-105. Disclosure of security breaches

(a)(1) Any person or business that acquires, owns, or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

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

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

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

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

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

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

(1) Written notice;

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

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

(i) The cost of providing notice would exceed two hundred fifty thousand dollars ($250,000);
(ii) The affected class of persons to be notified exceeds five hundred thousand (500,000); or
(iii) The person or business does not have sufficient contact information.

(B) Substitute notice shall consist of all of the following:
(i) Electronic mail notice when the person or business has an electronic mail address for the subject persons;
(ii) Conspicuous posting of the notice on the website of the person or business if the person or business maintains a website; and
(iii) Notification by statewide media.

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

§ 4-110-108. Penalties

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

V. CALIFORNIA

§ 1798.29. Agencies owning, licensing, or maintaining computerized data including personal information; disclosure of security breach; notice requirements

(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
(1) The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described in paragraph (2) under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.

[STATUTE HAS FORM]

(h)(1) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
(2) For purposes of this section, “medical information” means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
(3) For purposes of this section, “health insurance information” means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
(4) For purposes of this section, “encrypted” means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.
(i) For purposes of this section, “notice” may be provided by one of the following methods:
(1) Written notice.
(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
(A) Email notice when the agency has an email address for the subject persons.
(B) Conspicuous posting, for a minimum of 30 days, of the notice on the agency's Internet Web site page, if the agency maintains one. For purposes of this subparagraph, conspicuous posting on the agency's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding

text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.
(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.
(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs 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 agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.
(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision 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 agency knows the resident customarily accesses the account.
(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.
(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, “agency” includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.
(*l*) For purposes of this section, “encryption key” and “security credential” mean the confidential key or process designed to render the data useable, readable, and decipherable.

§ 1798.82. Person or business who owns or licenses computerized data including personal information; breach of security of the system; disclosure requirements

(a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable. The disclosure shall be made in the most expedient time possible

and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.
(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.
(B) The title and headings in the notice shall be clearly and conspicuously displayed.
(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.
(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[FORM IN STATUTE]

VI. COLORADO

Colo. Rev. Stat. § 6-1-716

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

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

(B) Conspicuous posting of the notice on the website page of the individual or the commercial entity if the individual or the commercial entity maintains one; and
(C) Notification to major statewide media.
(2) Disclosure of breach. (a) An individual or a commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The individual or the commercial entity shall give notice as soon as possible to the affected Colorado resident unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.
(b) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a Colorado resident occurred or is likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets.
(c) Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and the law enforcement agency has notified the individual or commercial entity that conducts business in Colorado not to send notice required by this section. Notice required by this section shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation and has notified the individual or commercial entity that conducts business in Colorado that it is appropriate to send the notice required by this section.
(d) If an individual or commercial entity is required to notify more than one thousand Colorado residents of a breach of the security of the system pursuant to this section, the individual or commercial entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 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 paragraph (d) shall be construed to require the individual or commercial entity to provide to the consumer reporting agency the names or other personal information of breach notice recipients. This paragraph (d) shall not apply to a person who is subject to Title V of the federal “Gramm-Leach-Bliley Act”, 15 U.S.C. sec. 6801 et seq.
(3) Procedures deemed in compliance with notice requirements. (a) Under this section, an individual or a commercial entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information and whose procedures are otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notice requirements of this section if the individual or the commercial entity notifies affected Colorado customers in accordance with its policies in the event of a breach of security of the system.

(b) An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section.
(4) Violations. The attorney general may bring an action in law or equity to address violations of this section and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law.

VII. CONNECTICUT

Conn. Gen Stat. §§ 36a-701b, 4e-70

§ 36a-701b. Breach of security re computerized data containing personal information. Notice of breach. Provision of identity theft prevention services and identity theft mitigation services. Delay for criminal investigation. Means of notice. Unfair trade practice

(a) For purposes of this section, (1) “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; and (2) “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: (A) Social Security number; (B) driver's license number or state identification card number; or (C) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.
(b) (1) Any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall 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. Such notice shall be made without unreasonable delay but not later than ninety days after the discovery of such breach, unless a shorter time is required under federal law, subject to the provisions of subsection (d) of this section and the completion of an investigation by such person to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system. Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.
(2) If notice of a breach of security is required by subdivision (1) of this subsection:

(A) The person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the Attorney General; and
(B) The person who conducts business in this state, and who, in the ordinary course of such person's business, owns or licenses computerized data that includes personal information, shall offer to each resident whose personal information under subparagraph (A) of subdivision (4) of subsection (a) of section 38a-999b or subparagraph (A) of subdivision (2) of subsection (a) of this section was breached or is reasonably believed to have been breached, appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than twelve months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file.
(c) Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery, if the personal information of a resident of this state was breached or is reasonably believed to have been breached.
(d) Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after such law enforcement agency determines that notification will not compromise the criminal investigation and so notifies the person of such determination.
(e) Any notice to a resident, owner or licensee required by the provisions of this section may be provided by one of the following methods: (1) Written notice; (2) telephone notice; (3) electronic notice, provided such notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001; (4) substitute notice, provided such person demonstrates that the cost of providing notice in accordance with subdivision (1), (2) or (3) of this subsection would exceed two hundred fifty thousand dollars, that the affected class of subject persons to be notified exceeds five hundred thousand persons or 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.
(f) Any person that maintains such person's own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies, 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.
(g) Failure to comply with the requirements of this section shall constitute an unfair trade practice for purposes of section 42-110b and shall be enforced by the Attorney General.

Conn. Gen Stat. 4e-70

§ 4e-70. Requirements for state contractors who receive confidential information. Definitions. Minimum requirements. Prohibitions. Breach. Violation. Ban. Effect on other applicable laws

(a) As used in this section and section 4e-71:
(1) “Contractor” means an individual, business or other entity that is receiving confidential information from a state contracting agency or agent of the state pursuant to a written agreement to provide goods or services to the state.
(2) “State agency” means any agency with a department head, as defined in section 4-5.
(3) “State contracting agency” means any state agency disclosing confidential information to a contractor pursuant to a written agreement with such contractor for the provision of goods or services for the state.
(4) “Confidential information” means an individual's name, date of birth, mother's maiden name, motor vehicle operator's license number, Social Security number, employee identification number, employer or taxpayer identification number, alien registration number, government passport number, health insurance identification number, demand deposit account number, savings account number, credit card number, debit card number or unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation, personally identifiable information subject to 34 CFR 99, as amended from time to time and protected health information, as defined in 45 CFR 160.103, as amended from time to time. In addition, “confidential information” includes any information that a state contracting agency identifies as confidential to the contractor. “Confidential information” does not include information that may be lawfully obtained from publicly available sources or from federal, state, or local government records that are lawfully made available to the general public.
(5) “Confidential information breach” means an instance where an unauthorized person or entity accesses confidential information that is subject to or otherwise used in conjunction with any part of a written agreement with a state contracting agency in any manner, including, but not limited to, the following occurrences: (A) Any confidential information that is not encrypted or secured by any other method or technology that renders the personal information unreadable or unusable is misplaced, lost, stolen or subject to unauthorized access; (B) one or more third parties have accessed, or taken control or possession of, without prior written authorization from the state, (i) any confidential information that is not encrypted or protected, or (ii) any encrypted or protected confidential information together with the confidential process or key that is capable of compromising the integrity of the confidential information; or (C) there is a substantial risk of

identity theft or fraud of the client of the state contracting agency, the contractor, the state contracting agency or the state.
(b) Except as provided in section 4e-71, every written agreement that authorizes a state contracting agency to share confidential information with a contractor shall require the contractor to, at a minimum, do the following:
(1) At its own expense, protect from a confidential information breach any and all confidential information that it comes to possess or control, wherever and however stored or maintained;
(2) Implement and maintain a comprehensive data-security program for the protection of confidential information. The safeguards contained in such program shall be consistent with and comply with the safeguards for protection of confidential information as set forth in all applicable federal and state law and written policies of the state contained in the agreement. Such data-security program shall include, but not be limited to, the following: (A) A security policy for contractor employees related to the storage, access and transportation of data containing confidential information; (B) reasonable restrictions on access to records containing confidential information, including the area where such records are kept and secure passwords for electronically stored records; (C) a process for reviewing policies and security measures at least annually; and (D) an active and ongoing employee security awareness program that is mandatory for all employees who may have access to confidential information provided by the state contracting agency that, at a minimum, advises such employees of the confidentiality of the information, the safeguards required to protect the information and any applicable civil and criminal penalties for noncompliance pursuant to state and federal law;
(3) Limit access to confidential information to authorized contractor employees and authorized agents of the contractor, for authorized purposes as necessary for the completion of the contracted services or provision of the contracted goods;
(4) Maintain all electronic data constituting confidential information obtained from state contracting agencies: (A) In a secure server; (B) on secure drives; (C) behind firewall protections and monitored by intrusion detection software; (D) in a manner where access is restricted to authorized employees and their authorized agents; and (E) as otherwise required under state and federal law;
(5) Implement, maintain and update security and breach investigation procedures that are appropriate given the nature of the information disclosed and that are reasonably designed to protect the confidential information from unauthorized access, use, modification, disclosure, manipulation or destruction;
(6) Notify the state contracting agency and the Attorney General as soon as practical after the contractor becomes aware of or has reason to believe that any confidential information that the contractor possesses or controls has been subject to a confidential information breach;
(7) Immediately cease all use of the data provided by the state contracting agency or developed internally by the contractor pursuant to a written agreement with the state if so directed by the state contracting agency; and
(8) In accordance with the proposed timetable established pursuant to subdivision (1) of subsection (e) of this section, submit to the office of the Attorney General and the state contracting agency either (A) a report detailing the breach or suspected breach, including a plan to mitigate the effects of any breach and specifying the steps taken to ensure future breaches do not occur, or (B) a report detailing why, upon further investigation, the contractor believes no breach has occurred. Any report submitted under this subdivision shall be considered information given in confidence

and not required by statute, under subparagraph (B) of subdivision (5) of subsection (b) of section 1-210.
(c) A contractor shall not:
(1) Store data constituting confidential information on stand-alone computer or notebook hard disks or portable storage devices such as external or removable hard drives, flash cards, flash drives, compact disks or digital video disks, except as provided for in the agreement and including alternate measures of security assurance approved pursuant to section 4e-71; or
(2) Copy, reproduce or transmit data constituting confidential information, except as necessary for the completion of the contracted services or provision of the contracted goods.
(d) All copies of data constituting confidential information of any type, including, but not limited to, any modifications or additions to data that contain confidential information, are subject to the provisions of this section in the same manner as the original data.
(e) Except as provided in section 4e-71, every written agreement that authorizes a state contracting agency to share confidential information with a contractor shall:
(1) Include a proposed timetable for submittal to the office of the Attorney General and the state contracting agency either (A) a report detailing the breach or suspected breach, or (B) a report detailing why, upon further investigation, the contractor believes no breach has occurred; and
(2) Specify how the cost of any notification about, or investigation into, a confidential information breach is to be apportioned when the state contracting agency or contractor is the subject of such a breach.
(f) The notice required by subsection (b) of this section may be delayed (1) at the state contracting agency's sole discretion based on the report and, if applicable, the plan provided, or (2) if a law enforcement agency or intelligence agency notifies the contractor that such notification would impede a criminal investigation or jeopardize homeland or national security. If notice is delayed pursuant to this subsection, notification shall be given as soon as reasonably feasible by the contractor to the applicable state contracting agency.
(g) The Attorney General may investigate any violation of this section. If the Attorney General finds that a contractor has violated or is violating any provision of this section, the Attorney General may bring a civil action in the superior court for the judicial district of Hartford under this section in the name of the state against such contractor. Nothing in this section shall be construed to create a private right of action.
(h) If the confidential information or personally identifiable information, as defined in 34 CFR 99.3, that has been subject to a confidential information breach consists of education records, the contractor may be subject to a five-year ban from receiving access to such information imposed by the State Department of Education.
(i) The requirements of this section shall be in addition to the requirements of section 36a-701b and nothing in this section shall be construed to supersede a contractor's obligations pursuant to the Health Insurance Portability and Accountability Act of 1996 P.L. 104-191 (HIPAA), the Family Educational Rights and Privacy Act of 1974, 20 USC 1232g, (FERPA) or any other applicable federal or state law.

VIII. DELAWARE

Other Laws Relating to Commerce and Trade
CHAPTER 12B. COMPUTER SECURITY BREACHES [EFFECTIVE MAR. 14, 2018]

§ 12B-100 Protection of personal information [Effective Mar. 14, 2018]

Any person who conducts business in this State and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.

81 Del. Laws, c. 129, § 1.;

§ 12B-101 Definitions [Effective Mar. 14, 2018]

For purposes of this chapter:
(1) "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.
(2) "Determination of the breach of security'' means the point in time at which a person who owns, licenses, or maintains computerized data has sufficient evidence to conclude that a breach of security of such computerized data has taken place.
(3) "Encrypted'' means personal information that is rendered unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security.
(4) "Encryption key'' means the confidential key or process designed to render the encrypted personal information useable, readable, and decipherable.
(5) "Notice'' means any of the following:
a. Written notice.
b. Telephonic notice.
c. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 of Title 15 of the United States Code or if the person's primary means of communication with the resident is by electronic means.
d. Substitute notice, if the person required to provide notice under this chapter demonstrates that the cost of providing notice will exceed $75,000, or that the affected number of Delaware

residents to be notified exceeds 100,000 residents, or that the person does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:
1. Electronic notice if the person has email addresses for the members of the affected class of Delaware residents.
2. Conspicuous posting of the notice on the web site page of the person if the person maintains one.
3. Notice to major statewide media, including newspapers, radio, and television and publication on the major social media platforms of the person providing notice.
(6) "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.
(7)a. "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 health care 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.
b. "Personal information'' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely-distributed media.

75 Del. Laws, c. 61, § 1; 81 Del. Laws, c. 129, § 1.;

§ 12B-102 Disclosure of breach of security; notice [Effective Mar. 14, 2018]

(a) Any person who conducts business in this State and who owns or licenses computerized data that includes personal information shall provide notice of any breach of security following determination of the breach of security to any resident of this State whose personal information was breached or is reasonably believed to have been breached, 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.
(b) 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. For purposes of this subsection, "cooperation'' includes sharing with the owner or licensee information relevant to the breach.
(c) Notice required by subsection (a) of this section must be made without unreasonable delay but not later than 60 days after determination of the breach of security, except in the following situations:
(1) A shorter time is required under federal law.
(2) 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.
(3) When a person otherwise required by subsection (a) of this section 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 subsection (a) of this section to such residents as soon as practicable after the determination that the breach of security included the personal information of such residents, unless such person provides or has provided substitute notice in accordance with § 12B-101(5)d. of this title.
(d) If the affected number of Delaware residents to be notified exceeds 500 residents, the person required to provide notice shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the Attorney General.
(e) If the breach of security includes a Social Security number, the person shall offer to each resident, whose personal information, including Social Security number, was breached or is reasonably believed to have been breached, credit monitoring services at no cost to such resident for a period of 1 year. Such person shall provide all information necessary for such resident to enroll in such services and shall include information on how such resident can place a credit freeze on such resident's credit file. Such services are not required if, 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.
(f) In the case of a breach of security involving personal information defined in § 12B-101(7)a.5. of this title 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.

75 Del. Laws, c. 61, § 1; 81 Del. Laws, c. 129, § 1.;

§ 12B-103 Procedures deemed in compliance with security breach notice requirements [Effective Mar. 14, 2018]

(a) Under this chapter, 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.
(b) Under this chapter, a person that is regulated by state or federal law, including the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, as amended) and the Gramm Leach Bliley Act (15 U.S.C. § 6801 et seq., as amended) and that maintains procedures for a breach of security pursuant to the 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.

75 Del. Laws, c. 61, § 1; 81 Del. Laws, c. 129, § 1.;

§ 12B-104 Violations [Effective Mar. 14, 2018]

(a) Pursuant to the enforcement duties and powers of the Director of Consumer Protection of the Department of Justice under Chapter 25 of Title 29, 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. The provisions of this chapter are not exclusive and do not relieve a person subject to this chapter from compliance with all other applicable provisions of law.
(b) Nothing in this chapter may be construed to modify any right which a person may have at common law, by statute, or otherwise.

IX. DC

D.C. Code §§ 28- 3851 et seq.

§ 28-3852. Notification of security breach.

(a) Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and who discovers a breach of the security of the system, shall promptly notify any District of Columbia resident whose personal information was included in the breach. The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (d) of this section, and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
(b) Any person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own shall notify the owner or licensee of the information of any breach of the security of the system in the most expedient time possible following discovery.

(c) If any person or entity is required by subsection (a) or (b) of this section to notify more than 1,000 persons of a breach of security pursuant to this subsection, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by section 603(p) of the Fair Credit Reporting Act, approved October 26, 1970 (84 Stat. 1128; 15 U.S.C. § 1681a(p)), of the timing, distribution and content of the notices. Nothing in this subsection shall be construed to require the person to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients. This subsection shall not apply to a person or entity who is required to notify consumer reporting agencies of a breach pursuant to Title V of the Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1436; 15 U.S.C § 6801 *et seq*).
(d) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation but shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation.
(e) Notwithstanding subsection (a) of this section, a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this subchapter shall be deemed to be in compliance with the notification requirements of this section if the person or business provides notice, in accordance with its policies, reasonably calculated to give actual notice to persons to whom notice is otherwise required to be given under this subchapter. Notice under this section may be given by electronic mail if the person or entity's primary method of communication with the resident is by electronic means.
(f) A waiver of any provision of this subchapter shall be void and unenforceable.

§ 28-3852. Notification of security breach.

(a) Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and who discovers a breach of the security of the system, shall promptly notify any District of Columbia resident whose personal information was included in the breach. The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (d) of this section, and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
(b) Any person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own shall notify the owner or licensee of the information of any breach of the security of the system in the most expedient time possible following discovery.
(c) If any person or entity is required by subsection (a) or (b) of this section to notify more than 1,000 persons of a breach of security pursuant to this subsection, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by section 603(p) of the Fair Credit Reporting Act, approved October 26, 1970 (84 Stat. 1128; 15 U.S.C. § 1681a(p)), of the timing, distribution and content of the notices. Nothing in this subsection shall be construed to require the person to

provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients. This subsection shall not apply to a person or entity who is required to notify consumer reporting agencies of a breach pursuant to Title V of the Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1436; 15 U.S.C § 6801 *et seq*).
(d) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation but shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation.
(e) Notwithstanding subsection (a) of this section, a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this subchapter shall be deemed to be in compliance with the notification requirements of this section if the person or business provides notice, in accordance with its policies, reasonably calculated to give actual notice to persons to whom notice is otherwise required to be given under this subchapter. Notice under this section may be given by electronic mail if the person or entity's primary method of communication with the resident is by electronic means.
(f) A waiver of any provision of this subchapter shall be void and unenforceable.

X. FLORIDA

Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)

(2) Requirements for data security.**--**Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information.
(3) Notice to department of security breach.**--**
(a) A covered entity shall provide notice to the department of any breach of security affecting 500 or more individuals in this state. Such notice must be provided to the department as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred. A covered entity may receive 15 additional days to provide notice as required in subsection (4) if good cause for delay is provided in writing to the department within 30 days after determination of the breach or reason to believe a breach occurred.
(b) The written notice to the department 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.

(c) The covered entity must provide the following information to the department upon its request:
1. A police report, incident report, or computer forensics report.
2. A copy of the policies in place regarding breaches.
3. Steps that have been taken to rectify the breach.
(d) A covered entity may provide the department with supplemental information regarding a breach at any time.
(e) For a covered entity that is the judicial branch, the Executive Office of the Governor, the Department of Financial Services, or the Department of Agriculture and Consumer Services, in lieu of providing the written notice to the department, the covered entity may post the information described in subparagraphs (b)1.-4. on an agency-managed website.
(4) Notice to individuals of security breach.
(a) A covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized under paragraph (b) or waiver under paragraph (c).
(b) 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.
(c) Notwithstanding paragraph (a), 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. Such a determination must be documented in writing and maintained for at least 5 years. The covered entity shall provide the written determination to the department within 30 days after the determination.
(d) The notice to an affected individual shall be by one of the following methods:
1. Written notice sent to the mailing address of the individual in the records of the covered entity; or
2. E-mail notice sent to the e-mail address of the individual in the records of the covered entity.
(e) 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.
(f) A covered entity required to provide notice to an individual may provide substitute notice in lieu of direct notice if such direct notice is not feasible because the cost of providing notice would

exceed $250,000, because the affected individuals exceed 500,000 persons, or because the covered entity does not have an e-mail address or mailing address for the affected individuals. Such substitute notice shall include the following:
1. A conspicuous notice on the Internet website of the covered entity if the covered entity maintains a website; and
2. Notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside.
(g) 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. Under this paragraph, a covered entity that timely provides a copy of such notice to the department is deemed to be in compliance with the notice requirement in subsection (3).

XI. GEORGIA

Ga. Code §§ 10-1-910, -911, -912; § 46-5-214

§ 10-1-912. Notice of breach of security

(a) Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this Code section, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.
(b) Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own shall notify the information broker or data collector of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
(c) The notification required by this Code section may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation. The notification required by this Code section shall be made after the law enforcement agency determines that it will not compromise the investigation.
(d) In the event that an information broker or data collector discovers circumstances requiring notification pursuant to this Code section of more than 10,000 residents of this state at one time, the information broker or data collector shall also notify, without unreasonable delay, all consumer

reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by 15 U.S.C. Section 1681a, of the timing, distribution, and content of the notices.

§ 46-5-214. Notification required in the event of breach; procedures; violations

(a) In the event of a breach of a telephone record concerning a Georgia resident, the telecommunications company must provide notice to the Georgia resident immediately following discovery or notification of the breach if such breach is reasonably likely to cause quantifiable harm to the Georgia resident. The notice must be made in the most expedient manner 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 telephone record.
(b) Notwithstanding any provisions of this article to contrary, a telecommunications company 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 Code section shall be deemed to be in compliance with the notification requirements of this Code section if it notifies the individuals who are the subject of the notice in accordance with its policies in the event of a breach of the security of the system.
(c) The notice required by this Code section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this Code section shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.
(d) A violation of this Code section constitutes an unfair or deceptive practice in consumer transactions within the meaning of Part 2 of Article 15 of Chapter 1 of Title 10, the “Fair Business Practices Act of 1975.”

XII. GUAM

9 G.C.A. § 48.30

§ 48.30. Disclosure of Breach of Security of Computerized Personal Information by an Individual ***or*** Entity.

(a) General Rule. An individual *or* entity that owns *or* licenses computerized data that includes personal information *shall* disclose any breach of the security of the system following discovery *or* notification of the breach of the security of the system to any resident of Guam whose unencrypted and unredacted personal information was *or* is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, *or* the individual *or* entity reasonably believes has caused *or* will cause, identity theft *or* other fraud to any resident of Guam. *Except* as provided in

subsection (d) of this Section, o*r* in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the disclosure *shall* be made without unreasonable delay.
(b) Encrypted Information. An individual *or* entity must disclose the breach of the security of the system *if* encrypted information is accessed and acquired in an unencrypted form, *or if* the security breach involves a person with access to the encryption key and the individual *or* entity reasonably believes that such breach has caused *or* will cause identity theft *or* other fraud to any resident of Guam.
(c) An individual *or* entity that maintains computerized data that includes personal information that the individual *or* entity *does not* own or license *shall* notify the owner *or* licensee of the information of any breach of the security of the system as soon as practicable following discovery, *if* the personal information was, *or* if the entity reasonably believes was, accessed and acquired by an unauthorized person.
(d) 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. Notice required by this Section must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation *or* jeopardize national *or* homeland security.

§ 48.50. Violations.

(a) A violation of this Chapter that results in injury *or* loss to residents of Guam may be enforced by the Office of the Attorney General.
(b) *Except* as provided by § 48.40 of this Chapter, the Office of the Attorney General *shall* have exclusive authority to bring action and may obtain either actual damages for a violation of this Chapter *or* a civil penalty *not to exceed* One Hundred Fifty Thousand Dollars ($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.

XIII. HAWAII

§487N-2 Notice of security breach.

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

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

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

(d) The notice shall be clear and conspicuous. The notice shall include a description of the following:

(1) The incident in general terms;

(2) The type of personal information that was subject to the unauthorized access and acquisition;

(3) The general acts of the business or government agency to protect the personal information from further unauthorized access;

(4) A telephone number that the person may call for further information and assistance, if one exists; and

(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

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

(1) Written notice to the last available address the business or government agency has on record;

(2) Electronic mail notice, for those persons for whom a business or government agency has a valid electronic mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. section 7001;

(3) Telephonic notice, provided that contact is made directly with the affected persons; and

(4) Substitute notice, if the business or government agency demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of subject persons to be notified exceeds two hundred thousand, or if the business or government agency does not have sufficient contact information or consent to satisfy paragraph (1), (2), or (3), for only those affected persons without sufficient contact information or consent, or if the business or government agency is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

(A) Electronic mail notice when the business or government agency has an electronic mail address for the subject persons;

(B) Conspicuous posting of the notice on the website page of the business or government agency, if one is maintained; and

(C) Notification to major statewide media.

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

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

(1) A financial institution that is subject to the federal Interagency Guidance on Response Programs for Unauthorized Access to 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, 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.

[§487N-3] Penalties; civil action.

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

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

(c) The penalties provided in this section shall be cumulative to the remedies or penalties available under all other laws of this State. [L 2006, c 135, pt of §2]

XIV. IDAHO

Title 28 Commercial Transactions; Chapter 51 - Identity Theft

28-51-105. Disclosure of breach of security of computerized personal information by an agency, individual or a commercial entity.

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

When an agency becomes aware of a breach of the security of the system, it shall, within twenty-four (24) hours of such discovery, notify the office of the Idaho attorney general. Nothing contained in this section relieves a state agency's responsibility to report a security breach to the office of the chief information officer within the department of administration, pursuant to the Idaho technology authority policies.

Any governmental employee who intentionally discloses personal information not subject to disclosure otherwise allowed by law is guilty of a misdemeanor and, upon conviction thereof, shall be punished by a fine of not more than two thousand dollars ($2,000), or by imprisonment in the county jail for a period of not more than one (1) year, or both.

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

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

28-51-106. Procedures deemed in compliance with security breach requirements.

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

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

commercial entity complies with the maintained procedures when a breach of the security of the system occurs.

Title 28 Commercial Transactions; Chapter 51 – Identity Theft

28-51-107. Violations.

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

XV. ILLINOIS

(815 ILCS 530/10)

Sec. 10. Notice of breach.

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

(b) 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. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

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

(c) For purposes of this Section, notice to consumers may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is

consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the data collector

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

(d) Notwithstanding any other subsection in this Section, a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

(Source: P.A. 99-503, eff. 1-1-17; 100-201, eff. 8-18-17.)

(815 ILCS 530/12)

Sec. 12. Notice of breach; State agency.

(a) Any State agency that collects personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data or written material following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to information as follows:

(1) With respect to personal information defined in Section 5 in paragraph (1) of the definition of "personal information":

(i) the toll-free numbers and addresses for consumer reporting agencies;

(ii) the toll-free number, address, and website address for the Federal Trade Commission; and

(iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

(2) With respect to personal information as 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.

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

(b) For purposes of this Section, notice to residents may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

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

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

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

(e) Notice to Attorney General. Any State agency that suffers a single breach of the security of the data concerning the personal information of more than 250 Illinois residents shall provide notice to the Attorney General of the breach, including:

(A) The types of personal information compromised in the breach.

(B) The number of Illinois residents affected by such incident at the time of notification.

(C) Any steps the State agency has taken or plans to take relating to notification of the breach to consumers.

(D) The date and timeframe of the breach, if known at the time notification is provided.

Such notification must be made within 45 days of the State agency's discovery of the security breach or when the State agency provides any notice to consumers required by this Section, whichever is sooner, unless the State agency has good cause for reasonable delay to determine the scope of the breach and restore the integrity, security, and confidentiality of the data system, or when law enforcement requests in writing to withhold disclosure of some or all of the information required in the notification under this Section. If the date or timeframe of the breach is unknown at the time the notice is sent to the Attorney General, the State agency shall send the Attorney General the date or timeframe of the breach as soon as possible.

(Source: P.A. 99-503, eff. 1-1-17.)

(815 ILCS 530/15)

Sec. 15. Waiver. Any waiver of the provisions of this Act is contrary to public policy and is void and unenforceable.

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

(815 ILCS 530/20)

Sec. 20. Violation. A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.

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

(815 ILCS 530/25)

Sec. 25. Annual reporting. Any State agency that collects personal data and has had a breach of security of the system data or written material shall submit a report within 5 business days of the discovery or notification of the breach to the General Assembly listing the breaches and outlining any corrective measures that have been taken to prevent future breaches of the security of the system data or written material. Any State agency that has submitted a report under this Section shall submit an annual report listing all breaches of security of the system data or written materials and the corrective measures that have been taken to prevent future breaches.
(Source: P.A. 94-947, eff. 6-27-06.)

(815 ILCS 530/30)

Sec. 30. Safe disposal of information. Any State agency that collects personal data that is no longer needed or stored at the agency shall dispose of the personal data or written material it has collected in such a manner as to ensure the security and confidentiality of the material.
(Source: P.A. 94-947, eff. 6-27-06.)

(815 ILCS 530/40)

Sec. 40. Disposal of materials containing personal information; Attorney General.

(a) In this Section, "person" means: a natural person; a corporation, partnership, association, or other legal entity; a unit of local government or any agency, department, division, bureau, board, commission, or committee thereof; or the State of Illinois or any constitutional officer, agency, department, division, bureau, board, commission, or committee thereof.

(b) A person must dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable. Proper disposal methods include, but are not limited to, the following:

(1) Paper documents containing personal information may be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed.

(2) Electronic media and other non-paper media containing personal information may be destroyed or erased so that personal information cannot practicably be read or reconstructed.

(c) Any person disposing of materials containing personal information may contract with a third party to dispose of such materials in accordance with this Section. Any third party that contracts with a person to dispose of materials containing personal information must implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation, and disposal of materials containing personal information.

(d) 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. The

Attorney General may impose a civil penalty after notice to the person accused of violating this Section and an opportunity for that person to be heard in the matter. The Attorney General may file a civil action in the circuit court to recover any penalty imposed under this Section.

(e) In addition to the authority to impose a civil penalty under subsection (d), the Attorney General may bring an action in the circuit court to remedy a violation of this Section, seeking any appropriate relief.

(f) A financial institution under 15 U.S.C. 6801 et. seq. or any person subject to 15 U.S.C. 1681w is exempt from this Section.

(Source: P.A. 97-483, eff. 1-1-12.)

XVI. INDIANA

Ind. Code §§ 4-1-11 *et seq.*, 24-4.9 *et seq.*

4-1-11-5 State agency that owns or licenses computerized data; notice of breach

Sec. 5. (a) Any state agency that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system following discovery or notification of the breach to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

(b) The disclosure of a breach of the security of the system shall be made:

(1) without unreasonable delay; and

(2) consistent with:

(A) the legitimate needs of law enforcement, as described in section 7 of this chapter; and

(B) any measures necessary to:

(i) determine the scope of the breach; and

(ii) restore the reasonable integrity of the data system.

4-1-11-6 State agency that maintains computerized data; notice of breach

Sec. 6. (a) This section applies to a state agency that maintains computerized data that includes personal information that the state agency does not own.

(b) If personal information was or is reasonably believed to have been acquired by an unauthorized person, the state agency shall notify the owner or licensee of the information of a breach of the security of the system immediately following discovery. The agency shall provide the notice to state residents as required under section 5 of this chapter.

4-1-11-8 Manner of notice

Sec. 8. Except as provided in section 9 of this chapter, a state agency may provide the notice required under this chapter:

(1) in writing; or

(2) by electronic mail, if the individual has provided the state agency with the individual's electronic mail address.

IC 24-4.9-3-1

24-4.9-3-1 Duty of data base owner to disclose breach

Sec. 1. (a) Except as provided in section 4(c), 4(d), and 4(e) of this chapter, after discovering or being notified of a breach of the security of data, the data base owner shall disclose the breach to an Indiana resident whose:
(1) unencrypted personal information was or may have been acquired by an unauthorized person; or
(2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key;
if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident.
(b) A data base owner required to make a disclosure under subsection (a) to more than one thousand (1,000) consumers shall also disclose to each consumer reporting agency (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system.
(c) If a data base owner makes a disclosure described in subsection (a), the data base owner shall also disclose the breach to the attorney general.

24-4.9-3-3.5 Exceptions; reasonable procedures to protect personal information

Sec. 3.5. (a) Except as provided in subsection (b), this section does not apply to a data base owner that maintains its own data security procedures as part of an information privacy, security policy, or compliance plan under:
(1) the federal USA PATRIOT Act (P.L. 107-56);
(2) Executive Order 13224;
(3) the federal Driver's Privacy Protection Act (18 U.S.C. 2721 et seq.);
(4) the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(5) the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or
(6) the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191);
if the data base owner'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 data base owner and the data base owner complies with the data base owner's information privacy, security policy, or compliance plan.
(b) This section applies to a current or former health care provider (as defined by IC 4-6-14-2) who is a data base owner or former data base owner:
(1) to which an exemption under subsection (a)(6) applies or applied; and

(2) whose information privacy, security policy, or compliance plan:
(A) does not require the data base owner or former data base owner to maintain and implement reasonable procedures; or
(B) is not implemented by the data base owner or former data base owner;
to ensure that the personal information described in subsection (a), including health records (as defined by IC 4-6-14-2.5), is protected and safeguarded from unlawful use or disclosure after the data base owner or former data base owner ceases to be a covered entity under the federal Health Insurance Portability and Accountability Act (P.L. 104-191).
(c) A data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.
(d) A data base owner shall not dispose of or abandon records or documents containing unencrypted and unredacted personal information of Indiana residents without shredding, incinerating, mutilating, erasing, or otherwise rendering the personal information illegible or unusable.
(e) A person that knowingly or intentionally fails to comply with any provision of this section commits a deceptive act that is actionable only by the attorney general under this section.
(f) The attorney general may bring an action under this section to obtain any or all of the following:
(1) An injunction to enjoin further violations of this section.
(2) A civil penalty of not more than five thousand dollars ($5,000) per deceptive act.
(3) The attorney general's reasonable costs in:
(A) the investigation of the deceptive act; and
(B) maintaining the action.
(g) A failure to comply with subsection (c) or (d) in connection with related acts or omissions constitutes one (1) deceptive act.

XVII. IOWA

Iowa Code §§ 715C.1, 715C.2

715C.2. Security breach--notification requirements--remedies

1. Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security, or receipt of notification under subsection 2, to any consumer whose personal information was included in the information that was breached. The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection 3, and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.

2. 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.
3. 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.
4. For purposes of this section, notification to the consumer may be provided by one of the following methods:
a. Written notice to the last available address the person has in the person's records.
b. Electronic notice if the person's customary method of communication with the consumer is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in chapter 554D and the federal Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001.
c. 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.
5. 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.
6. Notwithstanding subsection 1, notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years.
7. This section does not apply to any of the following:
a. 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.

b. 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.
c. A person who is subject to and complies with regulations promulgated pursuant to Tit. V of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6801-6809.
8. Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security requiring notification to more than five hundred residents of this state pursuant to this section shall give written notice of the breach of security following discovery of such breach of security, or receipt of notification under subsection 2, to the director of the consumer protection division of the office of the attorney general within five business days after giving notice of the breach of security to any consumer pursuant to this section.
9. a. A violation of this chapter is an unlawful practice pursuant to section 714.16 and, in addition to the remedies provided to the attorney general pursuant to section 714.16, subsection 7, 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.
b. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under the law.

XVIII. KANSAS

50-7a02. Security breach; requirements.

(a) A person that conducts business in this state, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information shall, when it becomes aware of any breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information has occurred or is reasonably likely to occur, the person or government, governmental subdivision or agency shall give notice as soon as possible to the affected Kansas resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.
(b) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the data following discovery of a breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.
(c) Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by this section shall be made in

good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.
(d) Notwithstanding any other provision in this section, an individual or a commercial entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the individual or the commercial entity notifies affected consumers in accordance with its policies in the event of a breach of security of the system.
(e) An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section. This section does not relieve an individual or a commercial entity from a duty to comply with other requirements of state and federal law regarding the protection and privacy of personal information.
(f) In the event that a person discovers circumstances requiring notification pursuant to this section of more than 1,000 consumers at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution and content of the notices.
(g) For violations of this section, except as to insurance companies licensed to do business in this state, the attorney general is empowered to bring an action in law or equity to address violations of this section and for other relief that may be appropriate. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law.
(h) For violations of this section by an insurance company licensed to do business in this state, the insurance commissioner shall have the sole authority to enforce the provisions of this section.

XIX. KENTUCKY

365.732 Notification to affected persons of computer security breach involving their unencrypted personally identifiable information

(1) As used in this section, unless the context otherwise requires:
(a) “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;

(b) “Information holder” means any person or business entity that conducts business in this state; and
(c) “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.
(2) Any information holder shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of Kentucky whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (4) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
(3) Any information holder that maintains computerized data that includes personally identifiable information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data as soon as reasonably practicable following discovery, if the personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person.
(4) 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.
(5) For purposes of this section, notice may be provided by one (1) of the following methods:
(a) Written notice;
(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. sec. 7001; or
(c) Substitute notice, if the 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.
(6) Notwithstanding subsection (5) of this section, an information holder that maintains its own notification procedures as part of an information security policy for the treatment of personally identifiable information, and is otherwise consistent with the timing requirements of this section, shall be deemed to be in compliance with the notification requirements of this section, if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.
(7) If a person discovers circumstances requiring notification pursuant to this section of more than one thousand (1,000) persons at one (1) time, the person shall also notify, without unreasonable

delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 1681a, of the timing, distribution, and content of the notices.
(8) The provisions of this section and the requirements for nonaffiliated third parties in KRS Chapter 61 shall not apply to any person who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended, or the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended, or any agency of the Commonwealth of Kentucky or any of its local governments or political subdivisions.

61.931 Definitions for KRS 61.931 to 61.934

As used in KRS 61.931 to 61.934:
(1) “Agency” means:
(a) The executive branch of state government of the Commonwealth of Kentucky;
(b) Every county, city, municipal corporation, urban-county government, charter county government, consolidated local government, and unified local government;
(c) Every organizational unit, department, division, branch, section, unit, office, administrative body, program cabinet, bureau, board, commission, committee, subcommittee, ad hoc committee, council, authority, public agency, instrumentality, interagency body, special purpose governmental entity, or public corporation of an entity specified in paragraph (a) or (b) of this subsection or created, established, or controlled by an entity specified in paragraph (a) or (b) of this subsection;
(d) Every public school district in the Commonwealth of Kentucky; and
(e) Every public institution of postsecondary education, including every public university in the Commonwealth of Kentucky and public college of the entire Kentucky Community and Technical College System;
(2) “Commonwealth Office of Technology” means the office established by KRS 42.724;
(3) “Encryption” means the conversion of data using technology that:
(a) Meets or exceeds the level adopted by the National Institute of Standards Technology as part of the Federal Information Processing Standards: and
(b) Renders the data indecipherable without the associated cryptographic key to decipher the data;
(4) “Law enforcement agency” means any lawfully organized investigative agency, sheriff's office, police unit, or police force of federal, state, county, urban-county government, charter county, city, consolidated local government, unified local government, or any combination of these entities, responsible for the detection of crime and the enforcement of the general criminal federal and state laws;
(5) “Nonaffiliated third party” means any person that:
(a) Has a contract or agreement with an agency; and
(b) Receives personal information from the agency pursuant to the contract or agreement;
(6) “Personal information” means an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
(a) An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
(b) A Social Security number;

(c) A taxpayer identification number that incorporates a Social Security number;
(d) A driver's license number, state identification card number, or other individual identification number issued by any agency;
(e) A passport number or other identification number issued by the United States government; or
(f) Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g;
(7) (a) "Public record or record," as established by KRS 171.410, means all books, papers, maps, photographs, cards, tapes, disks, diskettes, recordings, and other documentary materials, regardless of physical form or characteristics, which are prepared, owned, used, in the possession of, or retained by a public agency.
(b) "Public record" does not include any records owned by a private person or corporation that are not related to functions, activities, programs, or operations funded by state or local authority;
(8) "Reasonable security and breach investigation procedures and practices" means data security procedures and practices developed in good faith and set forth in a written security information policy; and
(9) (a) "Security breach" means:
1. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals; or
2. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted records or data containing personal information along with the confidential process or key to unencrypt the records or data that compromises or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals.
(b) "Security breach" does not include the good-faith acquisition of personal information by an employee, agent, or nonaffiliated third party of the agency for the purposes of the agency if the personal information is used for a purpose related to the agency and is not subject to unauthorized disclosure.

61.932 Personal information security and breach investigation procedures and practices for certain public agencies and nonaffiliated third parties

(1) (a) An agency or nonaffiliated third party that maintains or otherwise possesses personal information, regardless of the form in which the personal information is maintained, shall implement, maintain, and update security procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches.
(b) Reasonable security and breach investigation procedures and practices established and implemented by organizational units of the executive branch of state government shall be in accordance with relevant enterprise policies established by the Commonwealth Office of Technology. Reasonable security and breach investigation procedures and practices established and implemented by units of government listed under KRS 61.931(1)(b) and (c) that are not organizational units of the executive branch of state government shall be in accordance with

policies established by the Department for Local Government. The Department for Local Government shall consult with public entities as defined in KRS 65.310 in the development of policies establishing reasonable security and breach investigation procedures and practices for units of local government pursuant to this subsection. Reasonable security and breach investigation procedures and practices established and implemented by public school districts listed under KRS 61.931(1)(d) shall be in accordance with administrative regulations promulgated by the Kentucky Board of Education. Reasonable security and breach investigation procedures and practices established and implemented by educational entities listed under KRS 61.931(1)(e) shall be in accordance with policies established by the Council on Postsecondary Education. The Commonwealth Office of Technology shall, upon request of an agency, make available technical assistance for the establishment and implementation of reasonable security and breach investigation procedures and practices.

(c) 1. If an agency is subject to any additional requirements under the Kentucky Revised Statutes or under federal law, protocols, or agreements relating to the protection and privacy of personal information, the agency shall comply with these additional requirements, in addition to the requirements of KRS 61.931 to 61.934.

2. If a nonaffiliated third party is required by federal law or regulation to conduct security breach investigations or to make notifications of security breaches, or both, as a result of the nonaffiliated third party's unauthorized disclosure of one (1) or more data elements of personal information that is the same as one (1) or more of the data elements of personal information listed in KRS 61.931(6)(a) to (f), the nonaffiliated third party shall meet the requirements of KRS 61.931 to 61.934 by providing to the agency a copy of any and all reports and investigations relating to such security breach investigations or notifications that are required to be made by federal law or regulations. This subparagraph shall not apply if the security breach includes the unauthorized disclosure of data elements that are not covered by federal law or regulation but are listed in KRS 61.931(6)(a) to (f).

(2) (a) For agreements executed or amended on or after January 1, 2015, any agency that contracts with a nonaffiliated third party and that discloses personal information to the nonaffiliated third party shall require as part of that agreement that the nonaffiliated third party implement, maintain, and update security and breach investigation procedures that are appropriate to the nature of the information disclosed, that are at least as stringent as the security and breach investigation procedures and practices referenced in subsection (1)(b) of this section, and that are reasonably designed to protect the personal information from unauthorized access, use, modification, disclosure, manipulation, or destruction.

(b) 1. A nonaffiliated third party that is provided access to personal information by an agency, or that collects and maintains personal information on behalf of an agency shall notify the agency in the most expedient time possible and without unreasonable delay but within seventy-two (72) hours of determination of a security breach relating to the personal information in the possession of the nonaffiliated third party. The notice to the agency shall include all information the nonaffiliated third party has with regard to the security breach at the time of notification. Agreements referenced in paragraph (a) of this subsection shall specify how the cost of the notification and investigation requirements under KRS 61.933 are to be apportioned when a security breach is suffered by the agency or nonaffiliated third party.

2. The notice required by subparagraph 1. of this paragraph may be delayed if a law enforcement agency notifies the nonaffiliated third party that notification will impede a criminal investigation or jeopardize homeland or national security. If notice is delayed pursuant to this subparagraph, notification shall be given as soon as reasonably feasible by the nonaffiliated third party to the agency with which the nonaffiliated third party is contracting. The agency shall then record the notification in writing on a form developed by the Commonwealth Office of Technology that the notification will not impede a criminal investigation and will not jeopardize homeland or national security. The Commonwealth Office of Technology shall promulgate administrative regulations under KRS 61.931 to 61.934 regarding the content of the form.

61.932 Personal information security and breach investigation procedures and practices for certain public agencies and nonaffiliated third parties

(1) (a) An agency or nonaffiliated third party that maintains or otherwise possesses personal information, regardless of the form in which the personal information is maintained, shall implement, maintain, and update security procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches.
(b) Reasonable security and breach investigation procedures and practices established and implemented by organizational units of the executive branch of state government shall be in accordance with relevant enterprise policies established by the Commonwealth Office of Technology. Reasonable security and breach investigation procedures and practices established and implemented by units of government listed under KRS 61.931(1)(b) and (c) that are not organizational units of the executive branch of state government shall be in accordance with policies established by the Department for Local Government. The Department for Local Government shall consult with public entities as defined in KRS 65.310 in the development of policies establishing reasonable security and breach investigation procedures and practices for units of local government pursuant to this subsection. Reasonable security and breach investigation procedures and practices established and implemented by public school districts listed under KRS 61.931(1)(d) shall be in accordance with administrative regulations promulgated by the Kentucky Board of Education. Reasonable security and breach investigation procedures and practices established and implemented by educational entities listed under KRS 61.931(1)(e) shall be in accordance with policies established by the Council on Postsecondary Education. The Commonwealth Office of Technology shall, upon request of an agency, make available technical assistance for the establishment and implementation of reasonable security and breach investigation procedures and practices.
(c) 1. If an agency is subject to any additional requirements under the Kentucky Revised Statutes or under federal law, protocols, or agreements relating to the protection and privacy of personal information, the agency shall comply with these additional requirements, in addition to the requirements of KRS 61.931 to 61.934.
2. If a nonaffiliated third party is required by federal law or regulation to conduct security breach investigations or to make notifications of security breaches, or both, as a result of the nonaffiliated third party's unauthorized disclosure of one (1) or more data elements of personal information that is the same as one (1) or more of the data elements of personal information listed in KRS 61.931(6)(a) to (f), the nonaffiliated third party shall meet the requirements of KRS 61.931 to

61.934 by providing to the agency a copy of any and all reports and investigations relating to such security breach investigations or notifications that are required to be made by federal law or regulations. This subparagraph shall not apply if the security breach includes the unauthorized disclosure of data elements that are not covered by federal law or regulation but are listed in KRS 61.931(6)(a) to (f).
(2) (a) For agreements executed or amended on or after January 1, 2015, any agency that contracts with a nonaffiliated third party and that discloses personal information to the nonaffiliated third party shall require as part of that agreement that the nonaffiliated third party implement, maintain, and update security and breach investigation procedures that are appropriate to the nature of the information disclosed, that are at least as stringent as the security and breach investigation procedures and practices referenced in subsection (1)(b) of this section, and that are reasonably designed to protect the personal information from unauthorized access, use, modification, disclosure, manipulation, or destruction.
(b) 1. A nonaffiliated third party that is provided access to personal information by an agency, or that collects and maintains personal information on behalf of an agency shall notify the agency in the most expedient time possible and without unreasonable delay but within seventy-two (72) hours of determination of a security breach relating to the personal information in the possession of the nonaffiliated third party. The notice to the agency shall include all information the nonaffiliated third party has with regard to the security breach at the time of notification. Agreements referenced in paragraph (a) of this subsection shall specify how the cost of the notification and investigation requirements under KRS 61.933 are to be apportioned when a security breach is suffered by the agency or nonaffiliated third party.
2. The notice required by subparagraph 1. of this paragraph may be delayed if a law enforcement agency notifies the nonaffiliated third party that notification will impede a criminal investigation or jeopardize homeland or national security. If notice is delayed pursuant to this subparagraph, notification shall be given as soon as reasonably feasible by the nonaffiliated third party to the agency with which the nonaffiliated third party is contracting. The agency shall then record the notification in writing on a form developed by the Commonwealth Office of Technology that the notification will not impede a criminal investigation and will not jeopardize homeland or national security. The Commonwealth Office of Technology shall promulgate administrative regulations under KRS 61.931 to 61.934 regarding the content of the form.

61.933 Notification of personal information security breach; investigation; notice to affected individuals of result of investigation; personal information not subject to requirements; injunctive relief by Attorney General

(1) (a) Any agency that collects, maintains, or stores personal information that determines or is notified of a security breach relating to personal information collected, maintained, or stored by the agency or by a nonaffiliated third party on behalf of the agency shall as soon as possible, but within seventy-two (72) hours of determination or notification of the security breach:
1. Notify the commissioner of the Kentucky State Police, the Auditor of Public Accounts, and the Attorney General. In addition, an agency shall notify the secretary of the Finance and Administration Cabinet or his or her designee if an agency is an organizational unit of the executive branch of state government; notify the commissioner of the Department for Local

Government if the agency is a unit of government listed in KRS 61.931(1)(b) or (c) that is not an organizational unit of the executive branch of state government; notify the commissioner of the Kentucky Department of Education if the agency is a public school district listed in KRS 61.931(1)(d); and notify the president of the Council on Postsecondary Education if the agency is an educational entity listed under KRS 61.931(1)(e). Notification shall be in writing on a form developed by the Commonwealth Office of Technology. The Commonwealth Office of Technology shall promulgate administrative regulations under KRS 61.931 to 61.934 regarding the contents of the form; and

2. Begin conducting a reasonable and prompt investigation in accordance with the security and breach investigation procedures and practices referenced in KRS 61.932(1)(b) to determine whether the security breach has resulted in or is likely to result in the misuse of the personal information.

(b) Upon conclusion of the agency's investigation:

1. If the agency determined that a security breach has occurred and that the misuse of personal information has occurred or is reasonably likely to occur, the agency shall:

a. Within forty-eight (48) hours of completion of the investigation, notify in writing all officers listed in paragraph (a)1. of this subsection, and the commissioner of the Department for Libraries and Archives, unless the provisions of subsection (3) of this section apply;

b. Within thirty-five (35) days of providing the notifications required by subdivision a. of this subparagraph, notify all individuals impacted by the security breach as provided in subsection (2) of this section, unless the provisions of subsection (3) of this section apply; and

c. If the number of individuals to be notified exceeds one thousand (1,000), the agency shall notify, at least seven (7) days prior to providing notice to individuals under subdivision b. of this subparagraph, the Commonwealth Office of Technology if the agency is an organizational unit of the executive branch of state government, the Department for Local Government if the agency is a unit of government listed under KRS 61.931(1)(b) or (c) that is not an organizational unit of the executive branch of state government, the Kentucky Department of Education if the agency is a public school district listed under KRS 61.931(1)(d), or the Council on Postsecondary Education if the agency is an educational entity listed under KRS 61.931(1)(e); and notify all consumer credit reporting agencies included on the list maintained by the Office of the Attorney General that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. sec. 1681a(p), of the timing, distribution, and content of the notice; or

2. If the agency determines that the misuse of personal information has not occurred and is not likely to occur, the agency is not required to give notice, but shall maintain records that reflect the basis for its decision for a retention period set by the State Archives and Records Commission as established by KRS 171.420. The agency shall notify the appropriate entities listed in paragraph (a)1. of this subsection that the misuse of personal information has not occurred.

(2) (a) The provisions of this subsection establish the requirements for providing notice to individuals under subsection (1)(b)1.b. of this section. Notice shall be provided as follows:

1. Conspicuous posting of the notice on the Web site of the agency;

2. Notification to regional or local media if the security breach is localized, and also to major statewide media if the security breach is widespread, including broadcast media, such as radio and television; and

3. Personal communication to individuals whose data has been breached using the method listed in subdivision a., b., or c. of this subparagraph that the agency believes is most likely to result in actual notification to those individuals, if the agency has the information available:
a. In writing, sent to the most recent address for the individual as reflected in the records of the agency;
b. By electronic mail, sent to the most recent electronic mail address for the individual as reflected in the records of the agency, unless the individual has communicated to the agency in writing that they do not want email notification; or
c. By telephone, to the most recent telephone number for the individual as reflected in the records of the agency.
(b) The notice shall be clear and conspicuous, and shall include:
1. To the extent possible, a description of the categories of information that were subject to the security breach, including the elements of personal information that were or were believed to be acquired;
2. Contact information for the notifying agency, including the address, telephone number, and toll-free number if a toll-free number is maintained;
3. A description of the general acts of the agency, excluding disclosure of defenses used for the protection of information, to protect the personal information from further security breach; and
4. The toll-free numbers, addresses, and Web site addresses, along with a statement that the individual can obtain information from the following sources about steps the individual may take to avoid identity theft, for:
a. The major consumer credit reporting agencies;
b. The Federal Trade Commission; and
c. The Office of the Kentucky Attorney General.
(c) The agency providing notice pursuant to this subsection shall cooperate with any investigation conducted by the agencies notified under subsection (1)(a) of this section and with reasonable requests from the Office of Consumer Protection of the Office of the Attorney General, consumer credit reporting agencies, and recipients of the notice, to verify the authenticity of the notice.
(3) (a) The notices required by subsection (1) of this section shall not be made if, after consultation with a law enforcement agency, the agency receives a written request from a law enforcement agency for a delay in notification because the notice may impede a criminal investigation. The written request may apply to some or all of the required notifications, as specified in the written request from the law enforcement agency. Upon written notification from the law enforcement agency that the criminal investigation has been completed, or that the sending of the required notifications will no longer impede a criminal investigation, the agency shall send the notices required by subsection (1)(b)1. of this section.
(b) The notice required by subsection (1)(b)1.b. of this section may be delayed if the agency determines that measures necessary to restore the reasonable integrity of the data system cannot be implemented within the timeframe established by subsection (1)(b)1.b. of this section, and the delay is approved in writing by the Office of the Attorney General. If notice is delayed pursuant to this subsection, notice shall be made immediately after actions necessary to restore the integrity of the data system have been completed.
(4) Any waiver of the provisions of this section is contrary to public policy and shall be void and unenforceable.

(5) This section shall not apply to:
(a) Personal information that has been redacted;
(b) Personal information disclosed to a federal, state, or local government entity, including a law enforcement agency or court, or their agents, assigns, employees, or subcontractors, to investigate or conduct criminal investigations and arrests or delinquent tax assessments, or to perform any other statutory duties and responsibilities;
(c) Personal information that is publicly and lawfully made available to the general public from federal, state, or local government records;
(d) Personal information that an individual has consented to have publicly disseminated or listed; or
(e) Any document recorded in the records of either a county clerk or circuit clerk of a county, or in the records of a United States District Court.
(6) The Office of the Attorney General may bring an action in the Franklin Circuit Court against an agency or a nonaffiliated third party that is not an agency, or both, for injunctive relief, and for other legal remedies against a nonaffiliated third party that is not an agency to enforce the provisions of KRS 61.931 to 61.934. Nothing in KRS 61.931 to 61.934 shall create a private right of action.

XX. LOUISIANA

§3074. Disclosure upon breach in the security of personal information; notification requirements; exemption

A. Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall, following discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
B. Any agency or person that maintains computerized data that includes personal information that the agency or person does not own shall notify the owner or licensee of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of security of the system.
C. The notification required pursuant to Subsections A and B of this Section shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in Subsection D of this Section, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.
D. If a law enforcement agency determines that the notification required under this Section would impede a criminal investigation, such notification may be delayed until such law enforcement agency determines that the notification will no longer compromise such investigation.
E. Notification may be provided by one of the following methods:

(1) Written notification.
(2) Electronic notification, if the notification provided is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001.
(3) Substitute notification, if an agency or person demonstrates that the cost of providing notification would exceed two hundred fifty thousand dollars, or that the affected class of persons to be notified exceeds five hundred thousand, or the agency or person does not have sufficient contact information. Substitute notification shall consist of all of the following:
(a) E-mail notification when the agency or person has an e-mail address for the subject persons.
(b) Conspicuous posting of the notification on the Internet site of the agency or person, if an Internet site is maintained.
(c) Notification to major statewide media.
F. Notwithstanding Subsection E of this Section, an agency or person that maintains a notification procedure as part of its information security policy for the treatment of personal information which is otherwise consistent with the timing requirements of this Section shall be deemed to be in compliance with the notification requirements of this Section if the agency or person notifies subject persons in accordance with the policy and procedure in the event of a breach of security of the system.
G. Notification under this title[1] is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers
§3075. Recovery of damages
A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information.

XXI. MAINE

§1348. Security breach notice requirements

1. Notification to residents. The following provisions apply to notification to residents by information brokers and other persons.
A. If an information broker that maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the information broker shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person. [2005, c. 583, §6 (NEW); 2005, c. 583, §14 (AFF).]
B. If any other person who maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the person shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State if misuse of the personal

information has occurred or if it is reasonably possible that misuse will occur. [2005, c. 583, §6 (NEW); 2005, c. 583, §14 (AFF).]

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

[2005, c. 583, §14 (AFF); 2005, c. 583, §6 (RPR) .]

2. Notification to person maintaining personal information. A 3rd-party entity that maintains, on behalf of a person, computerized data that includes personal information that the 3rd-party entity does not own shall notify the person maintaining personal information of a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

[2005, c. 583, §7 (AMD); 2005, c. 583, §14 (AFF) .]

3. Delay of notification; criminal investigation by law enforcement. If, after the completion of an investigation required by subsection 1, 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.

[2009, c. 161, §3 (AMD); 2009, c. 161, §5 (AFF) .]

4. Notification to consumer reporting agencies. If a person discovers a breach of the security of the system that requires notification to more than 1,000 persons at a single time, the person shall also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 United States Code, Section 1681a(p). Notification must include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach.

[2005, c. 583, §8 (AMD); 2005, c. 583, §14 (AFF) .]

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

[2005, c. 583, §9 (AMD); 2005, c. 583, §14 (AFF) .]

XXII. MARYLAND [EFFECTIVE JANUARY 1, 2018]

Md. Code Com. Law §§ 14-3501 et seq., Md. State Govt. Code §§ 10-1301 to -1308

MD Code, Commercial Law, § 14-3501

§ 14**-**3501. Definitions

<Section effective Jan. 1, 2018. See, also, section 14-3501 effective until Jan. 1, 2018.>

(a) In this subtitle the following words have the meanings indicated.

(b)(1) “Business” means a sole proprietorship, partnership, corporation, association, or any other business entity, whether or not organized to operate at a profit.
(2) “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.
(c) “Encrypted” means the protection of data in electronic or optical form using an encryption technology that renders the data indecipherable without an associated cryptographic key necessary to enable decryption of the data.
(d) “Health information” means any information created by an entity covered by the federal Health Insurance Portability and Accountability Act of 1996 regarding an individual's medical history, medical condition, or medical treatment or diagnosis.
(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
(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.
(2) “Personal information” does not include:
(i) Publicly available information that is lawfully made available to the general public from federal, State, or local government records;
(ii) Information that an individual has consented to have publicly disseminated or listed; or
(iii) Information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act.[1]
(f) “Records” means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

§ 14-3504. Investigation, notification of breach of security

<Section effective until Jan. 1, 2018. See, also, section 14-3504 effective Jan. 1, 2018.>
(a) In this section:

(1) “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; and
(2) “Breach of the security of a system” does not include the good faith acquisition of personal information by an employee or agent of a business for the purposes of the business, provided that the personal information is not used or subject to further unauthorized disclosure.
(b)(1) A business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach.
(2) If, after the investigation is concluded, the business determines that misuse of the individual's personal information has occurred or is reasonably likely to occur as a result of a breach of the security of a system, the business shall notify the individual of the breach.
(3) Except as provided in subsection (d) of this section, the notification required under paragraph (2) of this subsection shall be given as soon as reasonably practicable after the business conducts the investigation required under paragraph (1) of this subsection.
(4) If after the investigation required under paragraph (1) of this subsection is concluded, the business determines that notification under paragraph (2) of this subsection is not required, the business shall maintain records that reflect its determination for 3 years after the determination is made.
(c)(1) A business that maintains computerized data that includes personal information that the business does not own or license shall notify the owner or licensee of the personal information of a breach of the security of a system if it is likely that the breach has resulted or will result in the misuse of personal information of an individual residing in the State.
(2) Except as provided in subsection (d) of this section, the notification required under paragraph (1) of this subsection shall be given as soon as reasonably practicable after the business discovers or is notified of the breach of the security of a system.
(3) A business that is required to notify an owner or licensee of personal information of a breach of the security of a system under paragraph (1) of this subsection shall share with the owner or licensee information relative to the breach.
(d)(1) The notification required under subsections (b) and (c) of this section 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.
(2) If notification is delayed under paragraph (1)(i) of this subsection, notification shall be given as soon as reasonably practicable after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security.
(e) The notification required under subsections (b) and (c) of this section may be given:
(1) By written notice sent to the most recent address of the individual in the records of the business;
(2) By electronic mail to the most recent electronic mail address of the individual in the records of the business, if:

(i) The individual has expressly consented to receive electronic notice; or
(ii) The business conducts its business primarily through Internet account transactions or the Internet;
(3) By telephonic notice, to the most recent telephone number of the individual in the records of the business; or
(4) By substitute notice as provided in subsection (f) of this section, if:
(i) The business demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of individuals to be notified exceeds 175,000; or
(ii) The business does not have sufficient contact information to give notice in accordance with item (1), (2), or (3) of this subsection.
(f) 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 Web site of the business, if the business maintains a Web site; and
(3) Notification to statewide media.
(g) The notification required under subsection (b) of this section 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 Web site 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.
(h) Prior to giving the notification required under subsection (b) of this section and subject to subsection (d) of this section, a business shall provide notice of a breach of the security of a system to the Office of the Attorney General.
(i) A waiver of any provision of this section is contrary to public policy and is void and unenforceable.
(j) Compliance with this section does not relieve a business from a duty to comply with any other requirements of federal law relating to the protection and privacy of personal information.

§ 14-3504. Investigation, notification of breach of security

<Section effective Jan. 1, 2018. See, also, section 14-3504 effective until Jan. 1, 2018.>
(a) In this section:
(1) “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; and

(2) “Breach of the security of a system” does not include the good faith acquisition of personal information by an employee or agent of a business for the purposes of the business, provided that the personal information is not used or subject to further unauthorized disclosure.
(b)(1) A business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach.
(2) If, after the investigation is concluded, the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the business shall notify the individual of the breach.
(3) Except as provided in subsection (d) of this section, the notification required under paragraph (2) of this subsection shall be given as soon as reasonably practicable, but not later than 45 days after the business concludes the investigation required under paragraph (1) of this subsection.
(4) If after the investigation required under paragraph (1) of this subsection is concluded, the business determines that notification under paragraph (2) of this subsection is not required, the business shall maintain records that reflect its determination for 3 years after the determination is made.
(c)(1) A business that maintains computerized data that includes personal information of an individual residing in the State that the business does not own or license, when it discovers or is notified of a breach of the security of a system, shall notify, as soon as practicable, the owner or licensee of the personal information of the breach of the security of a system.
(2) Except as provided in subsection (d) of this section, the notification required under paragraph (1) of this subsection shall be given as soon as reasonably practicable, but not later than 45 days after the business discovers or is notified of the breach of the security of a system.
(3) A business that is required to notify an owner or licensee of personal information of a breach of the security of a system under paragraph (1) of this subsection shall share with the owner or licensee information relative to the breach.
(d)(1) The notification required under subsections (b) and (c) of this section 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.
(2) If notification is delayed under paragraph (1)(i) of this subsection, notification shall be given as soon as reasonably practicable, but not later than 30 days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security.
(e) The notification required under subsection (b) of this section may be given:
(1) By written notice sent to the most recent address of the individual in the records of the business;
(2) By electronic mail to the most recent electronic mail address of the individual in the records of the business, if:
(i) The individual has expressly consented to receive electronic notice; or

(ii) The business conducts its business primarily through Internet account transactions or the Internet;
(3) By telephonic notice, to the most recent telephone number of the individual in the records of the business; or
(4) By substitute notice as provided in subsection (f) of this section, if:
(i) The business demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of individuals to be notified exceeds 175,000; or
(ii) The business does not have sufficient contact information to give notice in accordance with item (1), (2), or (3) of this subsection.
(f) 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 Web site of the business, if the business maintains a Web site; and
(3) Notification to statewide media.
(g) Except as provided in subsection (i) of this section, the notification required under subsection (b) of this section 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 Web site 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.
(h) Prior to giving the notification required under subsection (b) of this section and subject to subsection (d) of this section, a business shall provide notice of a breach of the security of a system to the Office of the Attorney General.
(i)(1) In the case of a breach of the security of a system involving personal information that permits access to an individual's e-mail account under § 14-3501(e)(1)(ii) of this subtitle and no other personal information under § 14-3501(e)(1)(i) of this subtitle, the business may comply with the notification requirement under subsection (b) of this section by providing the notification in electronic or other form that directs the individual whose personal information has been breached promptly to:
(i) Change the individual's password and security question or answer, as applicable; or
(ii) Take other steps appropriate to protect the e- mail account with the business and all other online accounts for which the individual uses the same user name or e-mail and password or security question or answer.
(2) Subject to paragraph (3) of this subsection, the notification provided under paragraph (1) of this subsection may be given to the individual by any method described in this section.

(3)(i) Except as provided in subparagraph (ii) of this paragraph, the notification provided under paragraph (1) of this subsection may not be given to the individual by sending notification by e-mail to the e-mail account affected by the breach.
(ii) The notification provided under paragraph (1) of this subsection may be given by a clear and conspicuous notice delivered to the individual online while the individual is connected to the affected e-mail account from an Internet Protocol address or online location from which the business knows the individual customarily accesses the account.
(j) A waiver of any provision of this section is contrary to public policy and is void and unenforceable.
(k) Compliance with this section does not relieve a business from a duty to comply with any other requirements of federal law relating to the protection and privacy of personal information.

Md. State Govt. Code §§ 10-1301 to -1308

MD Code, State Government, § 10-1301

§ 10-1301. Definitions

In general
(a) In this subtitle the following words have the meanings indicated.
Encryption
(b) “Encryption” means the protection of data in electronic or optical form, in storage or in transit, using a technology that:
(1) is certified to meet or exceed the level that has been adopted by the Federal Information Processing Standards issued by the National Institute of Standards and Technology; and
(2) renders such data indecipherable without an associated cryptographic key necessary to enable decryption of such data.
Personal information
(c) “Personal information” means an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:
(1) a Social Security number;
(2) a driver's license number, state identification card number, or other individual identification number issued by a unit;
(3) a passport number or other identification number issued by the United States government;
(4) an Individual Taxpayer Identification Number; or
(5) a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.
Reasonable security procedures and practices
(d) “Reasonable security procedures and practices” means data security procedures and practices developed, in good faith, and set forth in a written information security policy.
Records

(e) “Records” means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.
Unit
(f) “Unit” means:
(1) an executive agency, or a department, a board, a commission, an authority, a public institution of higher education, a unit or an instrumentality of the State; or
(2) a county, municipality, bi-county, regional, or multicounty agency, county board of education, public corporation or authority, or any other political subdivision of the State.

§ 10-1304. Security procedures and practices required to protect personal information

In general
(a) To protect personal information from unauthorized access, use, modification, or disclosure, a unit that collects personal information of an individual shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information collected and the nature of the unit and its operations.

XXIII. MASSACHUSSETTS

Section 3. (a) A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter. In addition to providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to, informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use. (b) A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter. The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or

use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident. Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation. The notice to be provided to the resident shall include, but not be limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use.

(c) If an agency is within the executive department, it shall provide written notification of the nature and circumstances of the breach or unauthorized acquisition or use to the information technology division and the division of public records as soon as practicable and without unreasonable delay following the discovery of a breach of security or unauthorized acquisition or use, and shall comply with all policies and procedures adopted by that division pertaining to the reporting and investigation of such an incident.

Section 6. The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

XXIV. MICHIGAN

Mich. Comp. Laws §§ 445.63, 445.72

Effective: April 1, 2011
M.C.L.A. 445.72

445.72. Notification of security breaches by owners, licensees, or persons maintaining databases; standards for furnishing, timeliness, and form of notice; notification of consumer reporting agencies; compliance with section by financial institutions and persons or agencies subject to federal health insurance portability and accountability act; furnishing of notice by public utilities; false notification of security breach; civil fines; preemption of local law

Sec. 12. (1) Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach under subsection (2), shall

provide a notice of the security breach to each resident of this state who meets 1 or more of the following:
(a) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person.
(b) That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.
(2) Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that maintains a database that includes data that the person or agency does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the security breach.
(3) In determining whether a security breach is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state under subsection (1) or (2), a person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.
(4) A person or agency shall provide any notice required under this section without unreasonable delay. A person or agency may delay providing notice without violating this subsection if either of the following is met:
(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. However, the agency or person shall provide the notice required under this subsection without unreasonable delay after the person or agency completes the 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 jeopardize homeland or national security. However, the agency or person shall provide the notice required under this section without unreasonable delay after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security.
(5) Except as provided in subsection (11), an agency or person shall provide any notice required under this section by providing 1 or more of the following to the recipient:
(a) Written notice sent to the recipient at the recipient's postal address in the records of the agency or person.
(b) Written notice sent electronically to the recipient if any of the following are met:
(*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.
(*iii*) The person or agency conducts its business primarily through internet account transactions or on the internet.
(c) If 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.
(d) 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.
(6) A notice under this section shall do all of the following:
(a) For a notice provided under subsection (5)(a) or (b), 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), 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.
(7) A person or agency may provide any notice required under this section pursuant to an agreement between that person or agency and another person or agency, if the notice provided pursuant to the agreement does not conflict with any provision of this section.
(8) Except as provided in this subsection, after a person or agency provides a notice under this section, the person or agency shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the security breach without unreasonable delay. A notification under this subsection shall include the number of notices that the person or agency provided to residents of this state and the timing of those notices. This subsection does not apply if either of the following is met:
(a) The person or agency is required under this section to provide notice of a security breach to 1,000 or fewer residents of this state.
(b) The person or agency is subject to 15 USC 6801 to 6809.
(9) 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 with, the interagency guidance on response programs for unauthorized access to customer information and customer notice prescribed by the board of governors of the federal reserve system and the other federal bank and thrift regulatory agencies, or similar guidance prescribed and adopted by the national credit union administration, and its affiliates, is considered to be in compliance with this section.

(10) A person or agency that is subject to and complies with the health insurance portability and accountability act of 1996, Public Law 104-191, and with regulations promulgated under that act, 45 CFR parts 160 and 164, for the prevention of unauthorized access to customer information and customer notice is considered to be in compliance with this section.
(11) A public utility that sends monthly billing or account statements to the postal address of its customers may provide notice of a security breach to its customers in the manner described in subsection (5), or alternatively by providing all of the following:
(a) As applicable, notice as described in subsection (5)(b).
(b) Notification to the media reasonably calculated to inform the customers of the public utility of the security breach.
(c) Conspicuous posting of the notice of the security breach on the website of the public utility.
(d) Written notice sent in conjunction with the monthly billing or account statement to the customer at the customer's postal address in the records of the public utility.
(12) A person that provides notice of a security breach in the manner described in this section when a security breach has not occurred, with the intent to defraud, is guilty of a misdemeanor punishable as follows:
(a) Except as otherwise provided under subdivisions (b) and (c), by imprisonment for not more than 93 days or a fine of not more than $250.00 for each violation, or both.
(b) For a second violation, by imprisonment for not more than 93 days or a fine of not more than $500.00 for each violation, or both.
(c) For a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than $750.00 for each violation, or both.
(13) Subject to subsection (14), a person that knowingly fails to provide any notice of a security breach required under this section may be ordered to pay a civil fine of not more than $250.00 for each failure to provide notice. The attorney general or a prosecuting attorney may bring an action to recover a civil fine under this section.
(14) The aggregate liability of a person for civil fines under subsection (13) for multiple violations of subsection (13) that arise from the same security breach shall not exceed $750,000.00.
(15) Subsections (12) and (13) do not affect the availability of any civil remedy for a violation of state or federal law.
(16) This section applies to the discovery or notification of a breach of the security of a database that occurs on or after July 2, 2006.
(17) This section does not apply to the access or acquisition by a person or agency of federal, state, or local government records or documents lawfully made available to the general public.
(18) This section deals with subject matter that is of statewide concern, and any charter, ordinance, resolution, regulation, rule, or other action by a municipal corporation or other political subdivision of this state to regulate, directly or indirectly, any matter expressly set forth in this section is preempted.

XXV. MINNESOTA

Minn. Stat. §§ 325E.61, 325E.64

325E.61. Data warehouses; notice required for certain disclosures

Subdivision 1. Disclosure of personal information; notice required. (a) Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (c), or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.
(b) Any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
(c) The notification required by this section and section 13.055, subdivision 6, may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation.
(d) For purposes of this section and section 13.055, subdivision 6, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security system, provided that the personal information is not used or subject to further unauthorized disclosure.
(e) For purposes of this section and section 13.055, subdivision 6, “personal information” means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:
(1) Social Security number;
(2) driver's license number or Minnesota identification card number; or
(3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(f) For purposes of this section and section 13.055, subdivision 6, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
(g) For purposes of this section and section 13.055, subdivision 6, “notice” may be provided by one of the following methods:
(1) written notice to the most recent available address the person or business has in its records;
(2) electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures in United States Code, title 15, section 7001; or

(3) substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice must consist of all of the following:
(i) e-mail notice when the person or business has an e-mail address for the subject persons;
(ii) conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and
(iii) notification to major statewide media.
(h) Notwithstanding paragraph (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section and section 13.055, subdivision 6, shall be deemed to be in compliance with the notification requirements of this section and section 13.055, subdivision 6, if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.
Subd. 2. Coordination with consumer reporting agencies. If a person discovers circumstances requiring notification under this section and section 13.055, subdivision 6, of more than 500 persons at one time, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.
Subd. 3. Waiver prohibited. Any waiver of the provisions of this section and section 13.055, subdivision 6, is contrary to public policy and is void and unenforceable.
Subd. 4. Exemption. This section and section 13.055, subdivision 6, do not apply to any "financial institution" as defined by United States Code, title 15, section 6809(3).
Subd. 5. Renumbered § 13.055, subd. 6, in St.2006.
Subd. 6. Remedies and enforcement. The attorney general shall enforce this section and section 13.055, subdivision 6, under section 8.31.

XXVI. MISSISSIPPI

Miss. Code § 75-24-29

Miss. Code Ann. § 75-24-29

§ 75-24-29. Notice of breach of security; application; definitions; requirement; grounds for delay of notice; compliance; effect of noncompliance

(1) 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.
(2) For purposes of this section, the following terms shall have the meanings ascribed unless the context clearly requires otherwise:

(a) “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;
(b) “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 or state 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;
(iv) “Affected individual” means any individual who is a resident of this state whose personal information was, or is reasonably believed to have been, intentionally acquired by an unauthorized person through a breach of security.
(3) A person who conducts business in this state shall disclose any breach of security to all affected individuals. The disclosure shall be made without unreasonable delay, subject to the provisions of subsections (4) and (5) of this section and the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the data system. Notification shall not be required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.
(4) 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.
(5) 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 or national security and the law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after the law enforcement agency determines that notification will not compromise the criminal investigation or national security and so notifies the person of that determination.
(6) Any notice required by the provisions of this section may be provided by one (1) of the following methods: (a) written notice; (b) telephone notice; (c) electronic notice, 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; or (d) substitute notice, provided the person demonstrates that the cost of providing notice in accordance with paragraph (a), (b) or (c) of this subsection 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. Substitute notice shall consist of the following: electronic mail notice when the person has an electronic mail address for the affected individuals; conspicuous posting of the notice on the Web site of the

person if the person maintains one; and notification to major statewide media, including newspapers, radio and television.
(7) 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. 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, as defined in 15 USCS 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided the person notifies affected individuals in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or federal functional regulator in the event of a breach of security of the system.
(8) Failure to comply with the requirements of this section shall constitute an unfair trade practice and shall be enforced by the Attorney General; however, nothing in this section may be construed to create a private right of action.

XXVII. MISSOURI

Mo. Rev. Stat. § 407.1500

407.1500. Definitions--notice to consumer for breach of security, procedure--attorney general may bring action for damages

1. As used in this section, the following terms mean:
(1) “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;
(2) “Consumer”, an individual who is a resident of this state;
(3) “Consumer reporting agency”, the same as defined by the federal Fair Credit Reporting Act, 15 U.S.C. Section 1681a;
(4) “Encryption”, the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key;
(5) “Health insurance information”, an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual;
(6) “Medical information”, any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;

(7) “Owns or licenses” includes, but is not limited to, personal information that a business retains as part of the internal customer account of the business or for the purpose of using the information in transactions with the person to whom the information relates;
(8) “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;
(9) “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.
“Personal information” does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public;
(10) “Redacted”, altered or truncated such that no more than five digits of a Social Security number or the last four digits of a driver's license number, state identification card number, or account number is accessible as part of the personal information.
2. (1) Any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri shall provide notice to the affected consumer that there has been a breach of security following discovery or notification of the breach. The disclosure notification shall be:
(a) Made without unreasonable delay;
(b) Consistent with the legitimate needs of law enforcement, as provided in this section; and
(c) Consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.
(2) Any person that maintains or possesses records or data containing personal information of residents of Missouri that the person does not own or license, or any person that conducts business in Missouri that maintains or possesses records or data containing personal information of a resident of Missouri that the person does not own or license, shall notify the owner or licensee of the information of any breach of security immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in this section.
(3) The notice required by this section may be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing or the person

documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the person its determination that notice will no longer impede the investigation or jeopardize national or homeland security.
(4) The notice shall at minimum include a description of the following:
(a) The incident in general terms;
(b) The type of personal information that was obtained as a result of the breach of security;
(c) A telephone number that the affected consumer may call for further information and assistance, if one exists;
(d) Contact information for consumer reporting agencies;
(e) Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.
(5) Notwithstanding subdivisions (1) and (2) of this subsection, notification is not required if, after an appropriate investigation by the person or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the documentation shall be maintained for five years.
(6) For purposes of this section, notice to affected consumers shall be provided by one of the following methods:
(a) Written notice;
(b) Electronic notice for those consumers for whom the person has a valid email address and who have agreed to receive communications electronically, if the notice provided is consistent with the provisions of 15 U.S.C. Section 7001 regarding electronic records and signatures for notices legally required to be in writing;
(c) Telephonic notice, if such contact is made directly with the affected consumers; or
(d) Substitute notice, if:
a. The person demonstrates that the cost of providing notice would exceed one hundred thousand dollars; or
b. The class of affected consumers to be notified exceeds one hundred fifty thousand; or
c. The person does not have sufficient contact information or consent to satisfy paragraphs (a), (b), or (c) of this subdivision, for only those affected consumers without sufficient contact information or consent; or
d. The person is unable to identify particular affected consumers, for only those unidentifiable consumers.
(7) Substitute notice under paragraph (d) of subdivision (6) of this subsection shall consist of all the following:
(a) Email notice when the person has an electronic mail address for the affected consumer;
(b) Conspicuous posting of the notice or a link to the notice on the internet website of the person if the person maintains an internet website; and
(c) Notification to major statewide media.
(8) In the event a person provides notice to more than one thousand consumers at one time pursuant to this section, the person shall notify, without unreasonable delay, the attorney general's

office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notice.
3. (1) 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.
(2) 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.
(3) A financial institution that is:
(a) Subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued 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, and any revisions, additions, or substitutions relating to said interagency guidance; or
(b) Subject to and in compliance with the National Credit Union Administration regulations in 12 CFR Part 748; or
(c) Subject to and in compliance with the provisions of Title V of the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. Sections 6801 to 6809;
shall be deemed to be in compliance with this section.
4. 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 one hundred fifty thousand dollars per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

XXVIII. MONTANA

Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 *et seq.*, 33-19-321

2-6-1501. Definitions

As used in this part, the following definitions apply:
(1) “Breach of the security of a data system” or “breach” means the unauthorized acquisition of computerized data that:
(a) materially compromises the security, confidentiality, or integrity of the personal information maintained by a state agency or by a third party on behalf of a state agency; and
(b) causes or is reasonably believed to cause loss or injury to a person.
(2) “Individual” means a human being.

(3) “Person” means an individual, a partnership, a corporation, an association, or a public organization of any character.
(4)(a) “Personal information” means a 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:
(i) a social security number;
(ii) a driver's license number, an identification card number issued pursuant to 61-12-501, a tribal identification number or enrollment number, or a similar identification number issued by any state, the District of Columbia, the Commonwealth of Puerto Rico, Guam, the Virgin Islands, or American Samoa;
(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 a person's financial account;
(iv) medical record information as defined in 33-19-104;
(v) a taxpayer identification number; or
(vi) an identity protection personal identification number issued by the United States internal revenue service.
(b) The term does not include publicly available information from federal, state, local, or tribal government records.
(5) “Redaction” means the alteration of personal information contained within data to make all or a significant part of the data unreadable. The term includes truncation, which means that no more than the last four digits of an identification number are accessible as part of the data.
(6)(a) “State agency” means an agency, authority, board, bureau, college, commission, committee, council, department, hospital, institution, office, university, or other instrumentality of the legislative or executive branch of state government. The term includes an employee of a state agency acting within the course and scope of employment.
(b) The term does not include an entity of the judicial branch.
(7) “Third party” means:
(a) a person with a contractual obligation to perform a function for a state agency; or
(b) a state agency with a contractual or other obligation to perform a function for another state agency.

2-6-1503. Notification of breach of security of data system

(1)(a) Upon discovery or notification of a breach of the security of a data system, a state agency that maintains computerized data containing personal information in the data system shall make reasonable efforts to notify any person whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.
(b) The notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (3) or with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.
(2)(a) A third party that receives personal information from a state agency and maintains that information in a computerized data system to perform a state agency function shall:
(i) notify the state agency immediately following discovery of the breach if the personal information is reasonably believed to have been acquired by an unauthorized person; and

(ii) make reasonable efforts upon discovery or notification of a breach to notify any person whose unencrypted personal information is reasonably believed to have been acquired by an unauthorized person as part of the breach. This notification must be provided in the same manner as the notification required in subsection (1).
(b) A state agency notified of a breach by a third party has no independent duty to provide notification of the breach if the third party has provided notification of the breach in the manner required by subsection (2)(a) but shall provide notification if the third party fails to do so in a reasonable time and may recover from the third party its reasonable costs for providing the notice.
(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay of notification. The notification required by this section must be made after the law enforcement agency determines that the notification will not compromise the investigation.
(4) All state agencies and third parties to whom personal information is disclosed by a state agency shall develop and maintain:
(a) an information security policy designed to safeguard personal information; and
(b) breach notification procedures that provide reasonable notice to individuals as provided in subsections (1) and (2).
(5) A state agency or third party that is required to issue a notification to an individual pursuant to this section shall simultaneously submit to the state's chief information officer at the department of administration and to the attorney general's consumer protection office an electronic copy of the notification and a statement providing the date and method of distribution of the notification. The electronic copy and statement of notification must exclude any information that identifies the person who is entitled to receive notification. If notification is made to more than one person, a single copy of the notification that includes the number of people who were notified must be submitted to the chief information officer and the consumer protection office.

30-14-1701

30-14-1702. Definitions

As used in 30-14-1701 through 30-14-1705, 30-14-1712, and 30-14-1713, unless the context requires otherwise, the following definitions apply:
(1)(a) “Business” means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or any other country or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records. The term also includes industries regulated by the public service commission or under Title 30, chapter 10.
(b) The term does not include industries regulated under Title 33.
(2) “Customer” means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.
(3) “Electronic mail message” means a message sent to a unique destination, commonly expressed as a string of characters, consisting of a unique user name or electronic mailbox and a reference to

an internet domain, whether or not displayed, to which an electronic message can be sent or delivered.
(4) “Individual” means a natural person.
(5) “Internet” has the meaning provided in 2-17-551.
(6) “Internet services provider” has the meaning provided in 2-17-602.
(7) “Personal information” means an individual's name, signature, address, or telephone number, in combination with one or more additional pieces of information about the individual, consisting of the individual's passport number, driver's license or state identification number, insurance policy number, bank account number, credit card number, debit card number, passwords or personal identification numbers required to obtain access to the individual's finances, or any other financial information as provided by rule. A social security number, in and of itself, constitutes personal information.
(8)(a) “Records” means any material, regardless of the physical form, on which personal information is recorded.
(b) The term does not include publicly available directories containing personal information that an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.
(9) “Website” means an electronic location that has a single uniform resource locator or other single location with respect to the internet.

30-14-1704. Computer security breach

(1) Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3), or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
(2) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data system immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person.
(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay in notification. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.
(4) For purposes of this section, the following definitions apply:
(a) “Breach of the security of the data system” means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of

the data system, provided that the personal information is not used or subject to further unauthorized disclosure.
(b)(i) “Personal information” means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
(A) social security number;
(B) driver's license number, 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 as defined in 33-19-104;
(E) a taxpayer identification number; or
(F) an identity protection personal identification number issued by the United States internal revenue service.
(ii) Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
(5)(a) For purposes of this section, notice may be provided by one of the following methods:
(i) written notice;
(ii) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001;
(iii) telephonic notice; or
(iv) substitute notice, if the person or business demonstrates that:
(A) the cost of providing notice would exceed $250,000;
(B) the affected class of subject persons to be notified exceeds 500,000; or
(C) the person or business does not have sufficient contact information.
(b) Substitute notice must consist of the following:
(i) an electronic mail notice when the person or business has an electronic mail address for the subject persons; and
(ii) conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; or
(iii) notification to applicable local or statewide media.
(6) Notwithstanding subsection (5), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and that does not unreasonably delay notice is considered to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the data system.
(7) If a business discloses a security breach to any individual pursuant to this section and gives a notice to the individual that suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual. The coordination may not unreasonably delay the notice to the affected individuals.
(8) 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 the attorney general's consumer protection office,

excluding any information that personally identifies any individual who is entitled to receive notification. If a notification is made to more than one individual, a single copy of the notification must be submitted that indicates the number of individuals in the state who received notification.

XXIX. NEBRASKA

87-803. Breach of security; investigation; notice to resident; notice to Attorney General.

(1) An individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident. Notice shall be made as soon as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.
(2) If notice of a breach of security of the system is required by subsection (1) of this section, the individual or commercial entity shall also, not later than the time when notice is provided to the Nebraska resident, provide notice of the breach of security of the system to the Attorney General.
(3) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach if use of personal information about a Nebraska resident for an unauthorized purpose occurred or is reasonably likely to occur. Cooperation includes, but is not limited to, sharing with the owner or licensee information relevant to the breach, not including information proprietary to the individual or commercial entity.
(4) Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.

87-804. Compliance with notice requirements; manner.

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

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

87-806. Attorney General; powers.

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

XXX. NEVADA

Nev. Rev. Stat. §§ 603A.010 *et seq*., 242.183

603A.040. "Personal information" defined
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.

603A.200. Destruction of certain records

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

(b) “Reasonable measures to ensure the destruction” means any method that modifies the records containing the personal information in such a way as to render the personal information contained in the records unreadable or undecipherable, including, without limitation:
(1) Shredding of the record containing the personal information; or
(2) Erasing of the personal information from the records.

N.R.S. 603A.220

603A.220. Disclosure of breach of security of system data; methods of disclosure

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

section if the data collector notifies subject persons in accordance with its policies and procedures in the event of a breach of the security of the system data.
(b) Is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq., shall be deemed to be in compliance with the notification requirements of this section.
6. If a data collector determines that notification is required to be given pursuant to the provisions of this section to more than 1,000 persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency, as that term is defined in 15 U.S.C. § 1681a(p), that compiles and maintains files on consumers on a nationwide basis, of the time the notification is distributed and the content of the notification.

XXXI. NEW HAMPSHIRE

N.H. Rev. Stat. §§ 359-C:19 et seq.

N.H. Rev. Stat. § 359-C:19

359**-**C**:**19 Definitions.

In this subdivision:
I. “Computerized data” means personal information stored in an electronic format.
II. “Encrypted” means the transformation of data through the use of an algorithmic process into a form for which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements completely unreadable or unusable. Data shall not be considered to be encrypted for purposes of this subdivision if it is acquired in combination with any required key, security code, access code, or password that would permit access to the encrypted data.
III. “Person” means an individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state.
IV. (a) “Personal information” means an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
(1) Social security number.
(2) Driver's license number or other government identification number.
(3) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(b) “Personal information” shall not include information that is lawfully made available to the general public from federal, state, or local government records.

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

359-C:20 Notification of Security Breach Required.

I. (a) Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision.
(b) Any person engaged in trade or commerce that is subject to RSA 358-A:3, I shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office. The notice shall include the anticipated date of the notice to the individuals and the approximate number of individuals in this state who will be notified. Nothing in this section shall be construed to require the person to provide to any regulator or the New Hampshire attorney general's office the names of the individuals entitled to receive the notice or any personal information relating to them. The disclosure shall be made to affected individuals as quickly as possible, after the determination required under this section.
(c) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was acquired by an unauthorized person. Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential or business information or trade secrets.
II. Notification pursuant to paragraph I may be delayed if a law enforcement agency, or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security.
III. The notice required under this section shall be provided by one of the following methods:
(a) Written notice.
(b) Electronic notice, if the agency or business' primary means of communication with affected individuals is by electronic means.
(c) Telephonic notice, provided that a log of each such notification is kept by the person or business who notifies affected persons.
(d) Substitute notice, if the person demonstrates that the cost of providing notice would exceed $5,000, that the affected class of subject individuals to be notified exceeds 1,000, or the person does not have sufficient contact information or consent to provide notice pursuant to subparagraphs I(a)-I(c). Substitute notice shall consist of all of the following:
(1) E-mail notice when the person has an e-mail address for the affected individuals.
(2) Conspicuous posting of the notice on the person's business website, if the person maintains one.

(3) Notification to major statewide media.
(e) Notice pursuant to the person's internal notification procedures maintained as part of an information security policy for the treatment of personal information.
IV. Notice under this section shall include at a minimum:
(a) A description of the incident in general terms.
(b) The approximate date of breach.
(c) The type of personal information obtained as a result of the security breach.
(d) The telephonic contact information of the person subject to this section.
V. Any person engaged in trade or commerce that is subject to RSA 358-A:3, I which maintains procedures for security breach notification pursuant to the laws, rules, regulations, guidances, or guidelines issued by a state or federal regulator shall be deemed to be in compliance with this subdivision if it acts in accordance with such laws, rules, regulations, guidances, or guidelines.
VI. (a) If a person is required to notify more than 1,000 consumers of a breach of security pursuant to this section, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. section 1681a(p), of the anticipated date of the notification to the consumers, the approximate number of consumers who will be notified, and the content of the notice. Nothing in this paragraph shall be construed to require the person to provide to any consumer reporting agency the names of the consumers entitled to receive the notice or any personal information relating to them.
(b) Subparagraph (a) shall not apply to a person who is subject to Title V of the Gramm, Leach-Bliley Act, 15 U.S.C. section 6801 et seq.

359-C:21 Violation.

I. Any person injured by any violation under this subdivision may bring an action for damages and for such equitable relief, including an injunction, as the court deems necessary and proper. If the court finds for the plaintiff, recovery shall be in the amount of actual damages. If the court finds that the act or practice was a willful or knowing violation of this chapter, it shall award as much as 3 times, but not less than 2 times, such amount. In addition, a prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees, as determined by the court. Any attempted waiver of the right to the damages set forth in this paragraph shall be void and unenforceable. Injunctive relief shall be available to private individuals under this chapter without bond, subject to the discretion of the court.
II. The New Hampshire attorney general's office shall enforce the provisions of this subdivision pursuant to RSA 358-A:4.
III. The burden shall be on the person responsible for the determination under RSA 359-C:20, I to demonstrate compliance with this subdivision.

XXXII. NEW JERSEY

N.J. Stat. § 56:8-161 et seq.

Effective: January 1, 2006
N.J.S.A. 56:8-161

56:8-161. Definitions concerning security of personal information

As used in sections 10 through 15 of this amendatory and supplementary act:[1]
“Breach of security” means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.
“Business” means a sole proprietorship, partnership, corporation, association, or other entity, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this State, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution.
“Communicate” means to send a written or other tangible record or to transmit a record by any means agreed upon by the persons sending and receiving the record.
“Customer” means an individual who provides personal information to a business.
“Individual” means a natural person.
“Internet” means the international computer network of both federal and non-federal interoperable packet switched data networks.
“Personal information” means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.
For the purposes of sections 10 through 15 of this amendatory and supplementary act[1], personal information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media.
“Private entity” means any individual, corporation, company, partnership, firm, association, or other entity, other than a public entity.
“Public entity” includes the State, and any county, municipality, district, public authority, public agency, and any other political subdivision or public body in the State. For the purposes of sections 10 through 15 of this amendatory and supplementary act,[1] public entity does not include the federal government.
“Publicly post” or “publicly display” means to intentionally communicate or otherwise make available to the general public.

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

56:8-162. Destruction of certain customer records; methods

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

56:8-163. Disclosure of breach of security of computerized records; report to Division of State Police; exception; forms of notification

a. Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.
b. Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.
c. (1) Any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.
(2) The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.
d. For purposes of this section, notice may be provided by one of the following methods:

(1) Written notice;
(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 101 of the federal "Electronic Signatures in Global and National Commerce Act" (15 U.S.C. s.7001); or
(3) Substitute notice, if the business or public entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the business or public entity does not have sufficient contact information. Substitute notice shall consist of all of the following:
(a) E-mail notice when the business or public entity has an e-mail address;
(b) Conspicuous posting of the notice on the Internet web site page of the business or public entity, if the business or public entity maintains one; and
(c) Notification to major Statewide media.
e. Notwithstanding subsection d. of this section, a business or public entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and is otherwise consistent with the requirements of this section, shall be deemed to be in compliance with the notification requirements of this section if the business or public entity notifies subject customers in accordance with its policies in the event of a breach of security of the system.
f. In addition to any other disclosure or notification required under this section, in the event that a business or public entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the business or public entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the federal "Fair Credit Reporting Act" (15 U.S.C. s. 1681a), of the timing, distribution and content of the notices.

XXXIII. NEW MEXICO

2017 H.B. 15, Chap. 36 (effective 6/16/2017)

Not on Westlaw

XXXIV. NEW YORK

N.Y. Gen. Bus. Law § 899-AA,

§ 899-aa. Notification; person without valid authorization has acquired private information

1. As used in this section, the following terms shall have the following meanings:
(a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;

(b) “Private information” shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:
(1) social security number;
(2) driver's license number or non-driver identification card number; or
(3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
“Private information” does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.
(c) “Breach of the security of the system” shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.
In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:
(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
(2) indications that the information has been downloaded or copied; or
(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
(d) “Consumer reporting agency” shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to any person or business required to make a notification under subdivision two of this section.
2. Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
3. Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

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

timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.
(b) In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.
9. The provisions of this section shall be exclusive and shall preempt any provisions of local law, ordinance or code, and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section.

N.Y. State Tech. Law 208

§ 208. Notification; person without valid authorization has acquired private information

1. As used in this section, the following terms shall have the following meanings:
(a) “Private information” shall mean personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:
(1) social security number;
(2) driver's license number or non-driver identification card number; or
(3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.
“Private information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
(b) “Breach of the security of the system” shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity. Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.
In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such state entity 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.
(c) “State entity” shall mean any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York, except:
(1) the judiciary; and
(2) all cities, counties, municipalities, villages, towns, and other local agencies.

(d) “Consumer reporting agency” shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to state entities required to make a notification under subdivision two of this section.

2. Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The state entity shall consult with the state office of information technology services to determine the scope of the breach and restoration measures.

3. Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the state entity who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;

(c) telephone notification provided that a log of each such notification is kept by the state entity who notifies affected persons; or

(d) Substitute notice, if a state entity demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such state entity has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on such state entity's web site page, if such agency maintains one; and

(3) notification to major statewide media.

6. Regardless of the method by which notice is provided, such notice shall include contact information for the state entity making the notification and a description of the categories of

information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.
7. (a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the department of state and the state office of information technology services as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.
(b) In the event that more than five thousand New York residents are to be notified at one time, the state entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.
8. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.

XXXV. NORTH CAROLINA

N.C.G.S.A. § 75-65

§ 75-65. Protection from security breaches

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

discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section.

- (c) The notice required by this section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.
- (d) The notice shall be clear and conspicuous. The notice shall include 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.
(e) For purposes of this section, notice to affected persons may be provided by one of the following methods:
(1) Written notice.
(2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001.
(3) Telephonic notice provided that contact is made directly with the affected persons.
(4) Substitute notice, if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2), or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:
a. E-mail notice when the business has an electronic mail address for the subject persons.
b. Conspicuous posting of the notice on the Web site page of the business, if one is maintained.
c. Notification to major statewide media.

(e1) In the event a business provides notice to an affected person pursuant to this section, the business shall notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.
(f) In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.
(g) Any waiver of the provisions of this Article is contrary to public policy and is void and unenforceable.
(h) A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; or a credit union that is subject to and in compliance with the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration; and any revisions, additions, or substitutions relating to any of the said interagency guidance, shall be deemed to be in compliance with this section.
(i) A violation of this section is a violation of G.S. 75-1.1. No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation.
(j) Causes of action arising under this Article may not be assigned.

XXXVI. NORTH DAKOTA

N.D. Cent. Code §§ 51-30-01 et seq.

NDCC, 51-30-01

§ 51-30-01. Definitions

In this chapter, unless the context or subject matter otherwise requires:
1. “Breach of the security system” means unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or 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.

2. “Health insurance information” means an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
3. “Medical information” means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
4. a. “Personal information” means an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted:
(1) The individual's social security number;
(2) The operator's license number assigned to an individual by the department of transportation under section 39-06-14;
(3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1;
(4) The individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts;
(5) The individual's date of birth;
(6) The maiden name of the individual's mother;
(7) 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.
b. “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

§ 51-30-02. Notice to attorney general and consumers

Any person that owns or licenses computerized data that includes personal information, shall disclose any breach of the security system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition, any person that experiences a breach of the security system as provided in this section shall disclose to the attorney general by mail or email any breach of the security system which exceeds two hundred fifty individuals. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.

XXXVII. OHIO

Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192

R.C. § 1349.19

1349.19 Disclosure of breach of security system; attorney general investigation; civil action

(A) As used in this section:
(1)(a) “Breach of the security of the system” means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.
(b) For purposes of division (A)(1)(a) of this section:
(i) Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security of the system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure.
(ii) Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a breach of the security of the system.
(2) “Business entity” means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, or the parent or subsidiary of a financial institution.
(3) “Consumer reporting agency that compiles and maintains files on consumers on a nationwide basis” means a consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's creditworthiness, credit standing, or credit capacity, each of the following regarding consumers residing nationwide:
(a) Public record information;
(b) Credit account information from persons who furnish that information regularly and in the ordinary course of business.
(4) “Encryption” means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
(5) “Individual” means a natural person.
(6) “Person” has the same meaning as in section 1.59 of the Revised Code, except that “person” includes a business entity only if the business entity conducts business in this state.
(7)(a) “Personal information” means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:
(i) Social security number;
(ii) Driver's license number or state identification card number;

(iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.
(b) “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed:
(i) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television;
(ii) Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media described in division (A)(7)(b)(i) of this section;
(iii) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation;
(iv) Any type of media similar in nature to any item, entity, or activity identified in division (A)(7)(b)(i), (ii), or (iii) of this section.
(8) “Record” means any information that is stored in an electronic medium and is retrievable in perceivable form. “Record” does not include any publicly available directory containing information an individual voluntarily has consented to have publicly disseminated or listed, such as name, address, or telephone number.
(9) “Redacted” means altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data.
(10) “System” means any collection or group of related records that are kept in an organized manner, that are maintained by a person, and from which personal information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. “System” does not include any published directory, any reference material or newsletter, or any routine information that is maintained for the purpose of internal office administration of the person, if the use of the directory, material, newsletter, or information would not adversely affect an individual, and there has been no unauthorized external breach of the directory, material, newsletter, or information.
(B)(1) Any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. The disclosure described in this division may be made pursuant to any provision of a contract entered into by the person with another person prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of this section and does not waive any provision of this section. For purposes of this section, a resident of this state is an individual whose principal mailing address as reflected in the records of the person is in this state.
(2) The person shall make the disclosure described in division (B)(1) of this section in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to

determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system.
(C) Any person that, on behalf of or at the direction of another person or on behalf of or at the direction of any governmental entity, is the custodian of or stores computerized data that includes personal information shall notify that other person or governmental entity of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of this state.
(D) The person may delay the disclosure or notification required by division (B), (C), or (G) of this section if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the person shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security.
(E) For purposes of this section, a person may disclose or make a notification by any of the following methods:
(1) Written notice;
(2) Electronic notice, if the person's primary method of communication with the resident to whom the disclosure must be made is by electronic means;
(3) Telephone notice;
(4) Substitute notice in accordance with this division, if the person required to disclose demonstrates that the person does not have sufficient contact information to provide notice in a manner described in division (E)(1), (2), or (3) of this section, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed two hundred fifty thousand dollars, or that the affected class of subject residents to whom disclosure or notification is required exceeds five hundred thousand persons. Substitute notice under this division shall consist of all of the following:
(a) Electronic mail notice if the person has an electronic mail address for the resident to whom the disclosure must be made;
(b) Conspicuous posting of the disclosure or notice on the person's web site, if the person maintains one;
(c) Notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds seventy-five per cent of the population of this state.
(5) Substitute notice in accordance with this division, if the person required to disclose demonstrates that the person is a business entity with ten employees or fewer and that the cost of providing the disclosures or notices to residents to whom disclosure or notification is required will exceed ten thousand dollars. Substitute notice under this division shall consist of all of the following:
(a) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the business entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;

(b) Conspicuous posting of the disclosure or notice on the business entity's web site, if the entity maintains one;
(c) Notification to major media outlets in the geographic area in which the business entity is located.
(F)(1) A financial institution, trust company, or credit union or any affiliate of a financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the requirements of this section.
(2) This section does not apply to any person or entity that is a covered entity as defined in 45 C.F.R. 160.103, as amended.
(G) If a person discovers circumstances that require disclosure under this section to more than one thousand residents of this state involved in a single occurrence of a breach of the security of the system, the person shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the person to the residents of this state. In no case shall a person that is required to make a notification required by this division delay any disclosure or notification required by division (B) or (C) of this section in order to make the notification required by this division.
(H) Any waiver of this section is contrary to public policy and is void and unenforceable.
(I) The attorney general may conduct pursuant to sections 1349.191 and 1349.192 of the Revised Code an investigation and bring a civil action upon an alleged failure by a person to comply with the requirements of this section.

XXXVIII. OKLAHOMA

Okla. Stat. §§ 74-3113.1, 24-161 to -166

XXXIX. OREGON

646A.602. Definitions

As used in ORS 646A.600 to 646A.628:
(1)(a) “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.
(b) “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.
(2) “Consumer” means an individual resident of this state.
(3) “Consumer report” means a consumer report as described in section 603(d) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)), as that Act existed on January 1, 2016, that a consumer reporting agency compiles and maintains.
(4) “Consumer reporting agency” means a consumer reporting agency as described in section 603(p) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(p)) as that Act existed on January 1, 2016.
(5) “Debt” means any obligation or alleged obligation arising out of a consumer transaction.
(6) “Encryption” means an algorithmic process that renders data unreadable or unusable without the use of a confidential process or key.
(7) “Extension of credit” means a right to defer paying debt or a right to incur debt and defer paying the debt, that is offered or granted primarily for personal, family or household purposes.
(8) “Identity theft” has the meaning set forth in ORS 165.800.
(9) “Identity theft declaration” means a completed and signed statement that documents alleged identity theft, using the form available from the Federal Trade Commission, or another substantially similar form.
(10) “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 as defined in ORS 174.109.
(11) “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:
(A) A consumer's Social Security number;
(B) A consumer's driver license number or state identification card number issued by the Department of Transportation;
(C) A consumer's passport number or other identification number issued by the United States;
(D) 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;
(E) 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;
(F) 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
(G) 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) Any of the data elements or any combination of the data elements described in paragraph (a) of this subsection without 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.
(c) “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.
(12) “Proper identification” means written information or documentation that a consumer or representative can present to another person as evidence of the consumer's or representative's identity, examples of which include:
(a) A valid Social Security number or a copy of a valid Social Security card;
(b) A certified or otherwise official copy of a birth certificate that a governmental body issued; and
(c) A copy of a driver license or other government-issued identification.
(13) “Protected consumer” means an individual who is:
(a) Not older than 16 years old at the time a representative requests a security freeze on the individual's behalf; or
(b) Incapacitated or for whom a court or other authority has appointed a guardian or conservator.
(14) “Protective record” means information that a consumer reporting agency compiles to identify a protected consumer for whom the consumer reporting agency has not prepared a consumer report.
(15) “Redacted” means altered or truncated so that no more than the last four digits of a Social Security number, driver license number, state identification card number, passport number or other number issued by the United States, financial account number, credit card number or debit card number is visible or accessible.
(16) “Representative” means a consumer who provides a consumer reporting agency with sufficient proof of the consumer's authority to act on a protected consumer's behalf.
(17) “Security freeze” means a notice placed in a consumer report at a consumer's request or a representative's request or in a protective record at a representative's request that, subject to certain exemptions, prohibits a consumer reporting agency from releasing information in the consumer report or the protective record for an extension of credit, unless the consumer temporarily lifts the security freeze on the consumer's consumer report or a protected consumer or representative removes the security freeze on or deletes the protective record.

646A.604. Notice of breach of security to consumer

(1) A person that owns or licenses personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities and that was subject to a breach of security shall give notice of the breach of security to:
(a) The consumer to whom the personal information pertains after the person discovers the breach of security or after the person receives notice of a breach of security under subsection (2) of this section. The person shall notify the consumer in the most expeditious manner possible, without unreasonable delay, consistent with the legitimate needs of law enforcement described in subsection (3) of this section and consistent with any measures that are necessary to determine sufficient contact information for the affected consumer, determine the scope of the breach of security and restore the reasonable integrity, security and confidentiality of the personal information.
(b) The Attorney General, either in writing or electronically, if the number of consumers to whom the person must send the notice described in paragraph (a) of this subsection exceeds 250. The

person shall disclose the breach of security to the Attorney General in the manner described in paragraph (a) of this subsection.
(2) A person that maintains or otherwise possesses personal information on behalf of, or under license of, another person shall notify the other person after discovering a breach of security.
(3) A person that owns or licenses personal information may delay notifying a consumer of a breach of security 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 person delay the notification.
(4) For purposes of this section, a person that owns or licenses personal information may notify a consumer of a breach of security:
(a) In writing;
(b) Electronically, if the person customarily communicates with the consumer electronically or if the notice is consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001) as that Act existed on January 1, 2016;
(c) By telephone, if the person contacts the affected consumer directly; or
(d) With substitute notice, if the person demonstrates that the cost of notification otherwise would exceed $250,000 or that the affected class of consumers exceeds 350,000, or if the person does not have sufficient contact information to notify affected consumers. For the purposes of this paragraph, “substitute notice” means:
(A) Posting the notice or a link to the notice conspicuously on the person's website if the person maintains a website; and
(B) Notifying major statewide television and newspaper media.
(5) 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 person that owned or licensed the personal information that was subject to the breach of security;
(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.
(6) If a person discovers a breach of security that affects more than 1,000 consumers, the person shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain reports on consumers on a nationwide basis of the timing, distribution and content of the notice the person gave to affected consumers and shall include in the notice any police report number assigned to the breach of security. A person may not delay notifying affected consumers of a breach of security in order to notify consumer reporting agencies.
(7) Notwithstanding subsection (1) of this section, a person does not need to notify consumers of a breach of security if, after an appropriate investigation or after consultation with relevant federal, state or local law enforcement agencies, the person reasonably determines that the consumers whose personal information was subject to the breach of security are unlikely to suffer harm. The person must document the determination in writing and maintain the documentation for at least five years.

(8) This section does not apply to:
(a) 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 rules, regulations, procedures, guidelines or guidance provide greater protection to personal information and disclosure requirements at least as thorough as the protections and disclosure requirements provided under this section.
(b) 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.
(c) A person that is subject to and complies with regulations promulgated pursuant to Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 to 6809) as that Act existed on January 1, 2016.
(d)(A) Except as provided in subparagraph (B) of this paragraph, a covered entity, as defined in 45 C.F.R. 160.103, as in effect on January 1, 2016, that is governed under 45 C.F.R. parts 160 and 164, as in effect on January 1, 2016, if the covered entity sends the Attorney General a copy of the notice the covered entity sent to consumers under ORS 646A.604 or a copy of the notice that the covered entity sent to the primary functional regulator designated for the covered entity under the Health Insurance Portability and Availability Act of 1996, (P.L. 104-191, 110 Stat. 1936, 42 U.S.C. 300(gg), 29 U.S.C. 118 et seq., 42 U.S.C. 1320(d) et seq., 45 C.F.R. parts 160 and 164).
(B) A covered entity is subject to the provisions of this section if the covered entity does not send a copy of a notice described in subparagraph (A) of this paragraph to the Attorney General within a reasonable time after the Attorney General requests the copy.
(9)(a) A person's violation of a provision of ORS 646A.600 to 646A.628 is an unlawful practice under ORS 646.607.
(b) The rights and remedies available under this section are cumulative and are in addition to any other rights or remedies that are available under law.

XL. PENNSYLVANIA

§ 2302. Definitions

The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:
“Breach of the security of the system.” The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.
“Business.” A sole proprietorship, partnership, corporation, association or other group, however organized and whether or not organized to operate at a profit, including a financial institution

organized, chartered or holding a license or authorization certificate under the laws of this Commonwealth, any other state, the United States or any other country, or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records.
“Encryption.” The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
“Entity.” A State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth.
“Individual.” A natural person.
“Notice.” May be provided by any of the following methods of notification:
(1) Written notice to the last known home address for the individual.
(2) Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.
(3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.
(4)(i) Substitute notice, if the entity demonstrates one of the following:
(A) The cost of providing notice would exceed $100,000.
(B) The affected class of subject persons to be notified exceeds 175,000.
(C) The entity does not have sufficient contact information.
(ii) Substitute notice shall consist of all of the following:
(A) E-mail notice when the entity has an e-mail address for the subject persons.
(B) Conspicuous posting of the notice on the entity's Internet website if the entity maintains one.
(C) Notification to major Statewide media.
“Personal information.”
(1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:
(i) Social Security number.
(ii) Driver's license number or a State identification card number issued in lieu of a driver's license.
(iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.
(2) The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records.
“Records.” Any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed or electromagnetically transmitted. The term does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.
“Redact.” The term includes, but is not limited to, alteration or truncation such that no more than the last four digits of a Social Security number, driver's license number, State identification card number or account number is accessible as part of the data.

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

§ 2303. Notification of breach

(a) General rule.--An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4[1] or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.
(b) Encrypted information.--An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.
(c) Vendor notification.--A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

XLI. PUERTO RICO

10 Laws of Puerto Rico §§ 4051 et seq.

XLII. RHODE ISLAND

§ 11-49.3-4 Notification of breach.

(a)(1) Any municipal agency, state agency, or person that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information shall provide notification as set forth in this section of any disclosure of personal information, or any breach of the security of the system, that poses a significant risk of identity theft to any resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity.

(2) The notification shall be made in the most expedient time possible, but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained in subsection (d) of this section, and shall be consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section. In the event that more than five hundred (500) Rhode Island residents are to be notified, the municipal agency, state agency, or person shall notify the attorney general and the major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals. Notification to the attorney general and the major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents.
(b) 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. The federal, state, or local law enforcement agency must notify the municipal agency, state agency, or person of the request to delay notification without unreasonable delay. If notice is delayed due to such determination, then, as soon as the federal, state, or municipal law enforcement agency determines and informs the municipal agency, state agency, or person that notification no longer poses a risk of impeding an investigation, notice shall be provided as soon as practicable pursuant to subsection (a)(2). The municipal agency, state agency, or person shall cooperate with federal, state, or municipal law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.
(c) Any municipal agency, state agency, or person required to make notification under this section and fails to do so is liable for a violation as set forth in § 11-49.3-5.
(d) 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.

XLIII. SOUTH CAROLINA

SECTION 39-1-90.

Breach of security of business data; notification; definitions; penalties; exception as to certain banks and financial institutions; notice to Consumer Protection Division.

(A) A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the 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 the resident. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (C), or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
(B) A person conducting business in this State and maintaining computerized data or other data that includes personal identifying information that the person does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.
(C) The notification required by this section may be delayed if a law enforcement agency determines that the notification 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.
(D) For purposes of this section:
(1) "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.
(2) "Person" has the same meaning as in Section 37-20-110(10).
(3) "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.
The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local governmental records lawfully made available to the general public.

(E) The notice required by this section may be provided by:
(1) written notice;
(2) electronic notice, if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures in Section 7001 of Title 15 USC and Chapter 6, Title 11 of the 1976 Code;
(3) telephonic notice; or
(4) substitute notice, if the person demonstrates that the cost of providing notice exceeds two hundred fifty thousand dollars or that the affected class of subject persons to be notified exceeds five hundred thousand or the person has insufficient contact information. Substitute notice consists of:
(a) e-mail notice when the person has an e-mail address for the subject persons;
(b) conspicuous posting of the notice on the web site page of the person, if the person maintains one; or
(c) notification to major statewide media.
(F) Notwithstanding subsection (E), 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.
(G) A resident of this State who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may:
(1) institute a civil action to recover damages in case of a wilful and knowing violation;
(2) institute a civil action that must be limited to actual damages resulting from a violation in ase of a negligent violation of this section;
(3) seek an injunction to enforce compliance; and
(4) recover attorney's fees and court costs, if successful.
(H) A person who knowingly and wilfully violates this section is subject to an administrative fine in the amount of one thousand dollars for each resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs.
(I) This section does not apply to a bank or financial institution that is subject to and in compliance with the privacy and security provision of the Gramm-Leach-Bliley Act.
(J) A financial institution that is subject to and in compliance with the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, as amended, is considered to be in compliance with this section.
(K) If a business provides notice to more than one thousand persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Department of Consumer Affairs and all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined in 15 USC Section 1681a(p), of the timing, distribution, and content of the notice.

XLIV. SOUTH DAKOTA

N/A

XLV. TENNESSEE

T. C. A. § 47-18-2107

§ 47-18-2107. Breaches of security systems; definitions; notice

(a) As used in this section:
(1) “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;
(2) “Encrypted” means computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key and in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2;
(3) “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;
(4) “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; and
(B) Does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable; and
(5) “Unauthorized person” includes an employee of the information holder who is discovered by the information holder to have obtained personal information with the intent to use it for an unlawful purpose.
(b) Following discovery or notification of a breach of system security by an information holder, the information holder shall disclose the breach of system security to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized

person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement, as provided in subsection (d).
(c) Any information holder that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information of any breach of system security if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement, as provided in subsection (d).
(d) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is delayed, it must be made no later than forty-five (45) days after the law enforcement agency determines that notification will not compromise the investigation.
(e) For purposes of this section, notice may be provided by one (1) of the following methods:
(1) Written notice;
(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 or if the information holder's primary method of communication with the resident of this state has been by electronic means; or
(3) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), that the affected class of subject persons to be notified exceeds five hundred thousand (500,000) persons, or the information holder does not have sufficient contact information and the notice consists of all of the following:
(A) Email notice, when the information holder has an email address for the subject persons;
(B) Conspicuous posting of the notice on the information holder's website, if the information holder maintains a website page; and
(C) Notification to major statewide media.
(f) Notwithstanding subsection (e), 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.
(g) If an information holder discovers circumstances requiring notification pursuant to this section of more than one thousand (1,000) persons at one (1) time, the information holder must also notify, without unreasonable delay, all consumer reporting agencies, as defined by 15 U.S.C. § 1681a, and credit bureaus that compile and maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.
(h) Any customer of an information holder who is a person or business entity, but who is not an agency of this state or any political subdivision of this state, and who is injured by a violation of this section, may institute a civil action to recover damages and to enjoin the information holder from further action in violation of this section. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

XLVI. TEXAS

Tex. Bus. & Com. Code §§ 521.002, 521.053

V.T.C.A., Bus. & C. § 521.002

§ 521.002. Definitions

(a) In this chapter:
(1) “Personal identifying information” means information that alone or in conjunction with other information identifies an individual, including an individual's:
(A) name, social security number, date of birth, or government-issued identification number;
(B) mother's maiden name;
(C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
(D) unique electronic identification number, address, or routing code; and
(E) telecommunication access device as defined by Section 32.51, Penal Code.
(2) “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.
(3) “Victim” means a person whose identifying information is used by an unauthorized person.
(b) For purposes of this chapter, the term “sensitive personal information” does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

V.T.C.A., Bus. & C. § 521.053

§ 521.053. Notification Required Following Breach of Security of Computerized Data

(a) In this section, “breach of system security” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, 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.

(b) A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
(b-1) If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of a state that requires a person described by Subsection (b) to provide notice of a breach of system security, the notice of the breach of system security required under Subsection (b) may be provided under that state's law or under Subsection (b).
(c) Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
(d) A person may delay providing notice as required by Subsection (b) or (c) at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.
(e) A person may give notice as required by Subsection (b) or (c) by providing:
(1) written notice at the last known address of the individual;
(2) electronic notice, if the notice is provided in accordance with 15 U. S.C. Section 7001; or
(3) notice as provided by Subsection (f).
(f) If the person required to give notice under Subsection (b) or (c) demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:
(1) electronic mail, if the person has electronic mail addresses for the affected persons;
(2) conspicuous posting of the notice on the person's website; or
(3) notice published in or broadcast on major statewide media.
(g) Notwithstanding Subsection (e), a person 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.
(h) If a person is required by this section to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person shall provide the notice required by this subsection without unreasonable delay.

XLVII. UTAH

13-44-202. Personal information -- Disclosure of system security breach.

(1) (a) A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes.

(b) If an investigation under Subsection (1)(a) reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident.

(2) A person required to provide notification under Subsection (1) shall provide the notification in the most expedient time possible without unreasonable delay:

(a) considering legitimate investigative needs of law enforcement, as provided in Subsection (4)(a);

(b) after determining the scope of the breach of system security; and

(c) after restoring the reasonable integrity of the system.

(3) (a) A person who maintains computerized data that includes personal information that the person does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur.

(b) Cooperation under Subsection (3)(a) includes sharing information relevant to the breach with the owner or licensee of the information.

(4) (a) Notwithstanding Subsection (2), a person may delay providing notification under Subsection (1) at the request of a law enforcement agency that determines that notification may impede a criminal investigation.

(b) A person who delays providing notification under Subsection (4)(a) shall provide notification in good faith without unreasonable delay in the most expedient time possible after the law enforcement agency informs the person that notification will no longer impede the criminal investigation.

(5) (a) A notification required by this section may be provided:

(i) in writing by first-class mail to the most recent address the person has for the resident;

(ii) electronically, if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001;

(iii) by telephone, including through the use of automatic dialing technology not prohibited by other law; or

(iv) by publishing notice of the breach of system security:

(A) in a newspaper of general circulation; and

(B) as required in Section 45-1-101.

(b) If a person maintains the person's own notification procedures as part of an information security policy for the treatment of personal information the person is considered to be in compliance with this chapter's notification requirements if the procedures are otherwise consistent with this chapter's timing requirements and the person notifies each affected Utah resident in accordance with the person's information security policy in the event of a breach.

(c) A person who is regulated by state or federal law and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with this part if the person notifies each affected Utah resident in accordance with the other applicable law in the event of a breach.

(6) A waiver of this section is contrary to public policy and is void and unenforceable.

XLVIII. VERMONT

§ 2435. Notice of security breaches

(a) This section shall be known as the Security Breach Notice Act.

(b) Notice of breach.

(1) Except as set forth in subsection (d) of this section, any data collector that owns or licenses computerized personally identifiable information that includes personal information concerning a consumer shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach. Notice of the security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency, as provided in subdivisions (3) and (4) of this subsection (b), or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.

(2) Any data collector that maintains or possesses computerized data containing personally identifiable information of a consumer that the data collector does not own or license or any data collector that acts or conducts business in Vermont that maintains or possesses records or data containing personally identifiable information that the data collector does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subdivisions (3) and (4) of this subsection (b).

(3) A data collector or other entity subject to this subchapter shall provide notice of a breach to the Attorney General or to the Department of Financial Regulation, as applicable, as follows:

(A) A data collector or other entity regulated by the Department of Financial Regulation under Title 8 or this title shall provide notice of a breach to the Department. All other data

collectors or other entities subject to this subchapter shall provide notice of a breach to the Attorney General.

(B)(i) The data collector shall notify the Attorney General or the Department, as applicable, of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach within 14 business days, consistent with the legitimate needs of the law enforcement agency as provided in this subdivision (3) and subdivision (4) of this subsection (b), of the data collector's discovery of the security breach or when the data collector provides notice to consumers pursuant to this section, whichever is sooner.

(ii) Notwithstanding subdivision (B)(i) of this subdivision (b)(3), a data collector who, prior to the date of the breach, on a form and in a manner prescribed by the Attorney General, had sworn in writing to the Attorney General that it maintains written policies and procedures to maintain the security of personally identifiable information and respond to a breach in a manner consistent with Vermont law shall notify the Attorney General of the date of the security breach and the date of discovery of the breach and shall provide a description of the breach prior to providing notice of the breach to consumers pursuant to subdivision (1) of this subsection (b).

(iii) If the date of the breach is unknown at the time notice is sent to the Attorney General or to the Department, the data collector shall send the Attorney General or the Department the date of the breach as soon as it is known.

(iv) Unless otherwise ordered by a court of this State for good cause shown, a notice provided under this subdivision (3)(B) shall not be disclosed to any person other than the Department, the authorized agent or representative of the Attorney General, a State's Attorney, or another law enforcement officer engaged in legitimate law enforcement activities without the consent of the data collector.

(C)(i) When the data collector provides notice of the breach pursuant to subdivision (1) of this subsection (b), the data collector shall notify the Attorney General or the Department, as applicable, of the number of Vermont consumers affected, if known to the data collector, and shall provide a copy of the notice provided to consumers under subdivision (1) of this subsection (b).

(ii) The data collector may send to the Attorney General or the Department, as applicable, a second copy of the consumer notice, from which is redacted the type of personally identifiable information that was subject to the breach, and which the Attorney General or the Department shall use for any public disclosure of the breach.

XLIX. VIRGIN ISLANDS

§ 2208 Notices of security breach

(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the Virgin Islands whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c), or any

measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
(c) The notification required by this section may be delayed, if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.
(d) For purposes of this section, 'breach of the security of the syste m' means unauthorized acquisition of computerized data that compromises the se curity, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
(e) For purposes of this section, 'personal information' means an in dividual'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.
(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(f) For purposes of this section, 'personal information' does not in clude publicly available information that is lawfully made available to the general public from federal, state, or territorial government records.
(g) For purposes of this section, 'notice' may be provided by one of the following methods:
(1) Written notice.
(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of Title 15 of the United States Code.
(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed $100,000, or that the affected class of subject persons to be notified exceeds 50,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
(A) E-mail notice when the agency has an e-mail address for the subject persons.
(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.
(C) Notification to major territory-wide media.
(h) Notwithstanding subsection (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

§ 2209 Disclosure of breach of security

(a) Any person or business that conducts business in the Virgin Islands, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the Virgin Islands whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
(d) For purposes of this section, 'breach of the security of the syste m' means unauthorized acquisition of computerized data that compromises the se curity, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
(e) For purposes of this section, 'personal information' means an in dividual'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.
(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(f) For purposes of this section, 'personal information' does not in clude publicly available information that is lawfully made available to the general public from federal, state, or local government records.
(g) For purposes of this section, 'notice' may be provided by one of the following methods:
(1) Written notice.
(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of subject persons to be notified exceeds 50,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:
(A) E-mail notice when the person or business has an e-mail address for the subject persons.
(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.
(C) Notification to major territory-wide media.

(h) Notwithstanding subsection (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this subchapter is 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.

L. VIRGINIA

A Code Ann. § 18.2-186.6

§ 18.2-186.6. Breach of personal information notification

A. As used in this section:
"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.
"Encrypted" means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable.
"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.
"Financial institution" has the meaning given that term in 15 U.S.C. § 6809 (3).
"Individual" means a natural person.
"Notice" means:
1. Written notice to the last known postal address in the records of the individual or entity;
2. Telephone notice;
3. Electronic notice; or
4. Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described in subdivisions 1, 2, or 3 of this definition. Substitute notice consists of all of the following:

a. E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents;
b. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and
c. Notice to major statewide media.
Notice required by this section shall not be considered a debt communication as defined by the Fair Debt Collection Practices Act in 15 U.S.C. § 1692a.
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.
“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; or
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.
The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.
“Redact” means alteration or truncation of data such that no more than the following are accessible as part of the personal information:
1. Five digits of a social security number; or
2. The last four digits of a driver's license number, state identification card number, or account number.
B. If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay. 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. Notice shall

be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.
C. An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.
D. An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the personal information was accessed and acquired by an unauthorized person or the individual or entity reasonably believes the personal information was accessed and acquired by an unauthorized person.
E. In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to this section, the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a (p), of the timing, distribution, and content of the notice.
F. 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.
G. An entity that is subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) and maintains procedures for notification of a breach of the security of the system in accordance with the provision of that Act and any rules, regulations, or guidelines promulgated thereto shall be deemed to be in compliance with this section.
H. 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 state or federal regulator shall be in compliance with this section.
I. Except as provided by subsections J and K, pursuant to the enforcement duties and powers of the Office of the Attorney General, the Attorney General may bring an action to address violations of this section. The Office of the Attorney General may impose a civil penalty not to exceed $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation. Nothing in this section shall limit an individual from recovering direct economic damages from a violation of this section.
J. A violation of this section by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator.
K. A violation of this section by an individual or entity regulated by the State Corporation Commission's Bureau of Insurance shall be enforced exclusively by the State Corporation Commission.
L. The provisions of this section shall not apply to criminal intelligence systems subject to the restrictions of 28 C.F.R. Part 23 that are maintained by law-enforcement agencies of the

Commonwealth and the organized Criminal Gang File of the Virginia Criminal Information Network (VCIN), established pursuant to Chapter 2 (§ 52-12 et seq.) of Title 52.
M. Notwithstanding any other provision of this section, any employer or payroll service provider that owns or licenses computerized data relating to income tax withheld pursuant to Article 16 (§ 58.1-460 et seq.) of Chapter 3 of Title 58.1 shall notify the Office of the Attorney General without unreasonable delay after the discovery or notification of unauthorized access and acquisition of unencrypted and unredacted computerized data containing a taxpayer identification number in combination with the income tax withheld for that taxpayer that compromises the confidentiality of such data and that creates a reasonable belief that an unencrypted and unredacted version of such information was accessed and acquired by an unauthorized person, and causes, or the employer or payroll provider reasonably believes has caused or will cause, identity theft or other fraud. With respect to employers, this subsection applies only to information regarding the employer's employees, and does not apply to information regarding the employer's customers or other non-employees.
Such employer or payroll service provider shall provide the Office of the Attorney General with the name and federal employer identification number of the employer as defined in § 58.1-460 that may be affected by the compromise in confidentiality. Upon receipt of such notice, the Office of the Attorney General shall notify the Department of Taxation of the compromise in confidentiality. The notification required under this subsection that does not otherwise require notification under this section shall not be subject to any other notification, requirement, exemption, or penalty contained in this section.

LI. WASHINGTON

19.255.010. Disclosure, notice--Definitions--Rights, remedies

(1) Any person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.
(2) Any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
(3) 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. The

notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
(4) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.
(5) For purposes of this section, “personal information” means an individual's first name or first initial and last name in combination with any one or more of the following data elements:
(a) Social security number;
(b) Driver's license number or Washington identification card number; or
(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(6) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
(7) For purposes of this section, “secured” means encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.
(8) For purposes of this section and except under subsections (9) and (10) of this section, “notice” may be provided by one of the following methods:
(a) Written notice;
(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or
(c) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:
(i) Email notice when the person or business has an email address for the subject persons;
(ii) Conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one; and
(iii) Notification to major statewide media.
(9) A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.
(10) A covered entity under the federal health insurance portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et seq., is deemed to have complied with the requirements of this section 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, Public Law 111-5 as it existed on July 24, 2015. Covered entities shall notify the attorney general pursuant to subsection (15) of this

section in compliance with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5 as it existed on July 24, 2015, notwithstanding the notification requirement in subsection (16) of this section.
(11) 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 section with respect to "sensitive customer information" as defined in the interagency guidelines establishing information security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they existed on July 24, 2015, if the financial institution provides notice to affected consumers pursuant to the interagency guidelines and the notice complies with the customer notice provisions of the interagency guidelines establishing information security standards and the interagency guidance on response programs for unauthorized access to customer information and customer notice under 12 C.F.R. Part 364 as it existed on July 24, 2015. The entity shall notify the attorney general pursuant to subsection (15) of this section in addition to providing notice to its primary federal regulator.
(12) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.
(13)(a) Any consumer injured by a violation of this section may institute a civil action to recover damages.
(b) Any person or business that violates, proposes to violate, or has violated this section may be enjoined.
(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.
(14) Any person or business 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; and
(iii) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.
(15) Any person or business 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, by the time notice is provided to affected consumers, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the attorney general. The person or business shall also provide to the attorney general the number of Washington consumers affected by the breach, or an estimate if the exact number is not known.
(16) Notification to affected consumers and to the attorney general under this section must be made in the most expedient time possible and without unreasonable delay, no more than forty-five calendar days after the breach was discovered, unless at the request of law enforcement as

provided in subsection (3) of this section, or due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
(17) The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this section. For actions brought by the attorney general to enforce this section, the legislature finds that the practices covered by this section are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. For actions brought by the attorney general to enforce this section, a violation of this section is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of applying the consumer protection act, chapter 19.86 RCW. An action to enforce this section may not be brought under RCW 19.86.090.

West's RCWA 42.56.590

42.56.590. Personal information--Notice of security breaches

(1)(a) Any agency that owns or licenses data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.
(b) For purposes of this section, “agency” means the same as in RCW 42.56.010.
(2) Any agency that maintains data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
(3) 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. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
(4) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.
(5) For purposes of this section, “personal information” means an individual's first name or first initial and last name in combination with any one or more of the following data elements:
(a) Social security number;

(b) Driver's license number or Washington identification card number; or
(c) Full account number, credit or debit card number, or any required security code, access code, or password that would permit access to an individual's financial account.
(6) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
(7) For purposes of this section, “secured” means encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.
(8) For purposes of this section and except under subsections (9) and (10) of this section, notice may be provided by one of the following methods:
(a) Written notice;
(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or
(c) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
(i) Email notice when the agency has an email address for the subject persons;
(ii) Conspicuous posting of the notice on the agency's web site page, if the agency maintains one; and
(iii) Notification to major statewide media.
(9) An agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.
(10) A covered entity under the federal health insurance portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et seq., is deemed to have complied with the requirements of this section 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, Public Law 111-5 as it existed on July 24, 2015. Covered entities shall notify the attorney general pursuant to subsection (14) of this section in compliance with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5 as it existed on July 24, 2015, notwithstanding the notification requirement in subsection (15) of this section.
(11) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.
(12)(a) Any individual injured by a violation of this section may institute a civil action to recover damages.
(b) Any agency that violates, proposes to violate, or has violated this section may be enjoined.
(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

(13) Any agency 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 agency 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) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.
(14) Any agency 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, by the time notice is provided to affected individuals, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the attorney general. The agency shall also provide to the attorney general the number of Washington residents affected by the breach, or an estimate if the exact number is not known.
(15) Notification to affected individuals and to the attorney general must be made in the most expedient time possible and without unreasonable delay, no more than forty-five calendar days after the breach was discovered, unless at the request of law enforcement as provided in subsection (3) of this section, or due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

LII. WEST VIRGINIA

§46A-2A-102. Notice of breach of security of computerized personal information.

(a) An individual or entity that owns or licenses computerized data that includes personal information shall give notice of any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person 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. Except as provided in subsection (e) of this section or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the notice shall be made without unreasonable delay.
(b) An individual or entity must give notice of the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state.
(c) An individual or entity that maintains computerized data that includes personal information that the individual or 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 system as soon as practicable following

discovery, if the personal information was or the entity reasonably believes was accessed and acquired by an unauthorized person.
(d) 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.
(e) 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. Notice required by this section must be made without unreasonable delay after the law-enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.
(f) If an entity is required to notify more than one thousand persons of a breach of security pursuant to this article, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined by 15 U.S.C. §1681a (p), of the timing, distribution and content of the notices. Nothing in this subsection shall be construed to require the entity to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients. This subsection shall not apply to an entity who is subject to Title V of the Gramm Leach Bliley Act, 15 U.S.C. 6801, *et seq*.
(g) The notice required by this section shall not be considered a debt communication as defined by the Fair Debt Collection Practice Act in 15 U.S.C. §1692a.

§46A-2A-103. Procedures deemed in compliance with security breach notice requirements.

(a) 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.
(b) 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.
(c) 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.

§46A-2A-104. Violations.

(a) Except as provided by subsection (c) of this section, failure to comply with the notice provisions of this article constitutes an unfair or deceptive act of practice in violation of section one hundred four, article six, chapter forty-six-a of this code, which may be enforced by the Attorney General pursuant to the enforcement provisions of this chapter.
(b) Except as provided by subsection (c) of this section, 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 one hundred fifty thousand dollars per breach of security of the system or series of breaches of a similar nature that are discovered in a single investigation.
(c) A violation of this article by a licensed financial institution shall be enforceable exclusively by the financial institution's primary functional regulator.

§46A-2A-105. Applicability.

This article shall apply to the discovery or notification of a breach of the security of the system that occurs on or after the effective date of this article.

LIII. WISCONSIN

Wis. Stat. § 134.98

134.98 Notice of unauthorized acquisition of personal information

(1) Definitions. In this section:
(a)1. “Entity” means a person, other than an individual, that does any of the following:
a. Conducts business in this state and maintains personal information in the ordinary course of business.
b. Licenses personal information in this state.
c. Maintains for a resident of this state a depository account as defined in s. 815.18(2)(e).
d. Lends money to a resident of this state.
2. “Entity” includes all of the following:
a. The state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the constitution or any law, including the legislature and the courts.
b. A city, village, town, or county.
(am) “Name” means an individual's last name combined with the individual's first name or first initial.
(b) “Personal information” means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:

1. The individual's social security number.
2. The individual's driver's license number or state identification number.
3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account.
4. The individual's deoxyribonucleic acid profile, as defined in s. 939.74(2d)(a).
5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.
(c) "Publicly available information" means any information that an entity reasonably believes is one of the following:
1. Lawfully made widely available through any media.
2. Lawfully made available to the general public from federal, state, or local government records or disclosures to the general public that are required to be made by federal, state, or local law.
(2) Notice required. (a) If an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.
(b) If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident of this state who is the subject of the personal information.
(bm) If a person, other than an individual, that stores personal information pertaining to a resident of this state, but does not own or license the personal information, knows that the personal information has been acquired by a person whom the person storing the personal information has not authorized to acquire the personal information, and the person storing the personal information has not entered into a contract with the person that owns or licenses the personal information, the person storing the personal information shall notify the person that owns or licenses the personal information of the acquisition as soon as practicable.
(br) If, as the result of a single incident, an entity is required under par. (a) or (b) to notify 1,000 or more individuals that personal information pertaining to the individuals has been acquired, the entity shall without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the timing, distribution, and content of the notices sent to the individuals.
(cm) Notwithstanding pars. (a), (b), (bm), and (br), an entity is not required to provide notice of the acquisition of personal information if any of the following applies:
1. The acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.
2. The personal information was acquired in good faith by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity.

(3) Timing and manner of notice; other requirements. (a) Subject to sub. (5), an entity shall provide the notice required under sub. (2) within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination as to reasonableness under this paragraph shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.
(b) An entity shall provide the notice required under sub. (2) by mail or by a method the entity has previously employed to communicate with the subject of the personal information. If an entity cannot with reasonable diligence determine the mailing address of the subject of the personal information, and if the entity has not previously communicated with the subject of the personal information, the entity shall provide notice by a method reasonably calculated to provide actual notice to the subject of the personal information.
(c) Upon written request by a person who has received a notice under sub. (2)(a) or (b), the entity that provided the notice shall identify the personal information that was acquired.
(3m) Regulated entities exempt. This section does not apply to any of the following:
(a) An entity that is subject to, and in compliance with, the privacy and security requirements of 15 USC 6801 to 6827, or a person that has a contractual obligation to such an entity, if the entity or person has in effect a policy concerning breaches of information security.
(b) An entity that is described in 45 CFR 164.104(a), if the entity complies with the requirements of 45 CFR part 164.
(4) Effect on civil claims. Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.
(5) Request by law enforcement not to notify. A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required under sub. (2) for any period of time and the notification process required under sub. (2) shall begin at the end of that time period. Notwithstanding subs. (2) and (3), if an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.
(6m) Local ordinances or regulations prohibited. No city, village, town, or county may enact or enforce an ordinance or regulation that relates to notice or disclosure of the unauthorized acquisition of personal information.
(7m) Effect of federal legislation. If the joint committee on administrative rules determines that the federal government has enacted legislation that imposes notice requirements substantially similar to the requirements of this section and determines that the legislation does not preempt this section, the joint committee on administrative rules shall submit to the legislative reference bureau for publication in the Wisconsin administrative register a notice of its determination. This section does not apply after publication of a notice under this subsection.

LIV. WYOMING

Wyo. Stat. §§ 40-12-501 et seq.

§ 40-12-501. Definitions

(a) As used in this act:
(i) “Breach of the security of the data system” means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of this state. Good faith acquisition of personal identifying information by an employee or agent of a 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 identifying information is not used or subject to further unauthorized disclosure;
(ii) “Consumer” means any person who is utilizing or seeking credit for personal, family or household purposes;
(iii) “Consumer reporting agency” means any person whose business is the assembling and evaluating of information as to the credit standing and credit worthiness of a consumer, for the purposes of furnishing credit reports, for monetary fees and dues to third parties;
(iv) “Credit report” means any written or oral report, recommendation or representation of a consumer reporting agency as to the credit worthiness, credit standing or credit capacity of any consumer and includes any information which is sought or given for the purpose of serving as the basis for determining eligibility for credit to be used primarily for personal, family or household purposes;
(v) “Creditor” means the lender of money or vendor of goods, services or property, including a lessor under a lease intended as a security, rights or privileges, for which payment is arranged through a credit transaction, or any successor to the right, title or interest of any such lender or vendor, and an affiliate, associate or subsidiary of any of them or any director, officer or employee of any of them or any other person in any way associated with any of them;
(vi) “Financial institution” means any person licensed or chartered under the laws of any state or the United States as a bank holding company, bank, savings and loan association, credit union, trust company or subsidiary thereof doing business in this state;
(vii) “Personal identifying information” means the first name or first initial and last name of a person in combination with one (1) or more of the data elements specified in W.S. 6-3-901(b)(iii) through (xiv), when the data elements are not redacted;
(A) to (E) Repealed by Laws 2015, ch. 63, § 2, eff. July 1, 2015.
(viii) “Redact” means alteration or truncation of data such that no more than five (5) digits of the data elements provided in subparagraphs (vii)(A) through (D) of this subsection are accessible as part of the personal information;
(ix) “Security freeze” means a notice placed in a consumer's credit report, at the request of the consumer, that prohibits the credit rating agency from releasing the consumer's credit report or any information from it relating to an extension of credit or the opening of a new account, without the express authorization of the consumer;
(x) “Substitute notice” means:
(A) An electronic mail notice when the person or business has an electronic mail address for the subject persons;
(B) Conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; and
(C) Publication in applicable local or statewide media.

(xi) “This act” means W.S. 40-12-501 through 40-12-511.
(b) “Personal identifying information” as defined in paragraph (a)(vii) of this section does not include information, regardless of its source, contained in any federal, state or local government records or in widely distributed media that are lawfully made available to the general public.

§ 40-12-502. Computer security breach; notice to affected persons

(a) An individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. If the investigation determines that the misuse of personal identifying information about a Wyoming resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Wyoming resident. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.
(b) The notification required by this section may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation.
(c) Any financial institution as defined in 15 U.S.C. 6809 or federal credit union as defined by 12 U.S.C. 1752 that maintains notification procedures subject to the requirements of 15 U.S.C. 6801(b)(3) and 12 C.F.R. Part 364 Appendix B or Part 748 Appendix B, is deemed to be in compliance with this section if the financial institution notifies affected Wyoming customers in compliance with the requirements of 15 U.S.C. 6801 through 6809 and 12 C.F.R. Part 364 Appendix B or Part 748 Appendix B.
(d) For purposes of this section, notice to consumers may be provided by one (1) of the following methods:
(i) Written notice;
(ii) Electronic mail notice;
(iii) Substitute notice, if the person demonstrates:
(A) That the cost of providing notice would exceed ten thousand dollars ($10,000.00) for Wyoming-based persons or businesses, and two hundred fifty thousand dollars ($250,000.00) for all other businesses operating but not based in Wyoming;
(B) That the affected class of subject persons to be notified exceeds ten thousand (10,000) for Wyoming-based persons or businesses and five hundred thousand (500,000) for all other businesses operating but not based in Wyoming; or
(C) The person does not have sufficient contact information.
(iv) Substitute notice shall consist of all of the following:
(A) Conspicuous posting of the notice on the Internet, the World Wide Web or a similar proprietary or common carrier electronic system site of the person collecting the data, if the person maintains a public Internet, the World Wide Web or a similar proprietary or common carrier electronic system site; and

(B) Notification to major statewide media. The notice to media shall include a toll-free phone number where an individual can learn whether or not that individual's personal data is included in the security breach.
(e) Notice required under subsection (a) of this section shall be clear and conspicuous and shall include, at a minimum:
(i) A toll-free number:
(A) That the individual may use to contact the person collecting the data, or his agent; and
(B) From which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies.
(ii) The types of personal identifying information that were or are reasonably believed to have been the subject of the breach;
(iii) A general description of the breach incident;
(iv) The approximate date of the breach of security, if that information is reasonably possible to determine at the time notice is provided;
(v) In general terms, the actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches;
(vi) Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports;
(vii) Whether notification was delayed as a result of a law enforcement investigation, if that information is reasonably possible to determine at the time the notice is provided.
(f) The attorney general may bring an action in law or equity to address any violation of this section and for other relief that may be appropriate to ensure proper compliance with this section, to recover damages, or both. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law.
(g) Any person who maintains computerized data that includes personal identifying information on behalf of another business entity shall disclose to the business entity for which the information is maintained any breach of the security of the system as soon as practicable following the determination that personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person. The person who maintains the data on behalf of another business entity and the business entity on whose behalf the data is maintained may agree which person or entity will provide any required notice as provided in subsection (a) of this section, provided only a single notice for each breach of the security of the system shall be required. If agreement regarding notification cannot be reached, the person who has the direct business relationship with the resident of this state shall provide notice subject to the provisions of subsection (a) of this section.
(h) A covered entity or business associate that is subject to and complies with the Health Insurance Portability and Accountability Act, and the regulations promulgated under that act, 45 C.F.R. Parts 160 and 164, is deemed to be in compliance with this section if the covered entity or business associate notifies affected Wyoming customers or entities in compliance with the requirements of the Health Insurance Portability and Accountability Act and 45 C.F.R. Parts 160 and 164.