



Comparison of US State and Federal Security Breach Notification Laws

Current through September 1, 2017

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Alaska.....	2	New Hampshire.....	105
Arizona.....	6	New Jersey.....	108
Arkansas.....	9	New Mexico.....	113
California.....	11	New York.....	116
Colorado.....	22	North Carolina.....	120
Connecticut.....	24	North Dakota.....	124
Delaware.....	28	Ohio.....	128
District of Columbia.....	31	Oklahoma.....	132
Florida.....	33	Oregon.....	136
Georgia.....	37	Pennsylvania.....	141
Guam.....	41	Puerto Rico.....	144
Hawaii.....	44	Rhode Island.....	147
Idaho.....	48	South Carolina.....	151
Illinois.....	50	Tennessee.....	153
Indiana.....	55	Texas.....	156
Iowa.....	58	Utah.....	160
Kansas.....	61	Vermont.....	162
Kentucky.....	63	Virginia.....	168
Louisiana.....	65	Virgin Islands (US).....	172
Maine.....	67	Washington.....	174
Maryland.....	70	West Virginia.....	179
Massachusetts.....	76	Wisconsin.....	183
Michigan.....	80	Wyoming.....	187
Minnesota.....	85	Gramm-Leach-Bliley Act (GLBA).....	192
Mississippi.....	87	Health Insurance Portability and Accountability Act of 1996 (HIPAA)202	
Missouri.....	89		
Montana.....	93		
Nebraska.....	98		
Nevada.....	101		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Alaska								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Alaska Stat. §45.48.010 <i>et seq.</i>	<p>Covered entities: A “covered person” who “owns or licenses personal information in any form that includes personal information on a state resident.” (§45.48.010(a))</p> <p>“Covered person” is defined as “a (A) person doing business; (B) governmental agency; or (C) person with more than 10 employees.” (§45.48.090(2))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “[I]nformation 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) social security number; (ii) driver’s license or state ID card number; (iii) the Individual’s account number, credit card</p>	<p>Breach definition: A “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.” (§45.48.090(1))</p> <p>“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</p>	<p>Residents: “[E]ach state resident whose personal information was subject to the breach.” (§45.48.010(a))</p> <p>Credit reporting agency notice requirement: Yes. “(a) If an information collector is required . . . 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</p>	<p>Timing: “An information collector shall make the disclosure required by . . . this section in the most expeditious time possible and without unreasonable delay, except as [requested by law enforcement] and as necessary to determine the scope of the breach and restore the reasonable integrity of the information system.” (§45.48.010(b))</p> <p>Delay: “An information collector may delay disclosing the breach . . . if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation. However, the information collector shall disclose the breach to the state resident in the most expeditious time possible and without</p>	<p>Method: “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 <i>et seq.</i> (Electronic Signatures in Global and National Commerce Act); or (3) if the</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: No.</p>	<p>State enforcement: “If an information collector . . . 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 . . . 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.” (§45.48.080(b)(1))</p> <p>Private right of action: Yes. Alaska residents</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Alaska								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	required to comply with [the law's requirement to notify state residents]. 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 . . . this section." (§45.48.070(a)) "[C]ooperate' means sharing with the information distributor	number, or debit card number, if no access code, personal identification number, or password is required to access the account; (iv) the Individual's account number, credit card number, or debit card number in combination with an access code, a personal identification number, or a password required to access the account; or (v) passwords, personal ID numbers, or other access codes for financial accounts." (§45.48.090(7))	(B)." (§45.48.090(1)) "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." (45.48.090(4)) Exception: "[T]he 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	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)." (§45.48.040) Government notice requirement: Possibly. The section of the law describing the risk of harm analysis could be	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." (§45.48.020)	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." (§45.48.030)		injured by such violations may seek relief under AS 45.50.471 - 45.50.56. However, "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." (§45.48.080(b))

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Alaska								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>information relevant to the breach, except for confidential business information or trade secrets.” (§45.48.070(a))</p> <p>“[I]f an information recipient notifies an information distributor of a breach under (a) of this section, the information distributor shall comply with [the law’s requirement to notify state residents] as if the breach occurred to the information system maintained by the information distributor.” (§45.48.070(b))</p>		<p>not make further unauthorized disclosure of the personal information.” (§45.48.050)</p> <p>Risk of harm analysis: Yes. “[D]isclosure 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 shall not be</p>	<p>read as suggesting that the state attorney general must be notified whenever there is a breach: “[D]isclosure 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 notification required by this subsection shall not be considered a public record open to inspection by the public.” Because the section says that the determination about whether to notify consumers should be made after notification to the state Attorney General, it could be read as meaning that</p>				

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Alaska								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			considered a public record open to inspection by the public.” (§45.48.010(c))	the state Attorney General should be notified whenever there is a breach. However, notification to the Attorney General would not be required if the determination is made that there was no “breach of security” as defined by the statute. (§45.48.010(c)).				

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Arizona								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Ariz. Rev. Stat. Ann. §18-545	<p>Covered entities: “[A] person that conducts business in [Arizona] and that owns or licenses unencrypted computerized data that includes personal information.” (§18-545(A))</p> <p>Service provider requirement: Yes. 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.” (§18-545(B))</p>	<p>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, 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</p>	<p>Breach definition: A “breach of the security system” is defined as “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.” (§18-545(L)(1))</p> <p>Exception: “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</p>	<p>Residents: Individuals affected by the breach, where “individual” is defined as “a person that is a resident of this state as determined by a principal mailing address in [Arizona] as reflected in the records of the person conducting business in this state at the time of the breach.” (§§18-545(A), (L)(4))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: No.</p>	<p>Timing: Following a “determination that there has been a breach in the security system . . . notice shall be made in the most expedient manner possible and without unreasonable delay subject to the needs of law enforcement as provided in [§18-545(C)] 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.” (§18-545(A))</p> <p>Delay: “The notification required by [§18-545(A)] may be delayed if a law enforcement agency advises the person that the notification will impede a criminal investigation.” (§18-545(C))</p>	<p>Method: “The disclosure required by [§18-545(A)] 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</p>	<p>For establishing own notification method: Yes. “A person who maintains the person’s own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the person notifies subject individuals in accordance with the person’s policies if a breach of the security system occurs.” (§18-545(E))</p> <p>For following interagency guidelines: Yes. -- “A person that complies with the notification requirements or</p>	<p>State enforcement: “The attorney general may bring an action to obtain actual damages for a wilful [sic] and knowing violation . . . 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.” (§18-545(H))</p> <p>Private right of action: No. The law “may only be enforced by the attorney general.” (§18-545(H))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Arizona								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>in combination with any required security code, access code or password that would permit access to the individual's financial account.” (§18-545(L)(6)(a))</p> <p>Exception: 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.” (§18-545(L)(6)(b))</p>	<p>security system if the personal information is not used for a purpose unrelated to the person or subject to further wilful [sic] unauthorized disclosure.” (§18-545(L)(1))</p> <p>Risk of harm analysis: Yes. -- “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.” (§18-545(G)) -- A breach occurs only if the security or confidentiality of an individual's personal information is materially compromised and if the event “causes or</p>			<p>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.” (§18-545(D))</p> <p>Substitute notice: “Substitute notice shall consist of all of the following: (a) Electronic mail notice if the person has electronic mail addresses for the individuals subject to the notice. (b) Conspicuous posting of the notice on the web site of the person if the person maintains one. (c) Notification to major statewide media.” (§18-545(D)(4))</p>	<p>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.” (§18-545(F))</p> <p>-- “This section [also] does not apply to either of the following: 1. A person subject to title V of the Gramm-Leach-Bliley act of 1999 (P.L. 106-102; 113 Stat. 1338; 15 United States Code sections 6801 through 6809). 2. Covered entities as defined under regulations implementing the health insurance portability and accountability act, 45 Code of Federal Regulations section 160.103 (1996).” (§18-545(J))</p>	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Arizona								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			is reasonably likely to cause substantial economic loss to an individual.” (§18-545(L)(1))					

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Arkansas								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Ark. Code Ann. §4-110-101 <i>et seq.</i>	<p>Covered entities: “Any person or business that acquires, owns, or licenses computerized data that includes personal information” of Arkansas residents. (§4-110-105(a)(1))</p> <p>Service provider requirement: Yes. “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,</p>	<p>Personal information: “[A]n individual’s first name or first initial and his or her last name in combination with any one (1) or more of the following data elements, when either the name or the data element is not encrypted or redacted: (A) Social security number; (B) Driver’s license number or Arkansas identification card number; (C) Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account; and (D) Medical</p>	<p>Breach definition: A “[b]reach of the security of the system” is the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.” (§4-110-103(1)(A))</p> <p>Exception: “[D]oes not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure.” (§4-110-103(1)(B))</p>	<p>Residents: “[A]ny resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (§4-110-105(a)(1))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: No.</p>	<p>Timing: “[D]isclosure 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 [§4-110-105(c)] or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” (§4-110-105(a)(2))</p> <p>Delay: Notice may be delayed “if a law enforcement agency determines that the notification will impede a criminal investigation.” Notification “shall be made after the law enforcement agency determines that it will not compromise the investigation.” (§4-110-105(c))</p>	<p>Method: “[N]otice 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) 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</p>	<p>For establishing own notification method: Yes. If a person or business “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 the affected persons in accordance with its policies in the event of a breach of the security of the system.” (§4-110-105(f))</p> <p>For following interagency guidelines: Yes. “The provisions of this chapter do not apply to a person or business that is</p>	<p>State enforcement: “Any violation of this chapter is punishable by action of the Attorney General under the provisions of Ark. Code Ann. § 4-88-101 <i>et seq.</i> [regulating deceptive trade practices].” (§4-110-108)</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Arkansas								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	or is reasonably believed to have been, acquired by an unauthorized person.” (§4-110-105(b))	information.*” (§4-110-103(7)) * Medical information is defined as “any individually identifiable information, in electronic or physical form, regarding the individual’s medical history or medical treatment or diagnosis by a health care professional.” (§4-110-103(5))	Risk of harm analysis: Yes. Notification “is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.” (§4-110-105(d))			information.” (§4-110-105(e)) Substitute notice: “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.” (§4-110-105(e)(3)(B))	regulated by a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breaches of the security of personal information than that provided by this chapter [and the person or business complies] with the state or federal law....” (§4-110-106(a)(1), (2))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

California								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Cal. Civ. Code §§ 1798.29, 1798.80 <i>et seq.</i>	<p>Covered entities: “A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information.” (§1798.82(a))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “(1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social security number. (B) Driver’s license number or California 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</p>	<p>Breach definition: A “breach of the security of the system” is the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.” (§1798.82(g))</p> <p>Exception: “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.” (§1798.82(g))</p>	<p>Residents: “[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.” (§1798.82(a))</p> <p>Credit reporting</p>	<p>Timing: “[F]ollowing discovery or notification of the breach in the security of the data . . . [t]he 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 [§1798.82(c)], or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” (§1798.82(a))</p> <p>Non-binding guidance from the California Office of Privacy Protection provides that notice should be given “within 10 business days” of a determination “that the information was, or is reasonably believed to have been, acquired by an</p>	<p>Method: “[N]otice” may be provided by one of the following methods: (1) Written notice. (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code. (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information.” (§1798.82(j))</p>	<p>For establishing own notification method: Yes. “[A] person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.” (§1798.82(l))</p> <p>For following interagency guidelines: Yes. “A covered entity under the federal Health Insurance</p>	<p>State enforcement: “Any business that violates, proposes to violate, or has violated this title may be enjoined.” (§1798.84(e))</p> <p>Private right of action: Yes. -- “Any customer injured by a violation of this title may institute a civil action to recover damages.” (§1798.84(b)) -- “Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.” (§1798.84(a)) -- “The rights and remedies available under [the breach notification law] are cumulative to each other and to any other rights and remedies available under law.” (§1798.84(h))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

California								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	been, acquired by an unauthorized person.” (§1798.82(b))	information.* (E) Health insurance information.** (F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.” OR “(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.” (§1798.82(h)) * Medical information means “any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a	Non-binding guidance from the California Office of Privacy Protection suggests considering the following factors when determining whether unencrypted notice-triggering information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person: “(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 unencrypted notice-triggering information; (2) Indications that the information has been downloaded or copied; and (3) Indications that the information was	agency notice requirement: No. Government notice requirement: Yes. “Any person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General.” (§1798.82(f))	unauthorized person,” subject to the needs of law enforcement. <i>Recommended Practices on Notice of Security Breach Involving Personal Information</i> , California Office of Privacy Protection (Jan. 2012) Delay: Notice may be delayed “if a law enforcement agency determines that the notification will impede a criminal investigation.” Notification “shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.” (§1798.82(c))	Substitute notice: “Substitute notice shall consist of all of the following: (A) Email notice when the person or business has an email address for the subject persons. (B) Conspicuous posting, for a minimum of 30 days, of the notice on the Internet Web site page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person’s or business’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	Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.” (§1798.82(e))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

California								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>health care professional.” (§1798.82(i)(2))</p> <p>** 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.” (§1798.82(i)(3))</p> <p>Exception: Personal information “does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.”</p>	<p>used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.”</p> <p><i>Recommended Practices on Notice of Security Breach Involving Personal Information</i>, California Office of Privacy Protection (Jan. 2012), available at http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/recom_breach_prac.pdf</p> <p>Risk of harm analysis: No, except to the extent the definition of “breach” may incorporate elements of such a test.</p>			<p>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.” (§1798.82(j)(3))</p> <p>Notice contents requirement: “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</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

California								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		(§1798.82(i)(1))				<p>Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.</p> <p>(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.</p> <p>(B) The title and headings in the notice shall be clearly and conspicuously displayed.</p> <p>(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.</p> <p>(D) For a written notice described in [§1798.82(j)(1)], use of the model security breach</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

California								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>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.</p> <p>(E) For an electronic notice described in [§1798.82(j)(2)], 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.</p> <p>(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:</p>		

California								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>(A) The name and contact information of the reporting person or business subject to this section.</p> <p>(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.</p> <p>(C) If the information is possible to determine at the time the notice is provided, then any of the following:</p> <ul style="list-style-type: none"> (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. <p>The notification shall also include the date of the notice.</p> <p>(D) Whether notification was delayed as a result of a law</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

California								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>enforcement investigation, if that information is possible to determine at the time the notice is provided.</p> <p>(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.</p> <p>(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.</p> <p>(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

California								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of [§1798.82(h)].</p> <p>(3) At the discretion of the person or business, the security breach notification may also include any of the following:</p> <p>(A) Information about what the person or business has done to protect individuals whose information has been breached.</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

California								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.” (§1798.82(d))</p> <p>Exception: “In the case of a breach of the security of the system involving personal information defined in paragraph (2) of [§1798.82(h)] for an online account, and no other personal information defined in paragraph (1) of [§1798.82(h)], the person or business 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 promptly to change</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

California								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.” (§1798.82(j)(4))</p> <p>Exception: “In the case of a breach of the security of the system involving personal information defined in paragraph (2) of [§1798.82(h)] for login credentials of an email account furnished by the person or business, the person or business shall not comply with this</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

California								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						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 [§1798.82(j)] 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 or business knows the resident customarily accesses the account.” (§1798.82(j)(5))		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Colorado								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Colo. Rev. Stat. §6-1-716	<p>Covered entities: “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.” (§6-1-716(2)(a))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “[A] Colorado resident’s first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secure by any other method rendering the name or the element unreadable or unusable: (A) Social security number; (B) Driver’s license number or identification card number; (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that</p>	<p>Breach definition: “‘Breach of the security of the system’ means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.” (§6-1-716(1)(a))</p> <p>Exception: “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.” (§6-1-716(1)(a))</p>	<p>Residents: Notice must be given to the “affected Colorado resident.” (§6-1-716(2)(a))</p> <p>Credit reporting agency notice requirement: Yes. If a “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.” (§6-1-716(2)(d))</p>	<p>Timing: “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.” (§6-1-716(2)(a))</p> <p>Delay: Notice 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.” (§6-1-716(2)(c))</p>	<p>Method: “‘Notice’ means (I) Written notice to the postal address listed in the records of the individual or commercial entity; (II) Telephonic notice; (III) Electronic notice, if a primary means of communication by the individual or commercial entity with a Colorado resident is by electronic means or the notice provided is consistent with the provisions regarding electronic records and signatures or (IV) Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed two hundred fifty thousand dollars, the affected class of persons to be</p>	<p>For establishing own notification method: Yes. “[A]n 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.” (§6-1-716(3)(a))</p> <p>For following interagency guidelines: Yes. “An individual or a</p>	<p>State enforcement: “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.” (§6-1-716(4))</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Colorado								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	system immediately following discovery of a breach, if misuse of personal information about a Colorado resident occurred or is likely to occur.” (§6-1-716(2)(b))	would permit access to a resident’s financial account.” (§6-1-716(1)(d)(I)) Exception: Personal information “does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.” (§6-1-716(1)(d)(II))	Risk of harm analysis: Yes. After a reasonable investigation, a commercial entity must give notice of a breach unless “the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur.” (§6-1-716(2)(a))	Government notice requirement: No.		notified exceeds two hundred fifty thousand Colorado residents, or the individual or the commercial entity does not have sufficient contact information to provide notice.” (§6-1-716(1)(c)) Substitute notice: “Substitute notice consists of the following: (A) E-mail notice if the individual or the commercial entity has e-mail addresses for the members of the affected class of Colorado residents; (B) Conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains one; and (C) Notification to major statewide media.” (§6-1-716(1)(c)(IV))	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.” (§6-1-716(3)(b))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Connecticut								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Conn. Gen. Stat. §§36a-701b, 4e-70; [2015 Conn. Legis. Serv. P.A. 15-142 (S.B. 949)]	<p>Covered entities: “Any person who conducts business in [Connecticut], and who, in the ordinary course of such person’s business, owns, maintains or licenses computerized data that includes personal information.” (§36a-701b(b)(1))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “[A]n 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) Any 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.” (§36a-701b(a))</p> <p>Exception: “‘Personal information’ does not include publicly available information that is lawfully made</p>	<p>Breach definition: A “breach of security” is the “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.” (§36a-701b(a))</p> <p>Risk of harm analysis: Yes. “Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law</p>	<p>Residents: Any Connecticut resident “whose personal information was breached or is reasonably believed to have been breached.” (§36a-701b(b)(1))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: Yes. “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.” (§36a-701b(b)(2)(A))</p>	<p>Timing: “[F]ollowing the discovery of the breach . . . 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 [§36a-701b(d)] 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.” (§36a-701b(b)(1))</p>	<p>Method: “Any notice required by the provisions of this section may be provided by one of the following methods: (1) Written notice; (2) telephone notice; (3) electronic notice, provided such notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001; (4) substitute notice, provided such person demonstrates that the cost of providing notice in accordance with subdivision (1), (2) or (3) of this subsection would exceed two hundred fifty thousand dollars, that the affected class of subject persons to be notified exceeds five hundred thousand persons or</p>	<p>For establishing own notification method: Yes. “Any person that maintains such person’s own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies, as applicable, residents of this state, owners and licensees in accordance with such person’s policies in the event of a breach of security and in the case of notice to a resident, such person also notifies the Attorney</p>	<p>State enforcement: “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.” (§36a-701b(g))</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Connecticut								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>state was breached or is reasonably believed to have been breached.” (§36a-701b(c))</p> <p>Contractors: Connecticut law also places special requirements on state contractors. A “Contractor” is defined as “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.” (§4e-70(a)(1))</p> <p>Contractors must take special precautions with residents’ data. Any contract between the state or a state agency and a contractor must require that</p>	<p>available to the general public from federal, state or any local government records or widely distributed media.” (§36a-701b(a))</p>	<p>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.” (§36a-701b(b)(1))</p>			<p>the person does not have sufficient contact information.” (§36a-701b(e))</p> <p>Substitute notice: “Substitute notice shall consist of the following: (A) Electronic mail notice when the person, business or agency has an electronic mail address for the affected persons; (B) conspicuous posting of the notice on the web site of the person, business or agency if the person maintains one; and (C) notification to major state-wide media, including newspapers, radio and television.” (§36a-701b(e))</p> <p>Notice contents requirement: If a breach exposes Social Security Numbers, the notice to residents must include “appropriate</p>	<p>General not later than the time when notice is provided to the resident.” (§36a-701b(f))</p> <p>For following interagency guidelines: Yes. “Any person that maintains such [person’s own] 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) [of the Gramm Leach Bliley Act] shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies, as applicable, such residents of this state, owners, and licensees required to be notified under and in accordance</p>	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Connecticut								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>the contractor “[n]otify 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.” (§4e-70(b)(6))</p> <p>Every written agreement with a contractor must also: “(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,</p>					<p>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. [The covered entity] 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.” (§36a-701b(b)(2)(B))</p>	<p>with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security of the system.” (§36a-701b(f))</p>	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Connecticut								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>upon further investigation, the contractor believes no breach has occurred; and</p> <p>(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.” (§4e-70(e)(1)-(2))</p> <p>Health Insurers: Effective Oct. 1, 2017, health insurers and related companies will be subject to additional data privacy protections, and the Connecticut Insurance Commissioner will have authority to enforce those provisions. (P.A. 15-142 §5)</p>							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Delaware								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Del. Code Ann. tit. 6, §12B-101 <i>et seq.</i> ; H.B. 180 (effective April 14, 2018)	<p>Covered entities: “Any person who conducts business in this State and who owns or licenses computerized data that includes personal information.” (§12B-102(a))</p> <p>*“‘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.”</p> <p>Service provider requirement: Yes. “A person that maintains computerized data</p>	<p>Personal information: “[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</p>	<p>Breach definition: A “breach of security” means “[t]he unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.” (§12B-101(1)(a))</p> <p>Exception: --“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.” (§12B-101(1)(a))</p> <p>--“The unauthorized acquisition of computerized data that compromises</p>	<p>Residents: “[A]ny resident of this State whose personal information was breached or is reasonably believed to have been breached.” (§12B-102(a))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: Yes. “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.” (§12B-102(d))</p>	<p>Timing: “Notice ... must be made without unreasonable delay but not later than 60 days after determination of the breach of security.” (§12B-102(c))</p> <p>Delay: Notice required may be delayed if: “(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</p>	<p>Method: “‘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, the affected number of Delaware residents to be notified exceeds 100,000 residents, or that the</p>	<p>For establishing own notification method: Yes. “[A] person that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notice requirements of this chapter if the person notifies affected Delaware residents in accordance with its policies in the event of a breach of security.” (§12B-103(a))</p> <p>For following interagency guidelines: Yes. “Under this chapter, a person that is regulated by state or federal law,</p>	<p>State enforcement: “Pursuant to the enforcement duties and powers of the Director of Consumer Protection of the Department of Justice 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 entity person subject to this chapter from compliance with all other applicable provisions of law.” (§12B-104(a))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Delaware								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	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.” (§12B-102(b))	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.	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.” (§12B-101(1)(b)) Risk of harm analysis: Yes. “Any person who conducts business in this State and who owns or licenses computerized data that includes personal information shall		otherwise required ... to provide notice, could not, through reasonable diligence, identify within 60 days that the personal information of certain residents of this State was included in a breach of security, such person must provide the notice required by § 12B–102(a) ... 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(3)d.” (§12B-102(c))	person does not have sufficient contact information to provide notice.” (§12B-101(3)) Substitute 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) Notification to major statewide media, including newspapers, radio, and television and publication on the major social media platforms of the person providing notice.” (§12B-101(3)(d)) Breaches That Permit Access to Email Accounts: “In the case of a	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.” (§12B-103(b))	Private right of action: No. But “[n]othing in this chapter may be construed to modify any right which a person may have at common law, by statute, or otherwise.” (§12B-104(b))

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Delaware								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>9. An individual taxpayer identification number.” (§12B-101(4)(a))</p> <p>Exception: “[D]oes 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.” (§12B-101(4)(b))</p>	<p>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.” (§12B-102(a))</p>			<p>breach of security involving personal information defined in § 12B–101(4)a.6. 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(3) 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.” (§12B-102(f))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

District of Columbia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
D.C. Off'l Code §28-3851 <i>et seq.</i>	<p>Covered entities: “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.” (§28-3852(a))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “Personal information” means: (i) an individual’s first name or first initial and last name, or phone number, or address, and any one or more of the following data elements: (I) Social security number; or (II) Driver’s license number or District of Columbia Identification Card number; or (III) Credit card number or debit card number; or (ii) Any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual’s financial or credit</p>	<p>Breach definition: ““Breach of the security of the system” means unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data, that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.” (§28-3851(1))</p> <p>Exception: Does “not include a good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business if the personal information is not used improperly or subject to further unauthorized disclosure.” (§28-3851(1))</p>	<p>Residents: Notice must be given to “any District of Columbia resident whose personal information was included in the breach.” (§28-3852(a))</p> <p>Credit reporting agency notice requirement: Yes. If any person or entity is “required by [§28-3852(a) or §28-3852(b)] 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.” (§28-3852(c))</p> <p>Government notice requirement: No.</p>	<p>Timing: 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 [§28-3852(d)], and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” (§28-3852(a))</p> <p>Delay: Notice “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.” (§28-3851(d))</p>	<p>Method: ““Notify” or ‘notification’ means providing information through any one of the following methods: (A) Written notice; (B) Electronic notice, if the customer has consented to receipt of electronic notice consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act, approved June 30, 2000 (114 Stat. 641; 15 U.S.C.S. § 7001); or (C) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed \$50,000, the number of persons exceeds 100,000, or the person or business does not</p>	<p>For establishing own notification method: Yes. “[A] person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this 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.” (§28-3852(e))</p> <p>For following interagency guidelines: Yes.</p>	<p>Local enforcement: “The Attorney General may petition the Superior Court of the District of Columbia for temporary or permanent injunctive relief and for an award of restitution for property lost or damages suffered by District of Columbia residents as a consequence of the violation of this subchapter. In an action under this subsection, the Attorney General may recover a civil penalty not to exceed \$100 for each violation, the costs of the action, and reasonable attorney’s fees. Each failure to provide a District of Columbia resident with notification in accordance with this section shall constitute a separate violation.” (§28-3853(b))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

District of Columbia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
	expedient time possible following discovery.” (§28-3852(b))	account.” (§28-3851(3)(A)) Exception: Personal information “does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.” (§28-3851(3)(B))	Exception: “Acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party, shall not be deemed to be a breach of the security of the system.” (§28-3851(1)) Risk of harm analysis: No, except as definition of breach may incorporate such a test.			have sufficient contact information.” (§28-3851(2)) Substitute notice: “Substitute notice shall consist of all of the following: (I) E-mail notice when the person or business has an email 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 one; and (III) Notification to major local and, if applicable, national media.” (§28-3851(2)(C)(ii))	“A person or entity who maintains procedures for a breach notification system under Title V of the Gramm-Leach –Bliley Act . . . and provides notice in accordance with the Act, and any rules, regulations, guidance and guidelines thereto, to each affected resident in the event of a breach, shall be deemed to be in compliance with this section.” (§28-3852(g))	Private right of action: Yes. “Any District of Columbia resident injured by a violation of this subchapter may institute a civil action to recover actual damages, the costs of the action and reasonable attorney’s fees.” (§28-3853(a)) “The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.” (§28-3853(c))

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Florida								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Fla. Stat. Ann. §501.171	<p>Covered entities: “Covered entity” means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information.” (§501.171(1)(b))</p> <p>Service provider requirement: Yes. “(a) In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the</p>	<p>Personal information: “Personal information” means either of the following: a. An individual’s first name or first initial and last name in combination with any one or more of the following data elements for that individual: (I) A social security number; (II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (III) A financial account number or credit or debit card number, in combination with any required security code, access code, or</p>	<p>Breach definition: “Breach of security” or ‘breach’ means unauthorized access of data in electronic form containing personal information.” (§501.171(1)(a))</p> <p>Exception: “Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.” (§501.171(1)(a))</p> <p>Risk of harm analysis: Yes. “Notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement</p>	<p>Florida residents: “Each individual in [Florida] whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach.” (§501.171(4)(a))</p> <p>Credit reporting agency notice requirement: Yes. “If a covered entity discovers circumstances requiring notice pursuant to this section of more than 1,000 individuals at a single time, the covered entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.”</p>	<p>Timing: “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 an authorized delay for law enforcement purposes or an authorized waiver.” (§501.171)(4)(a))</p> <p>Delay: “If a federal, state, or local law enforcement agency determines that notice to individuals</p>	<p>Method: “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.” (§501.171)(4)(d))</p> <p>Notice contents requirement: “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</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: Yes. “Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity’s primary or functional federal regulator is deemed to be in compliance with the notice requirement in this subsection if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security. Under this paragraph, a covered entity that timely provides a copy of such notice</p>	<p>State enforcement: “(a) A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the department under s. 501.207 [of Title XXXIII of the Florida Statutes] against a covered entity or third-party agent. (b) In addition to the remedies provided for in [§501.171(9)(a)], a covered entity that fails to provide the required notice to the Department of Legal Affairs or to individuals shall be liable for a civil penalty not to exceed \$500,000, as follows: 1. In the amount of \$1,000 for each day up to the first 30 days following any violation, and thereafter, \$50,000 for each subsequent 30-day period or portion thereof for up to</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Florida								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	breach occurred. Upon receiving notice from a third-party agent, a covered entity shall provide notices required under §§501.171(3) and 501.171(4)]. A third-party agent shall provide a covered entity with all information that the covered entity needs to comply with its notice requirements. (b) An agent may provide notice as required under §§501.171(3) and 501.171(4)] on behalf of the covered entity; however, an agent's failure to provide proper notice shall be deemed a violation of this section against the covered entity." (§501.171(6))	password that is necessary to permit access to an individual's financial account; (IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online	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." (§501.171(4)(c))	(§501.171(5)) Government notice requirement: Yes. "(a) A covered entity shall provide notice to the [Florida Department of Legal Affairs] 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 [§501.171(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	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." (§501.171(4)(b))	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." (§501.171(4)(e)) Substitute notice: "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	to the department is deemed to be in compliance with the notice requirement." (§501.171(4)(g))	180 days. 2. If the violation continues for more than 180 days, in an amount not to exceed \$500,000. The civil penalties for failure to notify provided in this paragraph apply per breach and not per individual affected by the breach." (§501.171(9)) Private right of action: No. "This section does not establish a private cause of action." (§501.171(10))

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Florida								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>account.” (§501.171(1)(g)(1))</p> <p>Exception: -- “[Personal information] does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. -- [Personal information] also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.” (§501.171(1)(g)(2))</p>		<p>department must include:</p> <ol style="list-style-type: none"> 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 required notice or an explanation of the other actions taken pursuant to [§501.171(4)] of the statute. 5. The name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom 		<p>individuals. Such substitute notice shall include the following:</p> <ol style="list-style-type: none"> 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.” (§501.171(4)(f)) 		

Florida								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
				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.” (§501.171(3))				

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Georgia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Ga. Code Ann. §10-1-910 <i>et seq.</i> , §46-5-214	<p>Covered entities: “Any information broker or data collector that maintains computerized data that includes personal information.” (§10-1-912(a))</p> <p>Information broker: An “information broker” means “any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties.”</p>	<p>Personal information: “[A]n individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (A) Social security number; (B) Driver’s license number or state identification card number; (C) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords; (D) Account passwords or personal identification numbers or other</p>	<p>Breach definition: A “breach of the security of the system” is the “unauthorized acquisition of an individual’s computerized data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker or data collector.” (§10-1-911(1))</p> <p>Exception: “Good faith acquisition of personal information by an employee or agent of an information broker or data collector for the purposes of such information broker or data collector is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized</p>	<p>Residents: Notification must be given to “any resident of [Georgia] whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (§10-1-912(a))</p> <p>Credit reporting agency notice requirement: Yes. “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 [Georgia] 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</p>	<p>Timing: “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 [§10-1-912(c)], or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.” (§10-1-912(a))</p> <p>Delay: Notification “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.”</p>	<p>Method: “‘Notice’ means: (A) Written notice; (B) Telephone notice; (C) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code; or (D) Substitute notice, if the information broker or data collector demonstrates that the cost of providing notice would exceed \$50,000.00, that the affected class of individuals to be notified exceeds 100,000, or that the information broker or data collector does not have sufficient contact information to provide written or electronic notice to such individuals.” (§10-1-911(4))</p>	<p>For establishing own notification method: Yes. “[A]n information broker or data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system.” (§10-1-911(4))</p> <p>For following interagency guidelines: No.</p>	<p>Enforcement: Not specified.</p> <p>Private cause of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Georgia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>(§10-1-911(3))</p> <p>Data collector: A “data collector” means “any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity.” (§10-1-911(2))</p> <p>Exceptions: “Data collectors” and “information brokers” do not include “governmental agenc[ies] whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.” (§10-1-911(2)-(3))</p> <p>Person: “Person” means “any individual, partnership,</p>	<p>access codes; or (E) Any of the [above] items . . . when not in connection with the individual’s first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.” (§10-1-911(6))</p> <p>Exception: “[D]oes not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.” (§10-1-911(6))</p>	<p>disclosure.” (§10-1-911(1))</p> <p>Risk of harm analysis: No, except as the definition of “breach” may incorporate elements of such a test.</p>	<p>timing, distribution, and content of the notices.” (§10-1-912(d))</p> <p>Government notice requirement: No.</p>	<p>(§10-1-912(c))</p>	<p>Substitute notice: “Substitute notice shall consist of all of the following methods of contact: (i) E-mail notice, if the information broker or data collector has an e-mail address for the individuals to be notified; (ii) Conspicuous posting of the notice on the information broker’s or data collector’s website page, if the information broker or data collector maintains one; and (iii) Notification to major state-wide media.” (§10-1-911(4))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Georgia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>corporation, limited liability company, trust, estate, cooperative, association, or other entity.” (§10-1-911(5))</p> <p>Service provider requirement: Yes. “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 data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by</p>							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Georgia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>an unauthorized person.” (§10-1-912(b))</p> <p>Telecommunications companies: Notification is also required in the event of a breach of a telephone record concerning a Georgia resident under a separate statute, §46-5-214.</p>							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Guam								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
9 GCA § 48-10 <i>et seq.</i>	<p>Covered entities: “An individual or entity that owns or licenses computerized data that includes personal information.” (§48.30(a))</p> <p>Individual: An individual “means a natural person.” (§48.20(e))</p> <p>Entity: An 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</p>	<p>Personal information: “[F]irst 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 Guam, when the data elements are neither encrypted nor redacted: (1) Social Security number; (2)Driver’s license number or Guam identification card number issued in lieu of a driver’s license; 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.” (§48.20(f))</p>	<p>Breach definition: A “breach of the security of a system” is 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 Guam.” (§48.20(a))</p> <p>Exception: “Good faith acquisition of personal information by an</p>	<p>Residents: Any affected resident of Guam. (§48.30(a))</p> <p>Credit reporting agency requirement: No.</p> <p>Government notice requirement: No.</p>	<p>Timing: An individual or entity maintaining a computerized system with personal information “shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery.” (§48.30(c))</p> <p>Delay: “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</p>	<p>Method: “Notice means: (1) Written notice to the 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 Ten Thousand Dollars (\$10,000), or that the affected class of residents to be notified exceeds five thousand (5,000) persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in paragraphs 1, 2, or 3.” (§48.20(g))</p>	<p>For establishing own notification method: Yes. “An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this Chapter shall be deemed to be in compliance with the notification requirements of this Chapter if it notifies residents of Guam in accordance with its procedures in the event of a breach of security of the system.” (§48.40(a))</p> <p>For following interagency guidelines: Yes. “(1) A financial institution that complies with the notification</p>	<p>Local enforcement: “(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.” (§48.50)</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Guam								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>entity, whether for profit or not-for-profit.” (§48.20(b))</p> <p>Service Provider Requirement: Yes. “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</p>	<p>Exception: Personal information does not include “information that is lawfully obtained from publicly available information, or from Federal, State, or local government records lawfully made available to the general public.” (§48.20(f))</p>	<p>employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided, that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.” (§48.20(a))</p> <p>Risk of harm analysis: No.</p>		<p>enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.” (§48.30(d))</p>	<p>Substitute notice: “Substitute notice consists of any two (2) 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 commercial entity maintains a Website; and (C) Notice to major Guam media.” (§48.20(g))</p>	<p>requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this Chapter. (2) An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity’s primary or functional Federal regulator shall be in compliance with this Chapter.” (§48.40(b))</p>	<p>Private right of action: No.</p>

Guam								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	or other fraud to any resident of Guam.” (§48.30(a))							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Hawaii								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice permitted?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Hawaii Rev. Stat. §487N-1 <i>et seq.</i>	<p>Covered entities: “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.” (§487N-2(a))</p> <p>Service provider requirement: Yes. “Any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing</p>	<p>Personal information: “[A]n individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) Driver’s license number or Hawaii identification card number; or (3) Account number, credit or debit card number, access code, or password that would permit access to an individual’s financial account.” (§487N-1)</p> <p>Exception: Personal information “does not include publicly available information that is</p>	<p>Breach definition: A “security breach” is “an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach.” (§487N-1)</p> <p>Exception: “Good faith acquisition of personal information by an employee or agent</p>	<p>Affected persons: Notice must be given to the “affected person.” (§487N-2(a))</p> <p>Credit reporting agency and government notice requirements: Yes. “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.” (§487N-2(f))</p>	<p>Timing: “The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in [§487N-2(c)], 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.” (§487N-2(a))</p> <p>Delay: Notice “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</p>	<p>Method: “[N]otice 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</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: Yes. “The following shall be deemed in compliance with [the Hawaii statute]: (1) A financial institution that is subject to the Federal Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and Customer Notice published in the Federal Register on March 29, 2005 by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, or subject to 12 C.F.R. Part 748, and any</p>	<p>State enforcement: “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.” (§487N-3(a))</p> <p>Private right of action: Yes. “[A]ny 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</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Hawaii								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice permitted?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	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.” (§487N-2(b))	lawfully made available to the general public from federal, state, or local government records.” (§487N-1)	of the business for a legitimate purpose is not a security breach; provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.” (§487N-1) Risk of harm analysis: Yes. A breach occurs only when “illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person.” (§487N-1)		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.” (§487N-2(c)) Notice must 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.” (§487N-2(c))	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.” (§487N-2(e))	revisions, additions, or substitutions relating to said interagency guidance; and (2) Any health plan or healthcare provider that is subject to and in compliance with the standards for privacy or individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996.” (§487N-2(g))	attorneys’ fees to the prevailing party.” (§487N-3(b)) “The penalties provided in this section shall be cumulative to the remedies or penalties available under all other laws of [Hawaii].” (§487N-3(c))

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Hawaii								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice permitted?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>Substitute notice: “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.” (§487N-2(e)(4))</p> <p>Notice contents requirement: “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</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Hawaii								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice permitted?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						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.” (§487N-2(d))		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Idaho								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Id. Code Ann. §28-51-104 <i>et seq.</i>	<p>Covered entities: “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.” (§28-51-105(1))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “Idaho resident’s first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: (a) Social security number; (b) Driver’s license number or Idaho identification card number; or (c) Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial account.” (§28-51-104(5))</p>	<p>Breach definition: ““Breach of the security of the system’ means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an agency, individual or a commercial entity.” (§28-51-104(2))</p> <p>Exception: A breach does not include “[g]ood faith acquisition of personal information by an employee or agent of an agency, individual or a commercial entity for the purposes of the agency, individual or the commercial entity.” (§28-51-104(2))</p>	<p>Residents: The “affected Idaho resident.” (§28-51-105(1))</p> <p>Credit reporting agency requirement: No.</p> <p>Government notice requirement: Yes. “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.” (§28-51-105(1))</p>	<p>Timing: “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.” (§28-51-105(1))</p> <p>Delay: Notice “may be delayed if a law enforcement agency advises the agency, individual or commercial entity that the notice will impede a criminal investigation. Notice . . . must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency</p>	<p>Method: ““Notice’ means: (a) Written notice to the most recent address the agency, individual or commercial entity has in its records; (b) Telephonic notice; (c) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. section 7001; or (d) Substitute notice, if the agency, individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed twenty-five thousand dollars (\$25,000), or that the number of Idaho residents to be notified exceeds fifty thousand (50,000), or that the agency, individual or the commercial</p>	<p>For establishing own notification method: Yes. “An agency, individual or a commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of section 28-51-105, Idaho Code, is deemed to be in compliance with the notice requirements . . . if the agency, individual or the commercial entity notifies affected Idaho residents in accordance with its policies in the event of a breach of security of the system.” (§28-51-106(1))</p>	<p>State enforcement: “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</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Idaho								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	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.” (§28-51-105(2))	Exception: 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.” (§28-51-104(5))	Risk of harm analysis: Yes. Notice must only be given “[i]f the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur.” (§28-51-105(1))		advises the agency, individual or commercial entity that notification will no longer impede the investigation.” (§28-51-105(3))	entity does not have sufficient contact information to provide notice.” (§28-51-104(4)) Substitute notice: “Substitute notice consists of all of the following: (i) E-mail notice if the agency, individual or the commercial entity has e-mail addresses for the affected Idaho residents; and (ii) Conspicuous posting of the notice on the website page of the agency, individual or the commercial entity if the agency, individual or the commercial entity maintains one; and (iii) Notice to major statewide media.” (§28-51-104(4)(d))	For following interagency guidelines: Yes. “An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance . . . if the individual or the commercial entity complies with the maintained procedures when a breach of the security of the system occurs.” (§28-51-106(2))	subject to a fine of not more than twenty-five thousand dollars (\$25,000) per breach of the security of the system.” (§28-51-107) Criminal penalties for government employees: “Any governmental employee that 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.” (§28-51-105(1)) Private right of action: No.

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Illinois								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
815 Ill. Comp. Stat. 530/1 <i>et seq.</i>	<p>Covered entities: “Any data collector that owns or licenses personal information concerning an Illinois resident.” (815 ILCS 530/10(a))</p> <p>Data collector: A “[d]ata [c]ollector” may include, but is not limited to, ... “public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.” (815 ILCS 530/5)</p> <p>The requirements also expressly apply to any “[s]tate agency</p>	<p>Personal information: Either “(1) an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security: (A) Social security number. (B) Driver’s license number or State identification card number. (C) Account number or credit or debit card number, or an account number or</p>	<p>Breach definition: A “[b]reach of the security of the system data” is the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.” (815 ILCS 530/5)</p> <p>Exception: “[D]oes not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector’s business or subject to further unauthorized disclosure.” (815 ILCS 530/5)</p>	<p>Residents: Illinois residents. (815 ILCS 530/10(a))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: No.</p>	<p>Timing: “[F]ollowing discovery or notification of the breach . . . [t]he 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.” (815 ILCS 530/10(a))</p> <p>Delay: Delay is permitted “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.” (815 ILCS 530/10(b-5))</p>	<p>Method: “[N]otice” 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.” (815 ILCS 530/10(c))</p>	<p>For establishing own notification method: Yes. “[A] data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.” (815 ILCS 530/10(d))</p> <p>For following interagency guidelines: Yes. “Any covered entity or business associate that is subject to and in</p>	<p>State enforcement: -- A violation of the breach law is considered an unlawful practice under the Illinois Consumer Fraud and Deceptive Businesses Act. The Attorney General of Illinois has broad enforcement powers under that act, and may seek remedies including injunction, revocation of right to do business in Illinois, restitution, and a civil penalty up to \$50,000. -- If a court finds that the person’s actions were intended to defraud, it may impose a civil penalty of up to \$50,000 for each violation. -- If a person is to have committed a violation of the act against a person 65 years of age or older, the court may impose an additional civil</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Illinois								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>that collects personal information concerning an Illinois resident.” (815 ILCS 530/12)</p> <p>Service provider requirement: Yes. “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.” (815 ILCS 530/10(b))</p>	<p>credit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account. (D) Medical information.* (E) Health insurance information.** (F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. OR (2) user name or email address, in combination with</p>	<p>Risk of harm analysis: No, except as definition of “breach” may incorporate elements of such a test.</p>			<p>Substitute notice: “Substitute notice consists of all of the following methods of contact: (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.” (815 ILCS 530/10(c))</p> <p>The notice must</p>	<p>compliance with the privacy and security standards for the protection of electronic health information established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act shall be deemed to be in compliance with the provisions of this Act, provided that any covered entity or business associate required to provide notification of a breach to the Secretary of Health and Human Services pursuant to the Health Information Technology for Economic and Clinical Health Act also provides such notification to the Attorney General within 5 business</p>	<p>penalty of up to \$10,000 for each violation. (815 ILCS 530/20; 505/7)</p> <p>Private right of action: Yes, indirectly. The Consumer Fraud and Deceptive Businesses Act allows “any person who suffers actual damages” to bring a civil action. (815 ILCS 505/10a)</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Illinois								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.” (815 ILCS 530/5)</p> <p>*Medical information means “any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such</p>				<p>include, but need not be limited to information as follows: “(1) With respect to personal information as defined in [815 ILCS 530/5] 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 [815 ILCS 530/5] in paragraph (2) of the definition of ‘personal information,’ notice</p>	<p>days of notifying the Secretary.” (815 ILCS 530/50)</p>	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Illinois								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>information provided to a website or mobile application.” (815 ILCS 530/5)</p> <p>**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 medical information in an individual’s health insurance application and claims history, including any appeals records.” (815 ILCS 530/5)</p> <p>Exception: “[D]oes not include publicly available information that is lawfully made available to the general public from federal,</p>				<p>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.” (815 ILCS 530/10(a))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Illinois								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		State, or local government records.” (815 ILCS 530/5)						

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Indiana								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Ind. Code §24-4.9	<p>Covered entities: A “data base owner,” defined as “a person that owns or licenses computerized data that includes personal information.” (§24-4.9-2-3)</p> <p>Service provider requirement: Yes. “A person that maintains computerized data but that is not a data base owner shall notify the data base owner if the person discovers that personal information was or may have been acquired by an unauthorized person.” (§24-4.9-3-2)</p>	<p>Personal information: “(1) a Social Security number that is not encrypted or redacted; or (2) an individual’s first and last names, or first initial and last name, and one or more of the following data elements that are not encrypted or redacted: (A) A driver’s license number; (B) A state identification card number; (C) A credit card number; or (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person’s account.” (§24-4.9-2-10)</p>	<p>Breach definition: ““Breach of the security of data’ means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person.” (§24-4.9-2-2(a))</p> <p>“Breach includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.” (§24-2.9-2-2(a))</p> <p>Exception: Breach does not include the “[g]ood faith acquisition of personal information by an</p>	<p>Residents: Any “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.” (§24-4.9-3-1(a))</p> <p>Credit reporting agency notice requirement: Yes. “A data base owner required to make a disclosure under [§24-4.9-3-1(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</p>	<p>Timing: “A person required to make a disclosure or notification under this chapter shall make the disclosure or notification as soon as possible after: (1) delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach; or (2) the attorney general or a law enforcement agency notifies the person that delay will no longer impede a criminal or civil investigation or jeopardize national security.” (§24-4.9-3-3(b))</p> <p>“A person required to make a disclosure or notification under this chapter shall make the disclosure or notification without unreasonable delay. For purposes of this section, a delay is reasonable if the delay is: (1) necessary to</p>	<p>Method: “Except as provided in [§24-4.9-3-4(b) (“substitute notice”)], a data base owner required to make a disclosure under this chapter shall make the disclosure using one (1) of the following methods: (1) Mail. (2) Telephone. (3) Facsimile (fax). (4) Electronic mail, if the data base owner has the electronic mail address of the affected Indiana resident.” (§24-4.9-3-4(a))</p> <p>Substitute notice: “If a data base owner required to make a disclosure under this chapter is required to make the disclosure to more than five hundred thousand (500,000) Indiana residents, or if the data base owner required to make a disclosure under this chapter</p>	<p>For establishing own notification method: Yes, as long as the privacy policy is at least as stringent as the disclosure required by the Indiana statute or the federal statutes listed below. (§24-4.9-3-4(c))</p> <p>For following interagency guidelines: Yes. -- “A data base owner that maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under (1) The federal USA Patriot Act (P.L. 107-56); (2) Executive Order 13224; (3) The federal Driver’s Privacy Protection Act (18 U.S.C. 2781 <i>et seq.</i>); (4) The federal Fair Credit</p>	<p>State enforcement: “(a) A person that is required to make a disclosure or notification in accordance with IC 24-4.9-3 and that fails to comply with any provision of this article commits a deceptive act that is actionable only by the attorney general under this chapter. (b) A failure to make a required disclosure or notification in connection with a related series of breaches of the security of a system constitutes one (1) deceptive act.” (§24-4.9-4-1)</p> <p>Penalties: “The attorney general may bring an action under this chapter to obtain any or all of the following: (1) An injunction to enjoin future violations of this section. (2) A civil penalty</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Indiana								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>Exception: 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.” (§24-4.9-2-10)</p>	<p>employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure.” (§24-4.9-2-2(b)(1))</p> <p>Exception: Breach does not include the “[u]nauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key: (A) has not been compromised or disclosed; and (B) is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device.”</p>	<p>of an Indiana resident affected by the breach of the security of a system.” (§24-4.9-3-1(b))</p> <p>Government notice requirement: Yes. “If a data base owner makes a disclosure described in [§24-4.9-3-1(a)], the data base owner shall also disclose the breach to the attorney general.” (§24-4.9-3-1(c))</p>	<p>restore the integrity of the computer system; (2) necessary to discover the scope of the breach; or (3) in response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will: (A) impede a criminal or civil investigation; or (B) jeopardize national security.” (§24-4.9-3-3(a))</p>	<p>determines that the cost of the disclosure will be more than two hundred fifty thousand dollars (\$250,000), the data base owner required to make a disclosure under this chapter may elect to make the disclosure by using both of the following methods: (1) Conspicuous posting of the notice on the web site of the data base owner, if the data base owner maintains a web site. (2) Notice to major news reporting media in the geographic area where Indiana residents affected by the breach of the security of a system reside.” (§24-4.9-3-4(b))</p>	<p>Reporting Act (15 U.S.C. 1681 <i>et seq.</i>); (5) The federal Financial Modernization Act of 1999 (15 U.S.C. 6801 <i>et seq.</i>); or (6) The federal Health Insurance Portability and Accountability Act (HIPAA) (P.L.104-191); is not required to make a disclosure under this chapter if the data base owner’s information privacy, security policy, or compliance plan requires that Indiana residents be notified of a breach of the security of data without unreasonable delay and the data base owner complies with the data base owner’s information privacy, security policy, or compliance plan.” (§24-4.9-3-4(d)) -- “A financial institution that</p>	<p>of not more than one hundred fifty thousand dollars (\$150,000) per deceptive act. (3) The attorney general’s reasonable costs in: (A) the investigation of the deceptive act; and (B) maintaining the action.” (§24-4.9-4-2)</p> <p>Private right of action: No. Violations are “actionable only by the attorney general.” (§24-4.9-4-1)</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Indiana								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			(§24-4.9-2-2(b)(2)) Risk of harm analysis: Yes. Notice is required only “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.” (§24-4.9-3-1(a))				complies with the disclosure requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, as applicable, is not required to make a disclosure under this chapter.” (§24-4.9-3-4(e))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Iowa								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Iowa Code §715C.1 <i>et seq.</i>	<p>Covered entities: “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.” (§715C.2(1))</p> <p>Person: A “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.”</p>	<p>Personal information: Personal information means “an individual’s first name or first initial and last name in combination with any one or more of the following data elements 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: (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</p>	<p>Breach definition: “‘Breach of security’ means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information.” (§715C.1(1))</p> <p>Exception: “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,</p>	<p>Affected consumers: To “any consumer whose personal information was included in the information that was breached.” (§715C.2(1))</p> <p>Consumers: A “consumer” means any Iowa resident. (§715C.1(2))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: No.</p>	<p>Timing: “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 [§715C.2(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.” (§715C.2(1))</p> <p>Delay: “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</p>	<p>Method: “[N]otification 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</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: Yes. The law 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</p>	<p>State enforcement: The law deems a violation to be an unfair trade practice, and authorizes the state’s attorney general to both impose “a civil penalty not to exceed forty thousand dollars per violation” and seek additional damages “on behalf of a person injured” by a violation. (§§715C.2(8)(a), 714.16(7))</p> <p>“The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under the law.” (§715C.2(8)(b))</p> <p>Private right of action: No, although the attorney general may seek damages on behalf of person injured by a violation.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Iowa								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	(§715C.1(10)) Service provider requirement: Yes. “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.” (§715C.2(2))	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) Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.” (§715C.1(11))	confidentiality, or integrity of the personal information.” (§715C.1(1)) Risk of harm analysis: Yes. “[N]otification 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.” (§715C.2(6))		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.” (§715C.2(3))	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.” (§715C.2(4)) Substitute 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 web site of the person if the person maintains an internet web site. (3) Notification to major statewide media.” (§715C.2(4)(c)) Notice contents requirement: Notice “shall include, at a	protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this section.” OR (c) “A person who is subject to and complies with regulations promulgated pursuant to Title V of the Gramm Leach Bliley Act.” (§§715C.2(7))	(§715C.2(8)(a))

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Iowa								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		Exception: “[D]oes 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.” (§715C.1(11))				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.” (§715C.2(5))		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Kansas								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Kansas Stat. §50-7a01 <i>et seq.</i>	<p>Covered entities: “A person that conducts business in [Kansas], or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information.” (§50-7a02(a))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “[A] consumer’s first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted or redacted: (1) Social security number; (2) driver’s license number or state identification card number; or (3) financial account number or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer’s financial account.” (§50-7a01(g))</p>	<p>Breach definition: A security breach means “the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer.” (§50-7a01(h))</p> <p>Exception: “Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the</p>	<p>Residents: Affected Kansas residents. (§50-7a02(a))</p> <p>Credit reporting agency notice requirement: Yes. If notice must be given to “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 . . . of the timing, distribution and content of the notices.” (§50-7a02(f))</p> <p>Government notice requirement: No.</p>	<p>Timing: After an investigation, “[n]otice 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.” (§50-7a02(a))</p> <p>Delay: Notice “may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation.” (§50-7a02(c))</p>	<p>Method: “‘Notice’ means: (1) Written notice; (2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or (3) substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed \$100,000, or that the affected class of consumers to be notified exceeds 5,000, or that the individual or the commercial entity does not have sufficient contact information to provide notice.” (§50-7a01(c))</p> <p>Substitute notice: “‘Substitute’ notice means: (1) E-mail notice if</p>	<p>For establishing own notification method: Yes. “[A]n 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.” (§50-7a02(d))</p> <p>For following interagency guidelines: Yes. “An individual or a commercial entity</p>	<p>State enforcement: -- “For violations of this section, except as to insurance companies licensed to do business in [Kansas], 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.” (§50-7a02(g))</p> <p>-- “For violations of the law by an insurance company licensed to do business in [Kansas], the insurance commissioner shall have the sole authority to enforce the provisions of this section.”</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Kansas								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.” (§50-7a02(b))	Exception: Personal information “does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.” (§50-7a01(g))	system, provided that the personal information is not used for or is not subject to further unauthorized disclosure.” (§50-7a01(h)) Risk of harm analysis: Yes. Notice need only be given if an entity conducts an investigation that “determines that the misuse of information has occurred or is reasonably likely to occur.” (§§50-7a02(a), 50-7a01(h))			the entity has e-mail addresses for the affected class of consumers; (2) Conspicuous posting of the notice on the entity’s web site if the entity maintains a web site; and (3) Notification to major statewide media.” (§50-7a01(e))	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.” (§50-7a02(e))	(50-7a02(h)) Private right of action: No.

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Kentucky								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
KRS §365.732	<p>Covered entities: Any “information holder,” defined as “any person or business entity that conducts business in [Kentucky].” (§365.732(1)(b))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “‘Personally identifiable information’ means an individual’s first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted:</p> <ol style="list-style-type: none"> 1. Social Security number; 2. Driver’s license number; or 3. Account number, credit or debit card number, in combination with any required security code, access code, or password permit access to an individual’s financial account.” (§365.732(1)(c)) 	<p>Breach definition: “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.” (§365.732(1)(a))</p> <p>Exception: “Good faith acquisition of personally</p>	<p>Residents: “[A]ny resident of Kentucky whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (§365.732(2))</p> <p>Credit agency reporting requirement: Yes. “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.” (§365.732(7))</p>	<p>Timing: Notification shall be made “in in the most expedient time possible and without unreasonable delay.” (§365.732(2))</p> <p>Delay: Delay is permitted 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.” (§365.732(4))</p>	<p>Method: “[N]otice may be provided by one (1) of the following methods:</p> <ol style="list-style-type: none"> (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.” (§365.732(5)) 	<p>For establishing own notification method: Yes. “[A]n 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.” (§365.732(6))</p> <p>For following interagency guidelines: Yes. Does not apply to “any person who is subject to the provisions of Title</p>	<p>Penalties: Not specified.</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Kentucky								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	been, acquired by an unauthorized person.” (§365.732(3))		<p>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.” (§365.732(1)(a))</p> <p>Risk of harm analysis: Yes. Security breach must “actually [cause], or [lead] the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky” in order to trigger the notice requirement. (§365.732(1)(a))</p>	Government notice requirement: No.		<p>Substitute notice: “Substitute notice shall consist of all of the following:</p> <ol style="list-style-type: none"> 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.” (§365.732(5)(c)) 	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.” (§365.732(8))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Louisiana								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
La. Rev. Stat. Ann. §51:3071 <i>et seq.</i> ; La. Admin. Code tit. 16, pt. III, §701.	<p>Covered entities: “Any person that conducts business in [Louisiana] or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information.” (R.S. 51:3074(A))</p> <p>Person: A “person” is defined as “any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity.” (R.S. 51:3073(3))</p> <p>Service provider requirement: Yes. “Any agency or person that maintains computerized data that includes</p>	<p>Personal information: “[A]n individual’s first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted: (i) Social security number; (ii) Driver’s license number; (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.” (R.S. 51:3073(4))</p> <p>Exception: Does not “include publicly available information that is lawfully made available to the</p>	<p>Breach definition: A “breach of the security of the system” is the “the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by an agency or person.” (R.S. 51:3073(2))</p> <p>Exception: “Good faith acquisition of personal information by an employee or agent of an agency or person for the purposes of the agency or person is not a breach of the security of the system, provided that the personal information is not used for, or is subject to, unauthorized</p>	<p>Residents: “[A]ny resident of [Louisiana] whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (R.S. 51:3074(A))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: Yes. -- “When notice to Louisiana citizens is required pursuant to R.S. 51:3074, the person or agency shall provide written notice detailing the breach of the security of the system to the Consumer Protection Section of the Attorney General’s Office. Notice shall include the names of all Louisiana citizens affected by the breach.” (La. Admin. Code §16:III.701(A)) -- “Written notification [to the Attorney General’s</p>	<p>Timing: Notice to residents “shall be made in the most expedient time possible and without unreasonable delay.” (R.S. 51:3074(C))</p> <p>Delay: Notice requirement must be “consistent with the legitimate needs of law enforcement, as provided in [R.S. 51:3074(D)] or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.” (R.S. 51:3074(C))</p>	<p>Method: “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.” (R.S. 51:3074(E))</p>	<p>For establishing own notification method: Yes. “[A]n 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.” (R.S. 51:3074(F))</p> <p>For following interagency guidelines: Yes. “A financial institution that is</p>	<p>State enforcement: “Failure to provide timely notice may be punishable by a fine not to exceed \$5,000 per violation. Notice to the attorney general shall be timely if received within 10 days of distribution of notice to Louisiana citizens. Each day notice is not received by the attorney general shall be deemed a separate violation.” (La. Admin. Code §16:III.701(B))</p> <p>Private right of action: Yes. “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.” (R.S. 51:3075)</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Louisiana								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	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.” (R.S. 51:3074(B))	general public from federal, state, or local government records.” (R.S. 51:3073(4))	disclosure.” (R.S. 51:3073(2)) Risk of harm analysis: Yes. “Notification under this title is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers.” (R.S. 51:3074(G))	Office] shall be mailed to: Louisiana Department of Justice Office of the Attorney General Consumer Protection Section 1885 N. Third Street Baton Rouge, LA 70802.” (La. Admin. Code §16:III.701(C))		Substitute notice: “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.” (R.S. 51:3074 (E)(3))	subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the office of the comptroller of the currency and the office of thrift supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance with this Chapter.” (R.S. 51:3076)	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Maine								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Maine Rev. Stat. Ann. tit. 10, §1346 <i>et seq.</i>	<p>Covered entities: “[A]n information broker that maintains computerized data that includes personal information.” (§1348(1)(A))</p> <p>Information broker: Information broker means “a person* who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated 3rd parties.” (§1347(3))</p>	<p>Personal information: “[A]n individual’s first name, or first initial, and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (A) Social security number. (B) Driver’s license number or state identification card number. (C) Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords. (D) Account passwords or personal identification numbers or other</p>	<p>Breach definition: A “breach of the security of the system” or “security breach” means “unauthorized acquisition of an individual’s computerized data that includes personal information that compromises the security, confidentiality or integrity of personal information of the individual maintained by a person.” (§1347(1))</p> <p>Exception: “Good faith acquisition, release or use of personal information by an employee or agent of a person on behalf of the person is not a breach of the security of the system if the personal information is not used for or subject to further unauthorized</p>	<p>Residents: The information broker must notify any “resident of [Maine] whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person.” (§1348(1)(A))</p> <p>Credit reporting agency notice requirement: Yes. “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</p>	<p>Timing: Notice “must be made as expediently as possible and without unreasonable delay” after either a person conducts an investigation to determine whether “the personal information has been or will be misused.” (§1348(1))</p> <p>Delay: Notice requirement must be “consistent with the legitimate needs of law enforcement pursuant to [§1348(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.” (§1348(1))</p>	<p>Method: “‘Notice’ means: A. Written notice; B. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 United States Code, Section 7001; or C. Substitute notice, if the person maintaining personal information demonstrates that the cost of providing notice would exceed \$5,000, that the affected class of individuals to be notified exceeds 1,000 or that the person maintaining personal information does not have sufficient contact information to provide written or electronic notice to those individuals.” (§1347(4))</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: Yes. “A person that complies with the security breach notification requirements of rules, regulations, procedures or guidelines established pursuant to federal law or the law of [Maine] is deemed to be in compliance with the requirements of §1348 as long as the law, rules, regulations or guidelines provide for notification procedures at least as protective as the notification requirements of [this chapter].” (§1349(4))</p>	<p>State enforcement: “The appropriate state regulators within the Department of Professional and Financial Regulation shall enforce this chapter for any person that is licensed or regulated by those regulators. The Attorney General shall enforce this chapter for all other persons.” (§1349(1))</p> <p>Penalties: “A person that violates the chapter is subject to a civil violation and is subject to one or more of the following: (A) A fine of not more than \$500 per violation up to \$2,500; (B) Equitable relief; or (C) Enjoinment from further violations of the chapter.” (§1349(2))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Maine								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>* Person means “an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity, including agencies of State Government, the University of Maine System, the Maine Community College System, Maine Maritime Academy and private colleges and universities.” (§1347(5))</p> <p>Exception: Information broker “does not include a governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes.” (§1347(3))</p>	<p>access codes; or (E) Any of the data elements contained in paragraphs A to D when not in connection with the individual’s first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.” (§1347(6))</p> <p>Exception: Personal information “does not include information from 3rd-party claims databases maintained by property and casualty insurers or publicly available information that is</p>	<p>disclosure to another person.” (§1347(1))</p> <p>Risk of harm analysis: Yes. -- For information brokers, notice must be given if “personal information has been, or is reasonably believed to have been, acquired by an unauthorized person.” (§1348(1)(A)) -- For any person other than an information broker, notice must be given only if “if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur.” (§1348(1)(B))</p>	<p>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.” (§1348(4))</p> <p>Government notice requirement: Yes. “When notice of a breach of the security of the system is required under [§1348(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.” (§1348(5))</p>		<p>Substitute notice: “Substitute notice must consist of all of the following: (1) An e-mail notice, if the person has the e-mail addresses of the individuals to be notified; (2) A conspicuous posting of the notice on the person’s publicly accessible website, if the person maintains one; and (3) Notification to major statewide media.” (§1347(4))</p>		<p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Maine								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	Service provider requirement: Yes. Notice is required from “any other person who maintains computerized data that includes personal information.” (§1348(1)(B))	lawfully made available to the general public from federal, state, or local government records or widely distributed media.” (§1347(6))						

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Maryland								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Maryland Code Ann., Com. Law. §14-3501 <i>et seq.</i> ; H.B. 974 (effective January 1, 2018)	<p>Covered entities: “[A] business* that owns or licenses computerized data that includes personal information of an individual residing in the State....” (§14-3504(b)(1))</p> <p>*“‘Business’ means a sole proprietorship, partnership, corporation, association, or any other business entity, whether or not organized to operate at a profit [and] includes a financial institution organized, chartered, licensed, or otherwise authorized under the laws of [Maryland], any other state, the United States, or any other country, and the parent or subsidiary of a financial</p>	<p>Personal information: Personal Information means “(i) [a]n 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</p>	<p>Breach definition: A “‘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.” (§14-3504(a)(1))</p> <p>Exception: Breach “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.” (§14-3504(a)(2))</p> <p>Risk of harm analysis: Yes. -- “A business that owns or licenses</p>	<p>Residents: “[A]n individual residing in [Maryland].” (§14-3504(b)(1))</p> <p>Credit reporting agency notice requirement: Yes. “If a business is required under § 14–3504 of this subtitle to give notice of a breach of the security of a system to 1,000 or more individuals, the business also shall notify, without unreasonable delay, each consumer reporting agency that compiles and maintains 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 . . . This section does not require the inclusion of the names or other personal identifying information of recipients of notices of the breach of the security of a system.”</p>	<p>Timing: Notice “shall be given as soon as reasonably practicable, but not later than 45 days after the business concludes the investigation required under [§14-3504(b)(1)].” (§14-3504(b)(3))</p> <p>Delay: “(1) The [required] notification . . . may be delayed: (i) If a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or (ii) To determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system. (2) If notification is delayed [it] shall be given as soon as reasonably</p>	<p>Method: “The [required] notification . . . 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 recipient has expressly consented to receive electronic notices; 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 . . . if:</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: Yes. -- “(1) A business that complies with the requirements for notification procedures, the protection or security of personal information, or the destruction of personal information under the rules, regulations, procedures, or guidelines established by the primary or functional federal or State regulator of the business shall be deemed to be in compliance . . . (2) A business that is subject to and in compliance with Gramm-Leach-Bliley, the Fair and Accurate Transactions Act, the Interagency Guidelines</p>	<p>State enforcement: A violation is considered an “unfair or deceptive trade practice” and is enforced pursuant to Maryland’s Consumer Protection Act (§13-101 <i>et seq.</i>), which authorizes actions by the Attorney General. (§14-3508)</p> <p>Private right of action: Yes. Maryland’s Consumer Protection Act (§13-101 <i>et seq.</i>) states that “any person may bring an action to recover for injury or loss sustained by him as the result of a [prohibited] practice.” (See §14-3508)</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Maryland								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>institution.” (§14-3501(b))</p> <p>Service provider requirement: Yes. “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.” (§14-3504(c)(1))</p>	<p>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</p>	<p>computerized data that includes personal information of an individual residing in [Maryland], 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 . . . 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.” (§§14-3504(b)(1), (2))</p>	<p>(§14-3506)</p> <p>Government notice requirement: Yes. “Prior to giving the notification required under [§14-3504(b)] and subject to [delay pursuant to §14-3504(d)], a business shall provide notice of a breach of the security of a system to the Office of the Attorney General.” (§14-3504(h))</p>	<p>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.” (§14-3504(d))</p>	<p>(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.” (§14-3504(e))</p> <p>Substitute notice: “Substitute notice . . . shall consist of all of the following methods of contact: (1) Electronically mailing the notice if the business has an electronic mail address for the individual to be notified; (2) Conspicuous posting of the notice on the website of the business; AND (3) Notification to major statewide media.” (§14-3504(f))</p>	<p>Establishing Information Security Standards, and the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed to be in compliance.” (§14-3507(c)) -- “A business [or affiliate] that is subject to and in compliance with the federal Health Insurance Portability and Accountability Act of 1996 shall be deemed to be in compliance with this subtitle.” (§14-3507(d))</p>	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Maryland								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>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</p> <p>(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.” (§14-3501(e)(1))</p> <p>Exception: ““Personal information’ does not include: (i) Publicly</p>	<p>-- “If after the investigation . . . the business determines that notification . . . is not required, the business shall maintain records that reflect its determination for 3 years after the determination is made.” (§14-3504(b)(4))</p>			<p>Notification contents requirement: “[T]he notification required under [§14-3504(b)] 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</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Maryland								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		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.” (§14-3501(e)(2))				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.” (§14-3504(g)) Breaches That Permit Access to Email Accounts: “(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–		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Maryland								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						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 [§14-3504(b)] 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		

Maryland								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						answer.” (§14-3504(i))		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Massachusetts								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
Massachusetts Gen Laws ch. 93H, §1, <i>et seq.</i>	<p>Covered entities: “A person* or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice . . . 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....” (§3(b))</p> <p>* Person: “Person” means a natural person, corporation, association, partnership or</p>	<p>Personal information: Personal information means “a resident’s first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) A Social Security number; (b) A driver’s license number or state-issued identification card number; (c) A financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident’s financial account.” (§1(a))</p>	<p>Breach definition: -- “Breach of security” [means] the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted* electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency, or employee or agent thereof, that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.” (§1(a))</p> <p>-- However, even if there has not been a “breach of security” as defined by the statute (with its “substantial risk of identity theft or fraud” threshold), notification is still required if a person that owns or</p>	<p>Notice must be given to:</p> <ul style="list-style-type: none"> -- The attorney general; -- the director of consumer affairs and business regulation and; -- the affected Massachusetts resident. <p>(§3(b))</p> <p>Credit reporting agency and government notice requirement: Yes. “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</p>	<p>Timing: Notice shall be given “as soon as practicable and without unreasonable delay.” (§3(b))</p> <p>Delay: Delay is permitted “if a law enforcement agency determines that provision of such notice may impede a criminal investigation and has notified the attorney general, in writing, thereof and informs the person or agency of such determination. If notice is delayed due to such determination and as soon as the law enforcement agency determines and informs the person or agency that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable and without unreasonable delay. The person or agency shall cooperate with</p>	<p>Method: “Notice” shall include:-</p> <ul style="list-style-type: none"> (i) written notice; (ii) electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 (c) of Title 15 of the United States Code; and chapter 110G; or (iii) substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed \$250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice.” (§1(a)) 	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: Yes. “[A] person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; provided further that the person also notifies the attorney general and the director of the office of consumer affairs and business regulation of the breach as soon as</p>	<p>State enforcement: “The attorney general may bring an action pursuant to section 4 of chapter 93A [the Massachusetts Consumer Protection Act] against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.” (§6)</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Massachusetts								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
	<p>other legal entity.” (§1(a))</p> <p>Service provider requirement: Yes. “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</p>	<p>Exception: Personal information does not include information that “is lawfully obtained from publicly available information or from federal, state or local government records lawfully made available to the general public.” (§1(a))</p>	<p>licenses data that includes personal information about a resident of the commonwealth “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.” (§3(b))</p> <p>* Encrypted: Encrypted [means] “transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation.” (§1(a))</p>	<p>to the incident. Upon receipt of [the] 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.” (§3(b))</p>	<p>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.” (§4)</p>	<p>Substitute notice: “‘Substitute notice’ shall consist of all of the following: (i) electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents; (ii) clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and (iii) publication in or broadcast through media or medium that provides notice throughout the commonwealth.” (§1(a))</p> <p>Notice contents requirement: “The notice to be provided to the resident shall include, but not be limited to, the consumer’s right to</p>	<p>practicable and without unreasonable delay following the breach. The notice to be provided to the attorney general and the director of the office of consumer affairs and business regulation shall consist of, but not be limited to, any steps the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines; provided further that if said person or agency does not comply with applicable federal laws, rules, regulations, guidance or guidelines, then it shall be subject to the provisions of this chapter.” (§5)</p>	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Massachusetts								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
	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		<p>Exception: “A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.” (§1(a))</p> <p>Risk of harm analysis: No. While a “breach of security” occurs only when there is a “substantial risk of identity theft or fraud,” notice must be given whenever a person that owns or licenses personal information about state residents “knows or has reason to know that the personal information...was</p>			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.” (§3(b))		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Massachusetts								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
	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.” (§3(a))		acquired or used by an unauthorized person or used for an unauthorized purpose.” (§3(b))					

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Michigan								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Michigan Comp. Laws § 445.63, <i>et seq.</i>	<p>Covered entities: “[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.” (§12(1))</p> <p>Person: “‘Person’ means an individual, partnership, corporation, limited liability company, association, or other legal entity.” (§3(p))</p> <p>Service provider requirement: Yes. “[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 that shall provide a notice to the</p>	<p>Personal information: “[T]he first name or first initial and last name linked to 1 or more of the following data elements of a resident of [Michigan]: (i) Social security number. (ii) Driver license number or state personal identification card number. (iii) Demand deposit or other 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 any of the resident’s accounts.” (§3(r))</p>	<p>Breach definition: A “‘breach of the security of a database’ or ‘security breach’ means the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency.” (§3(b))</p> <p>Exception: “These terms do not include unauthorized access to data by an employee or other individual if the access meets all of the following: (i) The employee or other individual acted in good faith in accessing the data; (ii) The access was related to the agency or person; (iii) The employee or other individual did not misuse any</p>	<p>Residents: Notice must be given “to each resident of [Michigan] 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.” (§12(1))</p> <p>Credit reporting agency notice requirement: Yes. -- “[A]fter 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.” -- Requirement does</p>	<p>Timing: “A person or agency shall provide any notice required under this section without unreasonable delay.” (§12(4))</p> <p>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.</p>	<p>Method: “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</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: Yes. -- “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</p>	<p>State enforcement: -- “Subject to [§12(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.” (§12(13))</p> <p>-- “The aggregate liability of a person for civil fines under [§12(13)] for multiple violations of [§12(13)] that arise from the same security breach shall not exceed \$750,000.00.” (§12(14))</p> <p>Criminal penalties for false reporting: “A person that provides notice of a security breach in</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Michigan								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	owner or licensor of the information of the security breach.” (§12(2))		personal information or disclosure any personal information to an unauthorized person.” (§3(b)) Risk of harm analysis: Yes. Notice is not required if “the person or agency determines that the security breach has not or is not likely to create substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of [Michigan].” (§12(1))	not apply if notice is required to 1,000 or fewer residents in [Michigan], or the person or agency is subject to title V of the Gramm-Leach Bliley Act, 15 U.S.C. §6801 et seq.” (§12(8)) Government notice requirement: No.	(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.” (§12(4))	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	administration, and its affiliates, is considered to be in compliance with this section.” (§12(9)) -- “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.” (§12(10))	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) [B]y 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; and (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.” (§12(12)) Private right of action: No.

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Michigan								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>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.</p> <p>(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.”</p> <p>(§12(5))</p> <p>Substitute notice: “Substitute notice must provide a telephone number or web address that an individual can</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Michigan								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>use to obtain additional assistance and information, and must consist of all of the following: (i) E-mail notice where the person has an email address for the affected customer(s); (ii) Conspicuous posting of the notice on the appropriate website maintained by the person; AND (iii) Notification to major statewide media.” (§12(5))</p> <p>* Limited exception for public utilities: “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 [(§12(5))], or alternatively by providing all of the following: (a) As applicable,</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Michigan								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						notice as described in [(§12(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(11))		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Minnesota								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
Minn. Stat. §325E.61	<p>Covered entities: “Any person or business that conducts business in [Minnesota], and that owns or licenses data that includes personal information.” (Subdiv. 1(a))</p> <p>Exception: The law “does not apply to any ‘financial institution’ as defined by United States Code, title 15, section 6809(3).” (Subdiv. 4)</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “[A]n 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; (3) account number or credit or debit card number, in combination with</p>	<p>Breach definition: A “breach of the security of the system” is the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or the business.” (Subdiv. 1(d))</p> <p>Exception: “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.” (Subdiv. 1(d))</p>	<p>Residents: “[A]ny resident of [Minnesota] whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (Subdiv. 1(a))</p> <p>Credit reporting agency notice requirement: Yes. “If a person discovers circumstances requiring notification under this section 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 [15 USC 1681a], of the timing, distribution, and content of the notices.” (Subdiv. 2)</p>	<p>Timing: “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 [Subdiv. 1(c)], or with any reasonable measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.” (Subdiv. 1(a))</p> <p>Delay: Delay is permitted if “a law enforcement agency affirmatively determines that the notification will impede a criminal investigation.” (Subdiv. 1(c))</p>	<p>Method: “[N]otice” 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</p>	<p>For establishing own notification method: Yes. If a person or business “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” under the law, then the person or business “shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.” (Subdiv. 1(h))</p> <p>For following interagency guidelines: No, but the statute does not apply to “any ‘financial</p>	<p>State enforcement: The Attorney General is given enforcement power to seek civil penalties not to exceed \$25,000 and injunctive relief under Minn. Stat. §8.31 (establishing the Attorney General’s authority to investigate and prosecute certain illegal acts). (Subdiv. 6)</p> <p>Private right of action: Yes. “In addition to the remedies otherwise provided by law, any person injured by a violation [of the state consumer protection law] may bring a civil action and recover damages, together with costs and disbursements, including costs of investigation and reasonable attorney’s fees, and receive other equitable relief as</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Minnesota								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
	immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (Subdiv. 1(b))	any required security code, access code, or password that would permit access to an individual’s financial account.” (Subdiv. 1(e)) Exception: Personal information “does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.” (Subdiv. 1(f))	Risk of harm analysis: No, except as definition of “breach” may incorporate elements of such a test.	Government notice requirement: No		be notified exceeds 500,000, or the person or business does not have sufficient contact information.” (Subdiv. 1(g)(3)) Substitute notice: “Substitute notice must consist of all of the following: (i) E-mail notice where the person has an email address for the affected customer(s); (ii) Conspicuous posting of the notice on the appropriate website maintained by the person; AND (iii) Notification to major statewide media.” (Subdiv. 1(g)(3))	institution” as defined by United States Code, title 15, section 6809(3).” (Subdiv. 4)	determined by the court.” (Subdiv. 6)

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Mississippi								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Miss. Code §75-24-29	<p>Covered entities: “[A]ny person who conducts business in [Mississippi] and who, in the ordinary course of the person’s business functions, owns, licenses or maintains personal information of any resident of [Mississippi].” (§75-24-29(1))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “‘Personal information’ means an individual’s first name or first initial and last name in combination with any one or more of the following data elements: (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.” (§75-24-29(2)(b))</p> <p>Exception: “[P]ersonal information’ does not include</p>	<p>Breach definition: “‘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.” (§75-24-29(2)(a))</p> <p>Risk of harm analysis: Yes. “Notification shall not be required [of a person who conducts business in Mississippi] if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected</p>	<p>Residents: “[A]ny individual who is a resident of [Mississippi] whose personal information was, or is reasonably believed to have been, intentionally acquired by an unauthorized person through a breach of security.” (§75-24-29(2)(b)(iv))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: No.</p>	<p>Timing: “[D]isclosure shall be made without unreasonable delay.” (§75-24-29(3))</p> <p>Delay: Delay is permitted “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.” (§75-24-29(5))</p>	<p>Method: “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</p>	<p>For establishing own notification method: Yes. “Any person who conducts business in [Mississippi] 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.” (§75-24-29(7))</p> <p>For following interagency guidelines: Yes. “Any person that maintains such a security breach</p>	<p>State enforcement: “Failure to comply with the requirements of this section shall constitute an unfair trade practice and shall be enforced by the Attorney General.” (§75-24-29(8))</p> <p>Private right of action: No. “[N]othing in this section may be construed to create a private right of action.” (§75-24-29(8))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Mississippi								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes.” (§75-24-29(4))	publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.” (§75-24-29(2)(b))	individuals.” (§75-24-29(3))			subject persons to be notified exceeds five thousand (5,000) individuals or the person does not have sufficient contact information.” (§75-24-29(6)) Substitute notice: “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.” (§75-24-29(6))	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.” (§75-24-29(8))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Missouri								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
Mo. Rev. Stat. § 407.1500	<p>Covered entities: “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.” (§407.1500.2(1))</p> <p>* “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.” (§407.1500.1(7))</p> <p>** “Person” means “any</p>	<p>Personal information: Personal information means “an individual’s first name or first initial and last name in combination with any one or more of the following data elements 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</p>	<p>Breach definition: “‘Breach of security’ or ‘breach’ [means] 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.” (§407.1500.1(1))</p> <p>Exception: “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</p>	<p>Consumers: Notification must be given to the “affected consumer.”* (§407.1500.2(1))</p> <p>* Consumer means “an individual who is a resident of [Missouri].” (§407.1500.1(2))</p> <p>Credit reporting agency and government notice requirement: Yes. “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</p>	<p>Timing: “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.” (§407.1500.2(1))</p> <p>Delay: Delay is permitted 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</p>	<p>Method: “[N]otice 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</p>	<p>For establishing own notification method: Yes. “A person that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the person notifies affected consumers in accordance with its policies in the event of a breach of security of the system.” (§407.1500.3(1))</p> <p>For following interagency guidelines: Yes. -- “A person that is regulated by state or federal law and that maintains procedures for a</p>	<p>State enforcement: “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.” (§407.1500.3(4))</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Missouri								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
	<p>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.” (§407.1500.1(8))</p> <p>Service provider requirement: Yes. Notice required of “[a]ny 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</p>	<p>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.” (§407.1500.1(9))</p> <p>Encryption: Encryption means “the use of an algorithmic process to transform data into a form in which</p>	<p>threat to the security, confidentiality, or integrity of the personal information.” (§407.1500.1(1))</p> <p>Risk of harm analysis: Yes. “[N]otification 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.” (§407.1500.2(5))</p>	<p>notice.” (§407.1500.2(8))</p>	<p>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.” (§407.1500.2(3))</p>	<p>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.” (§407.1500.2(6))</p> <p>Substitute notice: “Substitute notice . . . shall consist of all the following: (a) Email notice when the person has an electronic mail</p>	<p>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.” -- Notice is also not required of 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</p>	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Missouri								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
	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.” (§407.1500.2(2))	the data is rendered unreadable or unusable without the use of a confidential process or key.” (§407.1500.1(4)) Health insurance information: 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.” (§407.1500.1(5)) Medical information: Medical information means “any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care				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.” (§407.1500.2(7)) Notice contents requirement: “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	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.” (§§407.1500.3(2), (3))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Missouri								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
		<p>professional.” (§407.1500.1(6))</p> <p>Exception: “[D]oes 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.” (§407.1500.1(9))</p>				<p>information for consumer reporting agencies; (e) Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.” (§407.1500.2(4))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Montana								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Mont. Code Ann. §30-14-1701 <i>et seq.</i> , § 33-19-231	<p>Covered entities: “Any person, or business that conducts business in Montana and that owns or licenses computerized data that includes personal information.” (§30-14-1704(1))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “[A]n individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) social security number; (B) driver’s license number or state identification card number; (C) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.” (§30-14-1704(4) (b)(i))</p> <p>Exception: Personal information “does</p>	<p>Breach definition: “[B]reach 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.” (§30-14-1704(4)(a))</p> <p>Exception: “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</p>	<p>Residents: “[A]ny resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.” (§30-14-1704(1))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: No.</p>	<p>Timing: “[F]ollowing discovery or notification of the breach . . . [t]he disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the data system.” (§30-14-1704(1))</p> <p>Delay: Delay is permitted “if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay in notification.” Such notification “must be made after the law enforcement agency determines that it will not compromise the investigation.” (§30-14-1704(3))</p>	<p>Method: “[N]otice 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.” (§30-14-1704(5)(a))</p>	<p>For establishing own notification method: Yes. “[A] person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and that does not unreasonably delay notice is considered to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the data system.” (§30-14-1704(6))</p> <p>For following interagency guidelines: No.</p>	<p>Enforcement: Not specified.</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Montana								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>been acquired by an unauthorized person.” (§30-14-1704(2))</p> <p>Insurance companies: The Insurance Information and Privacy Protection Act, § 33-19-231, specifically requires “[a]ny licensee* or insurance-support organization** that conducts business in Montana and that owns or licenses computerized data that includes personal information [to] provide notice of any breach of the security of the system following discovery or notice of the breach of the security of the system to any individual whose unencrypted personal information was or is reasonably</p>	<p>not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.” (§30-14-1704(4)(b)(ii))</p>	<p>used or subject to further unauthorized disclosure.” (§30-14-1704(4)(a))</p> <p>Risk of harm analysis: Yes. Breach occurs only if the unauthorized acquisition “causes or is reasonably believed to cause loss or injury to a Montana resident.” (§30-14-1704(4)(a))</p>			<p>Substitute notice: “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.” (§30-14-1704(5)(b))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Montana								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>believed to have been acquired by an unauthorized person.” (§ 33-19-231)</p> <p>* “‘Licensee’ means: (a) an insurance institution, insurance producer, or other person who is licensed or required to be licensed, authorized or required to be authorized, or registered or required to be registered pursuant to this title; or (b) a surplus lines insurer.” (§ 33-19-104(16))</p> <p>** “(a) ‘Insurance-support organization’ means a person who assembles or collects information about natural persons for the purpose of providing the information to an</p>							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Montana								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	insurance institution or insurance producer for insurance transactions, including: (i) the furnishing of consumer reports or investigative consumer reports to an insurance institution or insurance producer for use in connection with an insurance transaction; or (ii) the collection of personal information from insurance institutions, insurance producers, or other insurance-support organizations for the purpose of detecting or preventing fraud, material misrepresentation, or material nondisclosure in connection with insurance underwriting or insurance claim							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Montana								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	activity. (b) The following persons are not insurance-support organizations for purposes of this chapter: insurance producers, government institutions, medical care institutions, and medical professionals.” (§ 33-19-104(13))							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Nebraska								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Neb. Rev. Stat. 87-801 <i>et seq.</i>	<p>Covered entities: “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.” (§87-803(1))</p> <p>Service provider requirement: Yes. “[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</p>	<p>Personal information: “Personal information means either of the following: (a) A Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable: (i) Social security number; (ii) Motor vehicle operator's license number or state identification card number; (iii) Account number or credit or debit card</p>	<p>Breach definition: “Breach of the security of the system means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.” (§87-802(1))</p> <p>Exception: “Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure.” (§87-802(1))</p>	<p>Residents: Notice must be given to the “affected Nebraska resident.” (§87-803(1))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: Yes. “If notice of a breach of security of the system is required by [§87-803(1)], 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.” (§87-803(2))</p>	<p>Timing: “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.” (§87-803(1))</p> <p>Delay: Notice 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.” (§87-803(4))</p>	<p>Method: “Notice means: (a) Written notice; (b) Telephonic notice; (c) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001, as such section existed on January 1, 2006; (d) Substitute notice, if the individual or commercial entity required to provide notice demonstrates that the cost of providing notice will exceed seventy-five thousand dollars, that the affected class of Nebraska residents to be notified exceeds one hundred thousand residents, or that the individual or commercial entity does not have sufficient contact information to</p>	<p>For establishing own notification method: Yes. “An individual or a commercial entity that maintains its own notice procedures which are part of an information security policy for the treatment of personal information and which are otherwise consistent with the timing requirements of [the law], is deemed to be in compliance with the notice requirements of [the law] 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.” (§87-804(1))</p> <p>For following interagency</p>	<p>State enforcement: “[T]he Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of the act.” (§87-806)</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Nebraska								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	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.” (§87-803(3))	number, in combination with any required security code, access code, or password that would permit access to a resident’s financial account; (iv) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or (v) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or (b) A user name or email address, in combination with a password or security question and answer, that would permit access to an online account.” (§87-802(5))	Exception: “Acquisition of personal information pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency is not a breach of the security of the system.” (§87-802(1)) Risk of harm analysis: Yes. Notice must be given “if the [individual’s or entity’s] investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur.” (§87-803(1))			provide notice.” (§87-802(4)) Substitute notice: “Substitute notice under [§87-802(4)(d)] requires all of the following: (i) Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents; (ii) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the individual or commercial entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks; (iii) Conspicuous	guidelines: Yes. “An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with [the law] 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.” (§87-804(2))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Nebraska								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		Exception: “Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.” (§87-802(5))				posting of the notice on the web site of the individual or commercial entity if the individual or commercial entity maintains a web site; and (iv) Notification to major media outlets in the geographic area in which the individual or commercial entity is located.” (§87-802(4)(d))		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Nevada								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Nev. Rev. Stat. §603A.010 <i>et seq.</i> ; S.B. 538	<p>Covered entities: “Any data collector that owns or licenses computerized data which includes personal information.” (§603A.220(1))</p> <p>Data collector: A data collector is “any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information.” (§603A.030)</p>	<p>Personal information: “[A] natural person’s first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: (1) Social security number. (2) Driver’s license number or identification card number. (3) Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person’s financial account.” (§603A.040)</p>	<p>Breach definition: A “breach of the security of the system data” is the “unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector.” (§603A.020)</p> <p>Exception: Breach “does not include the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, so long as the personal information is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure.” (§603A.020)</p>	<p>Residents: Any Nevada resident “whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (§603A.220(1))</p> <p>Credit reporting agency notice requirement: Yes. “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 . . . that compiles and maintains files on consumers on a nationwide basis, of the time the notification is distributed and the content of the notification.” (§603A.220(6))</p>	<p>Timing: Following discovery or notification of the breach, “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 [§603A.220(3)], or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.” (§603A.220(1))</p> <p>Delay: Notification “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.”</p>	<p>Method: “[T]he 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 <i>et seq.</i> (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.” (§603A.220(4))</p>	<p>For establishing own notification method: Yes. “A data collector which [m]aintains 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.” (§603A.220(5)(a))</p> <p>For following interagency guidelines: Yes. A data collector which “[i]s subject to and complies</p>	<p>State enforcement: “If the Attorney General or a district attorney of any county has reason to believe that any person is violating, proposes to violate or has violated the provisions of NRS 603A.010 to 603A.920, inclusive, the Attorney General or district attorney may bring an action against that person to obtain a temporary or permanent injunction against the violation.” (§603A.920)</p> <p>Private right of action: Yes – for data collectors. “A data collector that provides the notification required pursuant to NRS 603A.220 may commence an action for damages against a person that unlawfully obtained or benefited from personal</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Nevada								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>Service provider requirement: Yes. “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.” (§603A.220(2))</p> <p>“Operators” S.B. 538 also imposes certain notice requirements on “operators,” which “means a person who: (a) Owns or</p>	<p>Exception: Personal information “does not include the last four digits of a social security number, the last four digits of a driver’s license number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public.” (§603A.040)</p>	<p>Risk of harm analysis: No, except as definition of “breach” may incorporate elements of such a test.</p>	<p>Government notice requirement: No.</p>	<p>(§603A.220(3))</p>	<p>Substitute notice: “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.” (§603A.220(4)(c))</p>	<p>with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§6801 <i>et seq.</i>, shall be deemed to be in Compliance with the Notification requirements of this section.” (§603A.220(5)(b))</p>	<p>information obtained from records maintained by the data collector. A data collector that prevails in such an action may be awarded damages which may include, without limitation, the reasonable costs of notification, reasonable attorney’s fees and costs and punitive damages when appropriate. The costs of notification include, without limitation, labor, materials, postage and any other costs reasonably related to providing the notification.” (§603A.900)</p> <p>Restitution also available: “In addition to any other penalty provided by law for the breach of the security of the system data maintained by a data collector, the</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Nevada								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	operates an Internet website or online service for commercial purposes; (b) Collects and maintains covered information from consumers who reside in this State and use or visit the Internet website or online service; and (c) Purposefully directs its activities toward this State, consummates some transaction with this State or a resident thereof or purposefully avails itself of the privilege of conducting activities in this State. 2. The term does not include a third party that operates, hosts or manages an Internet website or online service on behalf of its owner or processes information on behalf of the							court may order a person who is convicted of unlawfully obtaining or benefiting from personal information obtained as a result of such breach to pay restitution to the data collector for the reasonable costs incurred by the data collector in providing the [required] notification . . . including, without limitation, labor, materials, postage and any other costs reasonably related to providing such notification.” (§603A.910)

Nevada								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	owner of an Internet website or online service.”							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

New Hampshire								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
N.H. Rev. Stat. Ann. §359-C:19 <i>et seq.</i>	<p>Covered entities: “Any person* doing business in [New Hampshire] who owns or licenses computerized data that includes personal information.” (§359-C:20(I)(a))</p> <p>* “‘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.” (§359-C:19(III))</p>	<p>Personal information: “‘Personal information’ means an individual’s first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:*</p> <p>(1) Social security Number.</p> <p>(2) Driver’s license number or other government identification number.</p> <p>(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.” (§359-C:19(IV)(a))</p>	<p>Breach definition: “‘Security breach’ means the unauthorized acquisition of computerized data* that compromises the security or confidentiality of personal information maintained by a person doing business in [New Hampshire].” (§359-C:19(V))</p> <p>* “‘Computerized data’ means personal information stored in an electronic format.” (§359-C:19(I))</p> <p>Exception: “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</p>	<p>“Affected individuals.” (§359-C:20(I)(a))</p> <p>Credit reporting agency notice requirement: Yes. “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.” (§359-C:20(VI))</p> <p>Government notice requirement: Yes. “Any person engaged in trade or commerce</p>	<p>Timing: “The disclosure shall be made to affected individuals as quickly as possible, after the determination required under this section.” (§359-C:20(b))</p> <p>Delay: Delay is permitted “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.” (§359-C:20(II))</p>	<p>Method: “The notice required under this section shall be provided by one of the following methods:</p> <p>(a) Written notice.</p> <p>(b) Electronic notice, if the agency or business’ primary means of communication with affected individuals is by electronic means.</p> <p>(c) Telephonic notice, provided that a log of each such notification is kept by the person or business who notifies affected persons.</p> <p>(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</p>	<p>For establishing own notification method: Yes. “Notice pursuant to the person’s internal notification procedures maintained as part of an information security policy for the treatment of personal information” is sufficient to comply with the law. (§359-C:20(III)(e))</p> <p>For following interagency guidelines: Yes. “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</p>	<p>State enforcement: “The New Hampshire attorney General’s office shall enforce [the law].” (§359-C:21(II))</p> <p>Private right of action: Yes. “Any person injured by any violation under this subdivision may bring an action for damages and for such equitable relief, including an injunction.” (§359-C:21(I))</p> <p>Burden of proof requirement: “The burden shall be on the person responsible for the determination [of whether ‘misuse of the information has occurred or is reasonably likely to occur’] to demonstrate compliance.” (§359-C:21(III))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

New Hampshire								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>Service provider requirement: Yes. An entity that does not own the personal information “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.” (§359-C:20(c))</p>	<p>* “‘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.” (§359-C:19(II))</p>	<p>personal information is not used or subject to further unauthorized disclosure.” (§359-C:19(V))</p> <p>Risk of harm analysis: Yes. If the entity determines “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.” (§359-C:20(I)(a))</p>	<p>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.”</p>		<p>or consent to provide notice pursuant to subparagraphs I(a)-I(c).” (§359-C:20(III))</p> <p>Substitute notice: “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.” (§359-C:20(III)(d))</p> <p>Notice contents requirement: “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</p>	<p>this subdivision if it acts in accordance with such laws, rules, regulations, guidances, or guidelines.” (§359-C:20(V))</p>	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

New Hampshire								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		Exception: “‘Personal information’ shall not include information that is lawfully made available to the general public from federal, state, or local government records.” (§359-C:19(IV)(b))		(§359-C:20(I)(b))		personal information obtained as a result of the security breach. (d) The telephonic contact information of the person subject to this section.” (§359-C:20(IV))		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

New Jersey								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
N.J. Stat. Ann. §56:8-161 <i>et seq.</i>	<p>Covered entities: “Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information.” (§56:8-163(a))</p> <p>Service provider requirement: Yes. “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 . . . of any breach of security of the computerized records immediately following discovery, if the personal information was,</p>	<p>Personal information: Personal information means “an individual’s first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) Driver’s license number or State identification card number. (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.” Additionally, “[d]issociated data that, if linked, would constitute personal information is personal information if the</p>	<p>Breach definition: A “breach of security” is the “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.” (§56:8-161)</p> <p>Exception: “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</p>	<p>Residents: “[A]ny customer* who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person.” (§56:8-163(a))</p> <p>* “Customer” means “an individual who provides personal information to a business.” (§56:8-161)</p> <p>Credit reporting agency notice requirement: Yes. “[I]n the event that a business or public entity discovers circumstances requiring notification . . . 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 . . .</p>	<p>Timing: “[F]ollowing discovery or notification of the breach, . . . [t]he 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 . . . or any measures necessary to determine the scope of the breach and restore reasonable integrity of the data system.” (§56:8-163(a))</p> <p>Delay: “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</p>	<p>Method: “[N]otice 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.” (§56:8-163(d))</p>	<p>For establishing own notification method: Yes. “[A] business or public entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and is otherwise consistent with the requirements of this section, shall be deemed to be in compliance with the notification requirements of this section 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.” (§56:8-163(e))</p> <p>For following interagency guidelines: No.</p>	<p>State enforcement: “It shall be an unlawful practice and a violation of P.L.1960, c.39 (C.56:8-1 <i>et seq.</i>) [the New Jersey Consumer Fraud Act] to willfully, knowingly or recklessly violate [the breach notification law].” (§56:8-166)</p> <p>“It shall be an unlawful practice and a violation of P.L.1960, c.39 (C.56:8-1 <i>et seq.</i>) [the New Jersey Consumer Fraud Act] to violate the provisions of [the specific health insurance provisions].” (§56:8-198)</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

New Jersey								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>or is reasonably believed to have been, accessed by an unauthorized person.” (§56:8-163(b))</p> <p>Health Insurance Carriers: New Jersey requires “health insurance carriers” that “compile or maintain computerized records that include personal information” to “[secure that information] by encryption or by any other method or technology rendering the information unreadable, undecipherable, or otherwise unusable by an unauthorized person. Compliance with this section shall require more than the use of a password protection computer</p>	<p>means to link the dissociated data were accessed in connection with access to the dissociated data.” (§56:8-161)</p> <p>Exception: 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.” (§56:8-161)</p>	<p>used for a purpose unrelated to the business or subject to further unauthorized disclosure.” (§56:8-161)</p> <p>Risk of harm analysis: Yes. “Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.” (§56:8-163(a))</p>	<p>of the timing, distribution and content of the notices.” (§56:8-163(f))</p> <p>Government notice requirement: Yes. “Any business or public entity required . . . 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.” (§56:8-163(c)(1))</p>	<p>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.” (§56:8-163(c)(2))</p>	<p>Substitute notice: “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.” (§56:8-163(d)(3))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

New Jersey								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>program, if that program only prevents general unauthorized access to the personal information, but does not render the information itself unreadable, undecipherable, or otherwise unusable by an unauthorized person operating altering, deleting, or bypassing the password protection computer program.”</p> <p>(§56:8-197(a))</p> <p>-- The law “shall only apply to end user computer systems and computerized records transmitted across public networks.”</p> <p>(§56:8-197 (b))</p> <p>-- “Health insurance carrier” is defined as “an insurance company, health service corporation,</p>							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

New Jersey								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>hospital service corporation, medical service corporation, or health maintenance organization authorized to issue health benefits plans in [New Jersey].” (§56:8-196)</p> <p>-- “Personal information” is defined in this context as “an individual’s first name or first initial and last name linked with any one or more of the following data elements:</p> <p>(1) Social Security Number;</p> <p>(2) driver’s license number or State identification card number;</p> <p>(3) address; or</p> <p>(4) identifiable health information.</p> <p>Dissociated data that, if linked, would constitute personal information is</p>							

New Jersey								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.” (§56:8-196)							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

New Mexico								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
2017 H.B. 15, Chap. 36 (effective June 16, 2017)	<p>Covered entities: “[Any] person that owns or licenses elements that include personal identifying information of a New Mexico resident.” (§6.A)</p> <p>Service provider requirement: Yes. “Any person that is licensed to maintain or possess computerized data containing personal identifying information of a New Mexico resident that the person does not own or license shall notify the owner or licensee of the information of any security breach in the most expedient time possible, but not later than forty-five calendar days following discovery of the breach, except as</p>	<p>Personal information: C. “[P]ersonal identifying information”: (1) means an individual’s first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable: (a) social security number; (b) driver’s license number; (c) government-issued identification number; (d) account number, credit card number or debit card number in combination with</p>	<p>Breach definition: A “security breach” is the “unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality or integrity of personal identifying information maintained by a person.” (§2.D)</p> <p>Exception: “‘Security breach’ does not include the good-faith acquisition of personal identifying information by an employee or agent of a person for a legitimate business purpose of the person; provided that the personal identifying information is not</p>	<p>Residents: “[E]ach New Mexico resident whose personal identifying information is reasonably believed to have been subject to a security breach.” (§6.A)</p> <p>Credit reporting agency notice requirement: Yes. “A person that is required to issue notification of a security breach pursuant to the Data Breach Notification Act to more than one thousand New Mexico residents as a result of a single security breach shall notify ... major 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 security breach in the most expedient time possible, and no later than forty-five calendar days, except</p>	<p>Timing: “Notification shall be made in the most expedient time possible, but not later than forty-five calendar days following discovery of the security breach, except as provided in Section 9 of the Data Breach Notification Act.”</p> <p>Delay: “The notification required by the Data Breach Notification Act may be delayed: A. if a law enforcement agency determines that the notification will impede a criminal investigation; or B. as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system.” (§9)</p>	<p>Method: “A person required to provide notification of a security breach pursuant to [§6.A] shall provide that notification by: (1) United States mail; (2) electronic notification, if the person required to make the notification primarily communicates with the New Mexico resident by electronic means or if the notice provided is consistent with the requirements of 15 U.S.C. Section 7001; or (3) a substitute notification, if the person demonstrates that: (a) the cost of providing notification would exceed one hundred thousand dollars (\$100,000); (b) the number of residents to be</p>	<p>For establishing own notification method: Yes. “A person that maintains its own notice procedures as part of an information security policy for the treatment of personal identifying information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the person notifies affected consumers in accordance with its policies in the event of a security breach.” (§6.F)</p> <p>For following interagency guidelines: Yes. “The provisions of the Data Breach Notification Act shall not apply to a person subject to the federal</p>	<p>State enforcement: “A. When the attorney general has a reasonable belief that a violation of the Data Breach Notification Act has occurred, the attorney general may bring an action on the behalf of individuals and in the name of the state alleging a violation of that act. B. In any action filed by the attorney general pursuant to the Data Breach Notification Act, the court may: (1) issue an injunction; and (2) award damages for actual costs or losses, including consequential financial losses. C. If the court determines that a person violated the Data Breach Notification Act knowingly or recklessly, the court may impose a civil penalty of the greater of twenty-</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

New Mexico								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	provided in Section 9 of the Data Breach Notification Act; provided that notification to the owner or licensee of the information is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud.” (§6.C)	any required security code, access code or password that would permit access to a person’s financial account; or (e) biometric data” (§2.C(1)) Exception: Personal information “does not mean information that is lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public.” (§2.C(2))	subject to further unauthorized disclosure” (§2.D) Risk of harm analysis: Yes. “[N]otification to affected New Mexico residents is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud.” (§6.B)	as provided in Section 9 of the Data Breach Notification Act.” (§10) Government notice requirement: Yes. “A person that is required to issue notification of a security breach pursuant to the Data Breach Notification Act to more than one thousand New Mexico residents as a result of a single security breach shall notify the office of the attorney general ... of the security breach in the most expedient time possible, and no later than forty-five calendar days, except as provided in Section 9 of the Data Breach Notification Act.” (§10)		notified exceeds fifty thousand; or (c) the person does not have on record a physical address or sufficient contact information for the residents that the person or business is required to notify.” (§6.D) Substitute notice: “Substitute notification ... shall consist of: (1) sending electronic notification to the email address of those residents for whom the person has a valid email address; (2) posting notification of the security breach in a conspicuous location on the website of the person required to provide notification if the person maintains a website; and (3) sending written notification to the	Gramm-Leach-Bliley Act or the federal Health Insurance Portability and Accountability Act of 1996.” (§8)	five thousand dollars (\$25,000) or, in the case of failed notification, ten dollars (\$10.00) per instance of failed notification up to a maximum of one hundred fifty thousand dollars (\$150,000).” (§11) Private right of action: No.

New Mexico								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						office of the attorney general and major media outlets in New Mexico.” (§6.E)		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

New York								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
N.Y. Gen. Bus. Law § 899-aa	<p>Covered entities: “Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information.” (§899-aa(2))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “Personal information” means “any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.” (§899-aa(1)(a))</p> <p>Private information: “Private information” means “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</p>	<p>Breach definition: “‘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 . . . 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</p>	<p>Residents: “[A]ny resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.” (§899-aa(2))</p> <p>Credit reporting agency notice requirement: Yes. “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.” (§899-aa(8)(b)))</p> <p>* “‘Consumer reporting agency’ shall mean any person which, for monetary fees, dues, or on a cooperative</p>	<p>Timing: “[F]ollowing discovery or notification of the breach in the security of the system . . . [t]he 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 [§899-aa(4)], or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.” (§899-aa(2))</p> <p>Delay: Notification “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</p>	<p>Method: “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.</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: No.</p>	<p>State enforcement: “(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,</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

New York								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	been, acquired by a person without valid authorization.” (§899-aa(3))	number; (2) driver’s license or state identification 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.” (§899-aa(1)(b)) Exception: “Private information” does not include “publicly available information that is lawfully made available to the general public from federal, state, or local government records.” (§899-aa(1)(b))	lost or stolen computer or other device containing information; (2) indications that the information has been downloaded or copied; (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.” (§899-aa(1)(c)) Exception: “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.” (§899-aa(1)(c))	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.” (§899-aa(1)(d)) Government notice requirement: Yes. “In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the	does not compromise such investigation.” (§899-aa(4))	(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.” (§899-aa(5)) Substitute notice: “Substitute notice shall consist of all of the following: (1) e-mail notice when such business has an e-mail address for the		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

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

New York								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			Risk of harm analysis: No, except as definition of “breach” may incorporate elements of such a test.	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.” (§899-aa(8)(a))		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.” (§899-aa(5)(d)) Notice contents requirement: “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		the date of discovery of such act.” (§899-aa(6)) Preemption: “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.” (§899-aa(9)) Private right of action: No.

New York								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						private information were, or are reasonably believed to have been, so acquired.” (§899-aa(7))		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

North Carolina								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
N.C. Gen. Stat. §75-60 <i>et seq.</i>	<p>Covered entities: “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).” (§75-65(a))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “‘Personal information’ [means a] person’s first name or first initial and last name in combination with identifying information* as defined in G.S. 14-113.20(b).” (§75-61(10))</p> <p>* “The term ‘identifying information’ . . . includes the following: (1) Social security or employer taxpayer identification numbers. (2) Drivers license, State identification card, or passport numbers. (3) Checking account numbers. (4) Savings account numbers. (5) Credit card numbers. (6) Debit card numbers.</p>	<p>Breach definition: A “security breach” is an “incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach.” (§75-61(14))</p> <p>Exception: “Good faith acquisition of personal information by an employee or agent</p>	<p>The “affected person.” (§75-65(a))</p> <p>Person: “Person” means “[a]ny individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency, or other entity.” (§75-61(9))</p> <p>Credit reporting agency notice requirement: Yes. “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</p>	<p>Timing: “[F]ollowing discovery or notification of the breach . . . [t]he disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in [§75-65(c)], 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.” (§75-65(a))</p> <p>Delay: Notification may 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</p>	<p>Method: “[N]otice 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</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: Yes. “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</p>	<p>State enforcement: Violations are treated as “[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce” for which the Attorney General may seek both civil and criminal penalties. (§§75-65(i), 75-1.1, 13, 15.2)</p> <p>Private right of action: Yes, but only if an “individual is injured as a result of the violation” of the Act. (§75-65(i))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

North Carolina								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	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 [(§75-65(c)].” (§75-65(b))	(7) Personal Identification (PIN) Code** as defined in G.S. 14-113.8(6). (8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names. (9) Digital signatures. (10) Any other numbers or information that can be used to access a person's financial resources. (11) Biometric data. (12) Fingerprints. (13) Passwords. (14) Parent's legal surname prior to marriage.” (§14-113.20(b)) ** “‘Personal identification code’ means a numeric and/or alphabetical code	of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.” (§75-61(14)) Risk of harm analysis: Yes. Notification is only required “where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security	nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.” (§75-65(f)) Government notice requirement: Yes. “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.” (§75-65(e1))	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. [Notice] 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.” (§75-65(c))	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.” (§75-65(e)) Substitute notice: “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	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.” (§75-65(h))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

North Carolina								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>assigned to the cardholder of a financial transaction card by the issuer to permit authorized electronic use of that FTC.” (§14-113.8(6))</p> <p>Exception: “Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records.” (§75-61(10))</p>	breach.” (§71-61(14))			<p>page of the business, if one is maintained. c. Notification to major statewide media.” (§75-65(e)(4))</p> <p>Notice contents requirement: “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.</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

North Carolina								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						(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." (§75-65(d))		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

North Dakota								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
N.D. Cent. Code §51-30-01 <i>et seq.</i>	<p>Covered entities: “Any person that owns or licenses computerized data that includes personal information.” (§51-30-02)</p> <p>Service provider requirement: Yes. “Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (§51-30-03)</p>	<p>Personal information: “‘Personal information’ means an individual’s first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted: (1) The individual’s social security number; (2) The operator’s license number assigned to an individual by the department of transportation 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</p>	<p>Breach definition: A “[b]reach of the security of the system” is the “unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or data bases unreadable or unusable.” (§51-30-01(1))</p> <p>Exception: “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.” (§51-30-01(1))</p>	<p>Residents: Any North Dakota resident “whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (§51-30-02)</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: Yes. “[A]ny 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.” (§51-30-02)</p>	<p>Timing: “[F]ollowing discovery or notification of the breach in the security of the data . . . [t]he disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.” (§51-30-02)</p> <p>Delay: Delay is permitted “if a law enforcement agency determines that the notification will impede a criminal investigation.” Notification “must be made after the law enforcement agency determines that it will not compromise the investigation.”</p>	<p>Method: “Notice under this chapter may be provided by one of the following methods: 1. Written notice; 2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of title 15 of the United States Code; or 3. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person does not have sufficient contact information.” (§51-30-05)</p>	<p>For establishing own notification method: Yes. If a person “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” under North Dakota’s law, then that person “is deemed to be in compliance with the notification requirements of [the law] if the person notifies the subject individuals in accordance with its policies in the event of a breach of the security of the system.” (§51-30-06)</p> <p>For following interagency guidelines: Yes. If a “financial institution, trust company, or credit union” is “subject</p>	<p>State enforcement: “The attorney general may enforce this chapter. The attorney general, in enforcing this chapter, has all the powers provided in chapter 51-15 [which prohibits ‘any deceptive act or practice’] and may seek all the remedies in chapter 51-15 [including injunctions and civil penalties of ‘not more than five thousand dollars for each violation’]. A violation of this chapter is deemed a violation of chapter 51-15. The remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties under chapter 51-15, or otherwise provided by law.” (§51-30-07)</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

North Dakota								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		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	Risk of harm analysis: No, except as definition of "breach" may incorporate elements of such a test.		(§51-30-04)	Substitute notice: "Substitute notice consists of the following: a. E-mail notice when the person has an e-mail address for the subject persons; b. Conspicuous posting of the notice on the person's website page, if the person maintains one; and c. Notification to major statewide media." (§51-30-05)	to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice" then such financial institution, trust company, or credit union "is deemed to be in compliance" with North Dakota's law. (§51-30-06)	Private right of action: No.

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

North Dakota								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>individual's digitized or other electronic signature.” (§51-30-01(4)(a))</p> <p>* 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.” (§51-30-01(3))</p> <p>** 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.” (§51-30-01(2))</p> <p>Exception: “‘Personal information’ does not include</p>						

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

North Dakota								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		publicly available information that is lawfully made available to the general public from federal, state, or local government records.” (§51-30-01(4)(b))						

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Ohio								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Ohio Rev. Code Ann. §1349.19	<p>Covered entities: “Any person* that owns or licenses computerized data that includes personal information.” (§1349.19(B)(1))</p> <p>* “[P]erson” includes a business entity only if the business entity conducts business in [Ohio].” (§1349.19(A)(6))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “[A]n 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</p>	<p>Breach definition: A “[b]reach of the security of the system” is “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 [Ohio].” (§1349.19(A)(1)(a))</p> <p>Exception: “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</p>	<p>Residents: “[A]ny resident of [Ohio] whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person.” (§1349.19(B)(1))</p> <p>Credit reporting agency notice requirement: Yes. “If a person discovers circumstances that require disclosure under this section to more than one thousand residents of [Ohio] 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</p>	<p>Timing: Notice should be given “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 [§1349.19(D)] 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.” (§1349.19(B)(2))</p> <p>Delay: “The person may delay the disclosure or notification . . . if a law enforcement agency determines that the disclosure or notification will impede a criminal</p>	<p>Method: “[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) Telephonic notice; (4) Substitute notice if the person required to disclose demonstrates that the person does not have sufficient contact information to provide notice in a manner described [above], the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed \$250,000, or the affected class of subject residents to whom disclosure or</p>	<p>For establishing own notification method: No, but disclosure “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.” (§1349.19(B)(1))</p> <p>For following interagency guidelines: Yes. “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,</p>	<p>State enforcement: “The attorney general may . . . bring a civil action upon an alleged failure by a person to comply with the requirements of this section.” (§1349.19(I))</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Ohio								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	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 [Ohio].” (§1349.19(C))	access to an individual’s financial account.” (§1349.19(A)(7)(a)) Exception: “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,	system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure.” (§1349.19(A)(1)(b)(i)) Exception: “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.” (§1349.19(A)(1)(b)(ii)) Risk of harm analysis: Yes. Notification is only required “if the access and acquisition by the unauthorized person causes or reasonably is believed will cause	disclosure given by the person to the residents of [Ohio].” (§1349.19(G)) Government notice requirement: No.	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.” (§1349.19(D))	notification is required exceeds 500,000 persons. Substitute notice under this provision 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 percent of the population of [Ohio]; (5) Substitute notice	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.” (§1349.19(F)(1))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Ohio								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		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.” (§1349.19(A)(7)(b))	a material risk of identity theft or other fraud to the resident.” (§1349.19(B)(1))			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.” (§1349.19(E)) Substitute notice: “Substitute notice under this provision shall consist of all of the following: (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		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Ohio								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>least once a week for three consecutive weeks;</p> <p>(b) Conspicuous posting of the disclosure or notice on the business entity's web site, if the entity maintains one;</p> <p>(c) Notification to major media outlets in the geographic area in which the business entity is located."</p> <p>(§1349.19(E))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Oklahoma								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Okla. Stat. tit. 24, §161 <i>et seq.</i>	<p>Covered entities: “An individual or entity that owns or licenses computerized data that includes personal information.” (§163(A))</p> <p>Entity: “[E]ntity” 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.” (§162(2))</p>	<p>Personal information: “[T]he 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[n] [Oklahoma] resident...when the data elements are neither encrypted nor redacted: (a) social security number (b) driver license number or state identification card number issued in lieu of a driver license, or (c) financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident.”</p>	<p>Breach definition: “‘Breach of the security of a system’ means the unauthorized access and acquisition of unencrypted* and unredacted** computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.” (§162(1))</p> <p>* “‘Encrypted’ means transformation of data through the use of an algorithmic process into a form in which there is a</p>	<p>Residents: “[A]ny resident of [Oklahoma] 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.” (§163(A))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: No.</p>	<p>Timing: “[F]ollowing discovery or notification of the breach of the security of the system . . . [e]xcept as [required by law enforcement] 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 disclosure shall be made without unreasonable delay.” (§163(A))</p> <p>Delay: Delay is permitted “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</p>	<p>Method: “‘Notice’ means: a. written notice to the postal address in the records of the individual or entity, b. telephone notice, c. electronic notice, or d. substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed Fifty Thousand Dollars (\$50,000.00), or that the affected class of residents to be notified exceeds one hundred thousand (100,000) persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in subparagraph a, b or c of this paragraph.” (§162(7))</p>	<p>For establishing own notification method: Yes. “An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies residents of this state in accordance with its procedures in the event of a breach of security of the system.” (§164(A))</p> <p>For following interagency guidelines: Yes: “A financial institution that complies with the notification requirements prescribed by the</p>	<p>State enforcement: “A. A violation of this act that results in injury or loss to residents of [Oklahoma] may be enforced by the Attorney General or a district attorney in the same manner as an unlawful practice under the Oklahoma Consumer Protection Act. B. Except as provided in subsection C of this section, the Attorney General or a district attorney shall have exclusive authority to bring action and may obtain either actual damages for a violation of this act or a civil penalty not to exceed One Hundred Fifty Thousand Dollars</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Oklahoma								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	Service provider requirement: Yes. “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.” (tit. 24, §163(C))	(§162(6)) Exception: Personal information “does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.” (§162(6))	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 unreadable or unusable.” (§162(3)) ** “‘Redact’ means alteration or truncation of data such that no more than the following are accessible as part of the personal information: a. five digits of a social security number, or b. the last four digits of a driver license number, state identification card number or account number.” (§162(8)) “An individual or entity must disclose the breach of the security of the system if encrypted information is accessed and		determines that notification will no longer impede the investigation or jeopardize national or homeland security.” (§163(D)) Notice may also be delayed “to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system.” (§163(A))	Substitute notice: Substitute notice consists of any two of the following: (1) e-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents, (2) conspicuous posting of the notice on the Internet web site of the individual or the entity if the individual or the entity maintains a public Internet web site, or (3) notice to major statewide media.” (§162(7)(d))	Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the provisions of this act.” (§164(B)(1))	(\$150,000.00) per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation. C. A violation of this act by a state-chartered or state-licensed financial institution shall be enforceable exclusively by the primary state regulator of the financial institution. Added by Laws.” (§165) Private right of action: No.

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Oklahoma								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			<p>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.” (§163(B))</p> <p>Exception: “Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further</p>					

Oklahoma								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			<p>unauthorized disclosure.” (§162(1))</p> <p>Risk of harm analysis: Yes. Notification is required only if the breach “causes, or the individual or entity reasonably believes [it] has caused or will cause, identity theft or other fraud to any [Oklahoma] resident.” (§163(A))</p>					

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Oregon								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Oregon Revised Statutes §646A.600 <i>et seq</i>	<p>Covered entities: “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.” (§604(1))</p> <p>Person: 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 [under Oregon law].” (§602(10))</p> <p>Service provider requirement: Yes. “A person that maintains or</p>	<p>Personal information: “‘Personal information’ means: (a) A consumer’s first name or first initial and last name in combination with any one or more of the following data elements, if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired: (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</p>	<p>Breach definition: A “[b]reach of security means an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains.” (§602(1)(a))</p> <p>Exception: “‘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.”</p>	<p>Consumers: “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.” (§604(1)(a))</p> <p>“‘Consumer’ means an individual resident of [Oregon].” (§602(2))</p> <p>Credit reporting agency notice requirement: Yes. “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</p>	<p>Timing: Notification shall be made “in the most expeditious manner possible, without unreasonable delay, consistent with the legitimate needs of law enforcement described in [§604(3)] 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.” (§604(1)(a))</p> <p>Delay: “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</p>	<p>Method: Notification can be made: “(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 the effective date of this 2015 Act; (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</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: Yes. “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, guidelines or guidance provide greater protection to personal information and disclosure requirements at least as thorough as the protections and disclosure requirements</p>	<p>State enforcement: “If the [Director of the Department of Consumer and Business Services] has reason to believe that any person has engaged or is engaging in any violation of [the breach notification law], the director may issue an order, subject to ORS chapter 183, directed to the person to cease and desist from the violation, or require the person to pay compensation to consumers injured by the violation.” (§624(3))</p> <p>Penalties: “(a) In addition to all other penalties and enforcement provisions provided by law, any person who violates or who procures, aids or abets in the violation of [the breach notification law] shall be subject to a penalty of not</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Oregon								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	otherwise possesses personal information on behalf of, or under license of, another person shall notify the other person after discovering a breach of security.” (§604(2))	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	(§602(1)(b)) Risk of harm analysis: Yes. “[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.” (§604(7))	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.” (§604(6)) Government notice requirement: Yes. Notice must be given to the “Attorney General, either in writing or electronically, if the number of consumers to whom the person must send the notice [. . .] exceeds 250.” (§604(1)(b))	will impede a criminal investigation and if the law enforcement agency requests in writing that the person delay the notification.” (§604(3))	exceeds 350,000, or if the person does not have sufficient contact information to notify affected consumers.” (§604(4)) Substitute notice: “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.” (§604(4)(d)) Notice contents requirement: “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	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 the effective date of this 2015 Act. (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 the effective date	more than \$1,000 for every violation, which shall be paid to the General Fund of the State Treasury. (b) Every violation is a separate offense and, in the case of a continuing violation, each day’s continuance is a separate violation, but the maximum penalty for any occurrence shall not exceed \$500,000. (c) Civil penalties under this section shall be imposed as provided in ORS 183.745.” (§624(4)) Private right of action: Yes (implicitly authorized). “The director [of the Department of Consumer and Business Services] may order compensation to consumers only upon a finding that enforcement of the rights of the

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Oregon								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		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				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.” (§604(5))	of this 2015 Act, that is governed under 45 C.F.R. parts 160 and 164, as in effect on the effective date of this 2015 Act, 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	consumers by private civil action would be so burdensome or expensive as to be impractical.” (§624(3))

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Oregon								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>paragraph (a) of this subsection without the consumer's first name or first initial and last name if:</p> <p>(i) Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and</p> <p>(ii) The data element or combination of data elements would enable a person to commit identity theft against a consumer.”</p> <p>(§§602(11)(a), (b))</p> <p>Exception: Personal information “does not include information in a federal, state or local government record, other than a Social Security number, that is lawfully made</p>					<p>notice described in subparagraph (A) of this paragraph to the Attorney General within a reasonable time after the Attorney General requests the copy.”</p> <p>(§604(8))</p>	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Oregon								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		available to the public.” (§602(11)(c))						

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Pennsylvania								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
73 Pa. Stat. §2301 <i>et seq.</i>	<p>Covered entities: “An entity* that maintains, stores, or manages computerized data that includes personal information.” (§2303(a))</p> <p>* “Entity” means a “[s]tate agency, a political subdivision of [Pennsylvania] or an individual or a business doing business in [Pennsylvania].” (§2302)</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal information: “An individual’s first name or first initial and last name in combination with and linked to any one or more of the following data elements, when the name and data elements are not encrypted or redacted: (i) Social security number; (ii) Driver’s license number or state identification card number; (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.” (§2302)</p>	<p>Breach definition: A “[b]reach of the security of the system” is “[t]he 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 [Pennsylvania].” (§2302)</p> <p>Exception: “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</p>	<p>Residents: “[A]ny resident of [Pennsylvania] whose unencrypted and unredacted personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person.” (§2303(a))</p> <p>Credit reporting agency notice requirement: Yes. “When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.” (§2305)</p> <p>Government notice requirement: No.</p>	<p>Timing: “Except as provided in [(§2304) authorization delay pursuant to the needs of law enforcement] 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.” (§2303(a))</p> <p>Delay: “The notification required by this act may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. The notification required by this act shall be made after the law enforcement agency determines that it will not compromise the</p>	<p>Method: “[Notice] [m]ay 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</p>	<p>For establishing own notification method: Yes. “An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.” (§2307(a))</p> <p>For following interagency guidelines: Yes. “(1) A financial institution that complies with the notification requirements prescribed by the</p>	<p>State enforcement: “A violation of this act shall be deemed to be an unfair or deceptive act or practice in violation of the act of December 17, 1968 (P.L.1224, No.387), known as the Unfair Trade Practices and Consumer Protection Law.” (§2308)</p> <p>Private right of action: No. “The Office of Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.” (§2308)</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Pennsylvania								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	maintains, stores, or manages the data.” (§2303(c))	Exception: “‘Personal information’ does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.” (§2302)	personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.” (§2302) Risk of harm analysis: No, except insofar as the definition of “breach” incorporates elements of such a test.		investigation or national or homeland security.” (§2304)	entity has a valid e-mail address for the individual. (4) . . . 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.” (§2302) Substitute notice: “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	Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this act. (2) An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity’s primary or functional Federal regulator shall be in compliance with this act.” (§2307(b))	

Pennsylvania								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						major Statewide media.” (§2302)		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Puerto Rico								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
10 L.P.R.A. St §4051 <i>et seq.</i>	<p>Covered entities: “Any entity* that is the owner or custodian of a database that includes personal information of citizen residents of Puerto Rico.” (§4052)</p> <p>* Entity means “every agency, board, body, examining board, corporation, public corporation, committee, independent office, division, administration, bureau, department, authority, official, instrumentality or administrative organism of the three branches of the Government; every corporation, partnership, association, private company or organization authorized to do business or operate in the Commonwealth of</p>	<p>Personal information: “‘Personal information file’ refers to a file containing at least the name or first initial and the surname of a person, together with any of the following data so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code: (1) Social security number; (2) Driver’s License Number, Voter’s Identification or other Official Identification; (3) Bank or financial account numbers of any type with or</p>	<p>Breach definition: “[Violation of the Security System] means any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. This includes both access to the data banks through the system and physical access to the recording media</p>	<p>Residents: Affected “citizen Residents of Puerto Rico.” A covered entity “must notify said citizens of any breach of the security of the system when the database whose security has been breached contains, in whole or in part, personal information files and the same are not protected by an encrypted code but only by a password.” (§4052)</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: Yes. The Department of Consumer Affairs must be notified within 10 days after the violation of the system’s security has been detected. (§4052)</p> <p>Additionally, “[i]n those cases in which the breach or irregularity in the</p>	<p>Timing: Clients [presumably meaning affected citizens] “must be notified as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system’s security.” (§4052)</p> <p>Delay: Before providing notice, covered entities may “tak[e] into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system’s security.” However, “[w]ithin a non-extendable term of ten (10) days after the violation of the system’s security has</p>	<p>Method: “To notify the citizens the entity shall have the following options: (1) Written direct notice to those affected by mail or by authenticated electronic means according to the Digital Signatures Act. (2) When the cost of notifying all those potentially affected according to subsection (1) of this section or of identifying them is excessively onerous due to the number of persons affected, to the difficulty in locating all persons or to the economic situation of the enterprise or entity; or whenever the cost exceeds one hundred thousand dollars (\$100,000) or the number of persons exceeds one hundred thousand [(\$100,000)], the entity shall issue the notice through the</p>	<p>For establishing own notification method: Possibly. The Act states that “[n]o provision of this Act shall be interpreted as being prejudicial to those institutional information and security policies that an enterprise or entity may have in force prior to its effectiveness and whose purpose is to provide protection equal or better to the information on security herein established.” (§4054)</p> <p>For following interagency guidelines: No.</p>	<p>State enforcement: The Secretary of State “may impose fines of five hundred (500) dollars up to a maximum of five thousand (5,000) dollars for each violation.” (§4055)</p> <p>Private right of action: Yes. “The fines [imposed by the Secretary of State] do not affect the rights of the consumers to initiate actions or claims for damages before a competent court.” (§4055)</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Puerto Rico								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>Puerto Rico; as well as every public or private educational institution, regardless of the level of education offered by it.” (§4051)(d))</p> <p>Service provider requirement: Yes. “Any entity that as part of their operations resells or provides access to digital data banks that at the same time contain personal information files of citizens must notify the proprietor, custodian or holder of said information of any violation of the system’s security that has allowed access to those files to unauthorized persons.” (§4052)</p>	<p>without passwords or access code that may have been assigned; (4) Names of users and passwords or access codes to public or private information systems; (5) Medical information protected by the HIPAA; (6) Tax information; or (7) Work-related evaluations.” (§4051)(a))</p> <p>Exception: A “personal information file” does not include “mailing [or] residential address[es]” or “information that is a public document and that is available to the citizens in general.” (§4051)(a))</p>	<p>that contain the same and any removal or undue retrieval of said recordings.” (§4051)(c))</p> <p>Risk of harm analysis: No, except insofar as definition of a “breach” incorporates elements of such a test.</p>	<p>security systems of the database occurs in a government agency or public corporation, it shall be notified to the Citizen's Advocate Office, which shall assume jurisdiction. For this purpose, the Citizen's Advocate shall designate a Specialized Advocate who shall address these types of cases.” (§4054a)</p>	<p>been detected, the parties responsible shall inform the Department [of Consumer Affairs], which shall make a public announcement of the fact within twenty-four (24) hours after having received the information.” (§4052)</p>	<p>following two (2) steps: (a) Prominent display of an announcement to that respect at the entities premises, on the web page of the entity, if any, and in any informative flier published and sent through mailing lists both postal and electronic, and (b) a communication to that respect to the media informing of the situation and providing information as to how to contact the entity to allow for better follow-up. When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented towards</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Puerto Rico								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>that sector.” (§4053)</p> <p>Notice contents requirement: “The notice of breach of the security of the system shall be submitted in a clear and conspicuous manner and should describe the breach of the security of the system in general terms and the type of sensitive information compromised. The notification shall also include a toll free number and an Internet site for people to use in order to obtain information or assistance.” (§4053)</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Rhode Island								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
R.I. Gen. Laws §11-49.3-1 <i>et seq.</i>	<p>Covered entities: “Any municipal agency, state agency, or person* that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information.” (§11-49.3-4(a)(1))</p> <p>*A “[p]erson” includes “any individual, sole proprietorship, partnership, association, corporation, joint venture, business or legal entity, trust, estate, cooperative, or other commercial entity.” (§11-49.3-3(a)(7))</p> <p>Service provider requirement: Yes. “(a)(1) Any municipal agency, state agency, or person that stores, owns, collects, processes, maintains,</p>	<p>Personal information: “[A]n individual’s first name or first initial and last name in combination with any one or more of the following data elements, when the name and the data elements are not encrypted or are in hard copy, paper format: (i) Social security number; (ii) Driver’s license number, Rhode Island identification card number, or tribal identification number; (iii) Account number, credit, or debit card number, in combination with any required security code, access code, password, or personal identification number, that would permit access to an</p>	<p>Breach definition: A “[b]reach of the security of the system” is the “unauthorized access or acquisition of unencrypted, computerized data information that compromises the security, confidentiality, or integrity of personal information maintained by the municipal agency, state agency, or person.” (§11-49.3-3(a)(1))</p> <p>Exception: “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.” (§11-49.3-3(a)(1))</p>	<p>Residents: “[A]ny resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity.” (§11-49.3-4(a)(1))</p> <p>Credit reporting agency notice requirement: Yes. “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 major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals. Notification to ... the major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents.” (§11-49.3-4(a)(2))</p>	<p>Timing: Following “any disclosure of personal information, or any breach of the security of the system, that poses a significant risk of identity theft,” “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 [§11-49.3-4(d)], and shall be consistent with the legitimate needs of law enforcement as provided in [§11-49.3-4(c)].” (§11-49.3-4(a))</p> <p>Delay: “The notification required by this section may be delayed if a federal, state, or local law enforcement agency determines that the notification will</p>	<p>Method: “[N]otice” may be provided by one of the following methods: (1) Written notice; (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set for the in 15 U.S.C. § 7001; or (3) Substitute notice, if the municipal agency, state agency, or person demonstrates that the cost of providing notice would exceed twenty-five thousand dollars (\$25,000), or that the affected class of subject persons to be notified exceeds fifty thousand (50,000), or the municipal agency, state agency, or person does not have sufficient contact information. (§11-49.3-3(c))</p>	<p>For establishing own notification method: Yes. “(a) Any municipal agency, state agency, or person shall be deemed to be in compliance with the security breach notification requirements of § 11-49.3-4 if: (1) The municipal agency, state agency, or person maintains its own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of § 11-49.3-4, and notifies subject persons in accordance with such municipal agency’s, state agency’s, or person’s notification policies in the event of a breach of security.” (§11-49.3-6(a)(1))</p>	<p>Civil penalties: “(a) Each reckless violation of this chapter is a civil violation for which a penalty of not more than one hundred dollars (\$100) per record may be adjudged against a defendant. (b) Each knowing and willful violation of this chapter is a civil violation for which a penalty of not more than two hundred dollars (\$200) per record may be adjudged against a defendant. (c) Whenever the attorney general has reason to believe that a violation of this chapter has occurred and that proceedings would be in the public interest, the attorney general may bring an action in the name of the state against the business or person in violation.” (§11-49.3-5)</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Rhode Island								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	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.” (§11-49.3-4(a)(1))	individual’s financial account. (iv) Medical* or health insurance** information; or (v) E-mail address with any required security code, access code, or password that would permit access to an individual’s personal, medical, insurance, or financial account.” (§11-49.3-3(a)(8)) * “Medical information” is “any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional or provider.” (§11-49.3-3(a)(4)) ** “Health insurance information” is “an individual’s health insurance	Risk of harm analysis: Yes. “(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.” (§11-49.3-4(a)(1))	Government notice requirement: Yes. “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 ... as to the timing, content, and distribution of the notices and the approximate number of affected individuals. Notification to the attorney general ... shall be made without delaying notice to affected Rhode Island residents.” (§11-49.3-4(a)(2))	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	Substitute notice: “Substitute notice shall consist of all of the following: (A) E-mail notice when the municipal agency, state agency, or person has an e-mail address for the subject persons; (B) Conspicuous posting of the notice on the municipal agency’s, state agency’s or person’s website page, if the municipal agency, state agency, or person maintains one; and (C) Notification to major statewide media.” (§11-49.3-3(c)(iii))	For following interagency guidelines: Yes. -- If “[t]he person maintains a security breach procedure pursuant to the rules, regulations, procedures, or guidelines established by the primary or functional regulator, as defined in 15 U.S.C. § 6809(2), and notifies subject persons in accordance with the policies or the rules, regulations, procedures, or guidelines established by the primary or functional regulator in the event of a breach of security of the system.” (§11-49.3-6(a)(2)) -- “A financial institution, trust company, credit union, or its affiliates that is subject to and examined for, and	Private right of action: No.

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Rhode Island								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>policy number, subscriber identification number, or any unique identifier used by a health insurer to identify the individual.” (§11-49.3-3(a)(3))</p> <p>Exception: “[P]ersonal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.” (§11-49.3-3(b))</p>			<p>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.” (§11-49.3-4(b))</p>		<p>found in compliance with, the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed in compliance with this chapter.” (§11-49.3-6(b))</p> <p>-- “A provider of health care, health care service plan, health insurer, or a covered entity governed by the medial privacy and security rules issued by the Federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with</p>	

Rhode Island								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
							this chapter.” (§11-49.3-6(c))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

South Carolina								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
S.C. Code §39-1-90	<p>Covered entities: “A person* conducting business in [South Carolina], and owning or licensing computerized data or other data that includes personal identifying information.” (§39-1-90(A))</p> <p>* A “person” includes “a natural person, an individual, or an organization.” (§37-20-110)</p> <p>Service provider requirement: Yes. “A person conducting business in [South Carolina] 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</p>	<p>Personal information: ““Personal identifying information” means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted: (a) social security number; (b) driver’s license number or state identification card number issued instead of a driver’s license; (c) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit</p>	<p>Breach definition: ““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.” (§39-1-90(D)(1))</p> <p>Exception: “Good faith acquisition of personal identifying information by an employee or agent of the person for the purposes of its</p>	<p>Residents: “[A] resident of [South Carolina] 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.” (§39-1-90(A))</p> <p>Credit reporting agency and government notice requirement: Yes. “If a business provides notice to more than one thousand persons at one time pursuant to this section, the business shall notify, without unreasonable</p>	<p>Timing: “[F]ollowing discovery or notification of the breach in the security . . . [t]he 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 [§39-1-90(D)], or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” (§39-1-90(A))</p> <p>Delay: Notification “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</p>	<p>Method: “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</p>	<p>For establishing own notification method: Yes. “[A] person that maintains its own notification procedures as part of an information security policy for the treatment of personal identifying information and is otherwise consistent with the timing requirements of this section is considered to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with its policies in the event of a breach of security of the system.” (§39-1-90(F))</p> <p>For following interagency guidelines: Yes. -- The law “does not apply to a bank or financial institution that is subject to and in compliance with</p>	<p>State enforcement: “A person who knowingly and wilfully [sic] 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.” (§39-1-90(H))</p> <p>Private right of action: Yes. “A resident of [South Carolina] 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 [sic] and knowing violation; (2) institute a civil action that must be</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

South Carolina								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	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.” (§39-1-90(B))	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.” (§39-1-90(D)(3)) Exception: Personal identifying information “does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.” (§39-1-90(D)(3))	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.” (§39-1-90(D)(1)) Risk of harm analysis: Yes. Notification is required only if “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.” (§39-1-90(A))	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.” (§39-1-90(K))	the investigation.” (§39-1-90(C))	person has insufficient contact information.” (§39-1-90(E)) Substitute notice: “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.” (§39-1-90(E)(4))	the privacy and security provision of the Gramm-Leach-Bliley Act.” (§39-1-90(I)) -- “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 [the law].” (§39-1-90(J))	limited to actual damages resulting from a violation in case 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.” (§39-1-90(G))

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Tennessee								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Tenn. Code Ann. §47-18-2107	<p>Covered entities: Any “information holder,” which is defined as “any person or business that conducts business in [Tennessee], or any agency of [Tennessee] or any of its political subdivisions, that owns or licenses computerized personal information of residents of [Tennessee].” (§§2107(b), (a)(3))</p> <p>Exception: “This section does not apply to any information holder that is subject to: (1) Title V of the Gramm-Leach-Bliley Act of 1999 (Pub. L. No. 106-102); or (2) The Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d et seq.), as expanded by the Health</p>	<p>Personal information: “[A]n 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 number, 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.” (§2107(a)(4)(A))</p> <p>Exception: Personal information “[d]oes not include information that is lawfully made available to the</p>	<p>Breach definition: A “[b]reach of system security” is the “acquisition of” “[u]nencrypted computerized data; or [e]ncrypted computerized data and the encryption key” “by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder.” (§2107(a)(1)(A))</p> <p>Exception: “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.”</p>	<p>Residents: “[A]ny resident of [Tennessee] whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (§2107(b))</p> <p>Credit reporting agency notice requirement: Yes. “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.” (§2107(g))</p>	<p>Timing: “[F]ollowing discovery or notification of a breach of system security ... [t]he 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 [§2107(d)].” (§2107(b))</p> <p>Delay: Delay permitted “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</p>	<p>Method: “[N]otice 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</p>	<p>For establishing own notification method: Yes. “[I]f 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.” (§2107(f))</p> <p>For following interagency guidelines: No.</p>	<p>State enforcement: Not specified.</p> <p>Private right of action: Yes. “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.” (§2107(h))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Tennessee								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>Information Technology for Clinical and Economic Health Act (42 U.S.C. § 300jj et seq., and 42 U.S.C. § 17921 et seq.).” (§2107(i))</p> <p>Service provider requirement: Yes. “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</p>	<p>general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable.” (§2107(a)(4)(B))</p>	<p>(§2107(a)(1)(B))</p> <p>Risk of harm analysis: No, except as definition of “breach” may incorporate elements of such a test.</p>	<p>Government notice requirement: No.</p>	<p>investigation.” (§2107(d))</p>	<p>does not have sufficient contact information.” (§2107(e))</p> <p>Substitute notice: “[C]onsists 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.” (§2107(e)(3))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Tennessee								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	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 [§2107(d)].” (§2107(c))							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Texas								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Tex. Bus. & Com. Code §§ 521.002, 521.053, 521.151	<p>Covered entities: “A person who conducts business in [Texas] and owns or licenses computerized data that includes sensitive personal information.” (§521.053(b))</p> <p>Service provider requirement: Yes. “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.” (§521.053(c))</p>	<p>Sensitive personal information: “‘Sensitive personal information’ means . . . (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;</p>	<p>Breach definition: 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.” (§521.053(a))</p> <p>Exception: “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</p>	<p>Affected individuals: “[A]ny individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (§521.053(b))</p> <p>Credit reporting agency notice requirement: Yes. “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.” (§521.053(h))</p>	<p>Timing: “The disclosure shall be made as quickly as possible....” (§521.053(b))</p> <p>Delay: Delay is permitted: -- “[A]s necessary to determine the scope of the breach and restore the reasonable integrity of the data system”; or -- “[A]t 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.” (§§521.053(b),(d))</p>	<p>Method: “(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) [substitute notice] [i]f the person required to give notice under [the law] demonstrates that the cost of providing notice would exceed \$250,000 [or] the number of affected persons exceeds 500,000....” (§521.053(e))</p> <p>Substitute notice: “[Substitute] 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</p>	<p>For establishing own notification method: Yes. “[A] person who maintains the person’s own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy.” (§521.053(g))</p> <p>For following interagency guidelines: No.</p>	<p>State enforcement: “The attorney general may bring an action to recover the civil penalty imposed under this subsection.” (§521.151(g))</p> <p>Penalties: -- “A person who violates this chapter is liable to this state for a civil penalty of at least \$2,000 but not more than \$50,000 for each violation. The attorney general may bring an action to recover the civil penalty imposed under this subsection.” (§521.151(a)) -- “In addition to [general civil] penalties assessed under [§521.151(a)], a person who fails to take reasonable action to comply with [the law] is liable to this state for a civil penalty of not more than \$100 for each individual</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Texas								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>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.” (§521.002(a)(2))</p> <p>Exception: “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.” (§521.002(b))</p>	<p>manner.” (§521.053(a))</p> <p>Risk of harm analysis: No, except as provided in the definition of a breach.</p>	Government notice requirement: No.		<p>(3) notice published in or broadcast on major statewide media.” (§521.053(f))</p> <p>Exception : “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 [§521.053(b)] to provide notice of a breach of system security, the notice of the breach of system security required under [§521.053(b)] may be provided under that state’s law or under [§521.053(b)].” (§521.053(b-1))</p>		<p>to whom notification is due under that subsection for each consecutive day that the person fails to take reasonable action to comply with that subsection. Civil penalties under this section may not exceed \$250,000 for all individuals to whom notification is due after a single breach. The attorney general may bring an action to recover the civil penalties imposed under this subsection.” (§521.151(a-1)) -- “In an action under this section, the court may grant any other equitable relief that the court considers appropriate to: (1) prevent any additional harm to a victim of identity theft or a further violation of this chapter; or (2) satisfy any</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Texas								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
								<p>judgment entered against the defendant, including issuing an order to appoint a receiver, sequester assets, correct a public or private record, or prevent the dissipation of a victim's assets." (§521.151(e))</p> <p>-- "The attorney general is entitled to recover reasonable expenses, including reasonable attorney's fees, court costs, and investigatory costs, incurred in obtaining injunctive relief or civil penalties, or both, under this section. Amounts collected by the attorney general under this section shall be deposited in the general revenue fund and may be appropriated only for the investigation and prosecution of other cases under this chapter." (§521.151(f))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Texas								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
								-- "The fees associated with an action under this section are the same as in a civil case, but the fees may be assessed only against the defendant." (§521.151(g)) Private right of action: No.

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Utah								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Utah Code 13-44-101 <i>et seq.</i>	<p>Covered entities: “A person who owns or licenses computerized data that includes personal information concerning a Utah resident.” (§13-44-202(1)(a))</p> <p>Service provider requirement: Yes. “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.” (§13-44-202(3)(a))</p>	<p>Personal information: “‘Personal information’ means a person’s first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable: (i) Social Security number; (ii) [F]inancial account number, or credit or debit card number [and] any required security code, access code, or password that would permit access to the person’s account; or (iii) [D]river license number or</p>	<p>Breach definition: “‘Breach of system security’ means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.” (§13-44-102(1)(a))</p> <p>Exception: A breach “does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner.” (§13-44-102(1)(b))</p> <p>Risk of harm analysis: Yes. “A person who owns or licenses</p>	<p>Residents: Affected Utah residents. (§13-44-202(1)(b))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: No.</p>	<p>Timing: Notice must be given “in the most expedient time possible without unreasonable delay: (a) considering legitimate investigative needs of law enforcement, as provided in [the law enforcement delay exception, described below]; (b) after determining the scope of the breach of system security; and (c) after restoring the reasonable integrity of the system.” (§13-44-202(2))</p> <p>Delay: (a) “[A] person may delay providing notification under [§13-44-202(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 . . . shall provide notification</p>	<p>Method: “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 [regulating publication and</p>	<p>For establishing own notification method: Yes. “If a person maintains the person’s own notification procedures as part of an information security policy for the treatment of personal information the person is considered to be in compliance with this chapter’s notification requirements if the procedures are otherwise consistent with this chapter’s timing requirements and the person notifies each affected Utah resident in accordance with the person’s information security policy in the event of a breach.” (§13-44-202(5)(b))</p> <p>For following interagency guidelines: Yes. “A person who is regulated by state</p>	<p>State enforcement: The Utah attorney general may seek an injunction against a violator, attorney fees and costs, and may also seek civil penalties: “(a) no greater than \$2,500 for a violation or series of violations concerning a specific consumer; and (b) no greater than \$100,000 in the aggregate for related violations concerning more than one consumer.” (§13-44-301(3))</p> <p>Private right of action: No. “Nothing in this chapter creates a private right of action [or] affects any private right of action existing under other law, including contract or tort.” (§13-44-301(2))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Utah								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>state identification card number.” (§13-44-102(3)(a))</p> <p>Exception: Personal information does not include “information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.” (§13-44-102(3)(b))</p>	<p>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 . . . [I]f an investigation . . . 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.” (§13-44-202(1)(a))</p>		<p>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.” (§13-44-202(4))</p>	<p>broadcasting].” (§13-44-202(5)(a))</p>	<p>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.” (§13-44-202(5)(c))</p>	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Vermont								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Vt. Stat. Ann. tit. 9, §2430 <i>et seq.</i>	<p>Covered entities: “[A]ny data collector* that owns or licenses computerized personal information that includes personal information concerning a consumer.” (§2435(b)(1))</p> <p>* Data collector “may include the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals</p>	<p>Personally identifiable information: “[A]n individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons: (i) Social Security number; (ii) Motor vehicle operator’s license number or nondriver identification card number; (iii) Financial account number or credit or debit card number, if circumstances exist in which the number could be used without</p>	<p>Breach definition: -- A “security breach” means “unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer’s personally identifiable information maintained by the data collector.” (§2430(8)(A))</p> <p>-- “In determining whether personally identifiable information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others: (i) indications that the information is in the physical</p>	<p>Consumers: “Consumers,” defined as Vermont residents. (§§2430(2), 2435(b)(1))</p> <p>Credit reporting agency notice requirement: Yes. If notice must be given to “more than 1,000 consumers at one time pursuant to [the law], the data collector shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice. This subsection shall not apply to a person who is licensed or registered under Title 8 by the department of banking, insurance, securities, and health care administration.” (§2435(c))</p>	<p>Timing: “Notice of the 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 [§2435(b)(3) and (4)], 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.” (§2435(b)(1))</p> <p>Delay: Delay is permitted “upon request of a law enforcement agency. A law enforcement agency may request the delay if it believes that notification may impede a law enforcement investigation, or a</p>	<p>Method: “For purposes of this subsection, notice to consumers may be provided by one of the following methods: (A) Direct notice to consumers, which may be by one of the following methods: (i) Written notice mailed to the consumer’s residence; (ii) Electronic notice, for those consumers for whom the data collector has a valid e-mail address if: (I) the data collector does not have contact information set forth in subdivisions (i) and (iii) of [§2435(b)(6)], the data collector’s primary method of communication with the consumer is by electronic means,</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: Yes. -- “[A] financial institution that is subject to the following guidances, and any revisions, additions, or substitutions relating to an interagency guidance shall be exempt from this section: (1) The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift</p>	<p>State enforcement: -- “[T]he Attorney General and state’s attorney shall have sole and full authority to investigate potential violations . . . and to enforce, prosecute, obtain, and impose remedies for [any] violation.” -- If the data collector is licensed or registered with the Department of Financial Regulation under Title 8, the Department shall have full authority. (§§2435(g)(1), (2))</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Vermont								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>with nonpublic personal information collector may include, but is not limited to, the state, state agencies, political subdivisions of the state, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.” (§2430(3))</p> <p>Service provider requirement: Yes. “Any data collector that</p>	<p>additional identifying information, access codes, or passwords; (iv) Account passwords or personal identification numbers or other access codes for a financial account.” (§2430(5)(A))</p> <p>Exception: Personally identifiable information “does not mean publicly available information that is lawfully made available to the general public from federal, state, or local government records.” (§2430(5)(B))</p>	<p>possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information; (ii) indications that the information has been downloaded or copied; (iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or (iv) that the information has been made public.” (§2430(8)(C))</p> <p>Exception: A security breach “does not include good faith but unauthorized acquisition or access of personal information by an employee or agent</p>	<p>Government notice requirement: Yes. 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 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.” -- “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</p>	<p>national or Homeland Security investigation or jeopardize public safety or national or Homeland Security interests. In the event law enforcement makes the request in a manner other than in writing, the data collector shall document such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The data collector shall provide notice required by this section without unreasonable delay upon receipt of a written communication, which includes facsimile or electronic communication, from the law enforcement agency withdrawing its request for delay.” (§2435(b)(4))</p>	<p>the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or (II) the notice provided is consistent with the provisions regarding electronic records and signatures for notices as set forth in 15 U.S.C. § 7001; or (iii) Telephonic notice, provided that telephonic contact is made directly with each affected consumer, and the telephonic contact is not</p>	<p>Supervision. (2) Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration.” -- The exemption does not apply to a “financial institution regulated by the Department of Financial Regulation.” (§2435(b)(f))</p>	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Vermont								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	maintains or possesses computerized data containing personal information of a consumer that the business does not own or license or any data collector that conducts business in Vermont that maintains or possesses records or data containing personal information that the data collector does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement.” (§2435(b)(2))		of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector’s business or subject to further unauthorized disclosure.” (§2430(8)(B)) Risk of harm analysis: Yes, subject to government notice requirement. -- Notice is “not required if the data collector establishes that misuse of personal information is not reasonably possible and the data collector provides notice of the determination that the misuse of the personal information is not reasonably possible pursuant to the requirements of this subsection.	breach within 14 business days, consistent with the legitimate needs of the law enforcement agency as provided in [§2435(b)(3) and (4)] 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.” -- Notwithstanding [the above] subdivision, 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		through a prerecorded message. (B) Substitute notice, if the data collector demonstrates that the cost of providing written or telephonic notice, pursuant to subdivision (A)(i) or (iii) of [§2435(b)(6)], to affected consumers would exceed \$5,000.00 or that the affected class of affected consumers to be provided written or telephonic notice, pursuant to subdivision (A)(i) or (iii) of [§2435(b)(6)], exceeds 5,000, or the data collector does not have sufficient contact information.” (§2435(b)(6)) Substitute notice: “Substitute notice shall consist of all of the following: (i) conspicuous		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Vermont								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			-- If the data collector establishes that misuse of the personal information is not reasonably possible, the data collector shall provide notice of its determination that misuse of the personal information is not reasonably possible and a detailed explanation for said determination to the Vermont attorney general or to the Department of Financial Regulation in the event that the data collector is a person or entity licensed or registered with the department under Title 8 or this title. The data collector may designate its notice and detailed explanation to the Vermont Attorney General or the Department of Financial Regulation as 'trade secret' if the notice and detailed	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 [§2435(b)(1)]." -- "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." -- "Unless otherwise ordered by a court of this State for good cause shown, a notice provided under this [section] 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		posting of the notice on the data collector's website page if the data collector maintains one; and (ii) notification to major statewide and regional media." (§2435(b)(6)(B)) Notice contents requirement: "The notice to a consumer shall be clear and conspicuous. The notice shall include a description of each of the following, if known to the data collector: (A) the incident in general terms; (B) the type of personally identifiable information that was subject to the security breach; (C) the general acts of the data collector to protect the personally identifiable information from further security breach;		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Vermont								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			<p>explanation meet the definition of trade secret contained in 1 V.S.A. § 317(c)(9).” -- “If a data collector established that misuse of personal information was not reasonably possible under [§2435(d)(2)] and subsequently obtains facts indicating that misuse of the personal information has occurred or is occurring, the data collector shall provide notice of the security breach pursuant to [the statute].” (§2435(d)(1))</p>	<p>enforcement officer engaged in legitimate law enforcement activities without the consent of the data collector.” (§2435(b)(3))</p> <p>Attorney General notice contents requirement: “When the data collector provides notice of the breach [to consumers], 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 consumersThe 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</p>		<p>(D) a telephone number, toll-free if available, that the consumer may call for further information and assistance; (E) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and (F) the approximate date of the security breach.” (§2435(b)(5))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Vermont								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
				<p>subject to the breach, and which the Attorney General or the Department shall use for any public disclosure of the breach.” (§2435(b)(3)(C))</p> <p>Vermont also recommends that a data collector inform either the Vermont state police or FBI of the breach in “the most expedient time possible and without unreasonable delay.” (Attorney General Security Breach Notification Guidance, July 26, 2012)</p>				

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Virginia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Va. Code §18.2-186.6	<p>Covered entities: “[A]n individual or entity* that owns or licenses computerized data that includes personal information.” (§18.2-186.6(B))</p> <p>* “‘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.” (§18.2-186.6(A))</p>	<p>Personal information: “[T]he first name or first initial and last name in combination 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</p>	<p>Breach definition: -- “‘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.” (§18.2-186.6(A))</p> <p>-- “An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and</p>	<p>Residents: “[T]he Office of the Attorney General and any affected resident of the Commonwealth.” (§18.2-186.6(B))</p> <p>Consumer credit reporting agency and government notice requirement: Yes. “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.” (§18.2-186.6(E))</p> <p>Breaches of payroll</p>	<p>Timing: “[F]ollowing discovery or notification of the breach of the security of the system” notice “to the Office of the Attorney General and any affected resident of the Commonwealth” must be made “without unreasonable delay.” (§18.2-186.6(B))</p> <p>Delay: Notice “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</p>	<p>Method: “‘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.” (§18.2-186.6(A))</p> <p>Substitute notice: “Substitute notice consists of all of the</p>	<p>For establishing own notification method: Yes. “An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information that are consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if it notifies residents of the Commonwealth in accordance with its procedures in the event of a breach of the security of the system.” (§18.2-186.6(F))</p> <p>For following interagency guidelines: Yes. -- “An entity that is subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et</p>	<p>State enforcement: “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.” (§18.2-186.6(I))</p> <p>-- “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.” (§18.2-186.6(J))</p> <p>-- “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.” (§18.2-186.6(K))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Virginia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	Service provider requirement: Yes. “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	accounts.” (§18.2-186.6(A)) Exception: Personal information “does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.” (§18.2-186.6(A))	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.” (§18.2-186.6(C)) Exception: “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	data: “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	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.” (§18.2-186.6(B))	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.” (§18.2-186.6(A)) Notice contents requirement: “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 or acquisition; (3) The general acts of the business to protect the personal	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.” (§18.2-186.6(G)) -- “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.” (§18.2-186.6(H))	Private right of action: Yes. “Nothing in this section shall limit an individual from recovering direct economic damages from a violation of this section.” (§18.2-186.6(I))

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Virginia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>accessed and acquired by an unauthorized person.” (§18.2-186.6(D))</p> <p>Note: Virginia has a separate provision that covers health information. Its application is limited only to government entities, which are defined as “any authority, board, bureau, commission, district or agency of the Commonwealth or of any political subdivision of the Commonwealth, including cities, towns and counties, municipal councils, governing bodies of counties, school boards and planning commissions; boards of visitors of public institutions of</p>		<p>disclosure.” (§18.2-186.6(A))</p> <p>Risk of harm analysis: Yes. Notice is required only if the breach “causes, or the individual or entity reasonably believes [it] has caused or will cause, identity theft or another fraud to any resident of the Commonwealth.” (§§18.2-186.6(A), (B))</p>	<p>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 ... 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</p>		<p>information from further unauthorized access or acquisition; (4) A telephone number that the consumer may call for further information and assistance, if one exists; and (5) Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.” (§18.2-186.6(A))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Virginia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	higher education; and other organizations, corporations, or agencies in VA supported wholly or principally by public funds.” (§32.1-127.1:05(A))			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.” (§18.2-186.6(M))				

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Virgin Islands (US)								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
14 V.I.C. §2208	<p>Covered entities: “Any agency that owns or licenses computerized data that includes personal information.” (§2208(a))</p> <p>Service provider requirement: Yes. “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.” (§2208(b))</p>	<p>Personal information: “[A]n individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number. (2) Driver’s license number. (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.” (§2208(e))</p> <p>Exception: Personal information does not include “publicly available information that is lawfully made available to the</p>	<p>Breach definition: A “‘breach of the security of the system’ means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency.” (§2208(d))</p> <p>Exception: “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.” (§2208(d))</p> <p>Risk of harm analysis: No.</p>	<p>Residents: To any “resident of the Virgin Islands whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” (§2208(a))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: No.</p>	<p>Timing: Notice must be given “in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in [§2208(c)], or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” (§2208(a))</p> <p>Delay: Notification 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.” (§2208(a))</p>	<p>Method: “[N]otice” 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.” (§2208(g))</p> <p>Substitute notice: “Substitute notice shall consist of all of the following:</p>	<p>For establishing own notification method: Yes. If an agency “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.” (§2208(h))</p> <p>For following interagency guidelines: No.</p>	<p>Local enforcement: “Any business that violates, proposes to violate, or has violated this title may be enjoined.” (§2211(b))</p> <p>Private right of action: Yes. “Any customer injured by a violation of this title may commence a civil action to recover damages.” (§2211(a))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Virgin Islands (US)								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		general public from federal, state, or territorial government records.” (§2208(f))				(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.” (§2208(g))		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Washington								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Was. Rev. Code. §19.255.010 <i>et seq.</i>	<p>Covered entities: “Any person or business that conducts business in [Washington] and that owns or licenses data that includes personal information.” (§19.255.010(1))</p> <p>Service provider requirement: Yes. “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.” (§19.255.010(2))</p>	<p>Personal information: “[A]n 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.” (§19.255.010(5))</p> <p>Exception: “[D]oes not include publicly available information that is lawfully made</p>	<p>Breach definition: A “[b]reach of the security of the system” is the “unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.” (§19.255.010(4))</p> <p>Exception: “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.” (§19.255.010(4))</p> <p>Risk of harm analysis: Yes. “Notice is not required if the</p>	<p>Residents: “[A]ny resident of [Washington] whose personal information was, or is reasonably believed to have been acquired by an unauthorized person and the personal information was not secured.”* (§19.255.010(1))</p> <p>* 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.” (§19.255.010(7))</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: Yes. “Any person or business that is required to issue a</p>	<p>Timing: Notification “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 [§19.255.010(3)], or due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” (§19.255.010(16))</p> <p>Delay: Delay is permitted “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</p>	<p>Method: “[N]otice” 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.” (§19.255.010(8))</p> <p>Substitute notice: “Substitute notice</p>	<p>For establishing own notification method: Yes. If a person or business “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,” then the person or business “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.” (§19.255.010(9))</p> <p>For following interagency guidelines: Yes. -- “A covered entity under the federal health insurance portability and accountability act of</p>	<p>State enforcement: “The attorney general may bring an action in the name of [Washington], or as parens patriae on behalf of persons residing in [Washington], to enforce this section.” (§19.255.010(17))</p> <p>Private right of action: Yes. “Any consumer injured by a violation of this section may institute a civil action to recover damages.” (§19.255.010(13)(a))</p> <p>“The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.” (§19.255.010(13)(c))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Washington								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		available to the general public from federal, state, or local government records.” (§19.255.010(6))	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.” (§19.255.010(1))	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.” (§19.255.010(15))	by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.” (§19.255.010(3))	shall consist of all of the following: (i) E-mail notice when the person or business has an e-mail address for the subject persons; (ii) Conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one; (iii) Notification to major statewide media.” (§19.255.010(8)(c)) Notice contents requirement: “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	1996, 42 U.S.C. Sec. 1320d et 5 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 the effective date of this section. 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 the effective date of this section,	Special liability for payment processors to financial institutions: “If a processor or business fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business or processor, and the failure is found to be the proximate cause of a breach, the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred by the financial institution to mitigate potential current or future damages to its credit card and debit card holders that reside in the state of Washington as a

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Washington								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>contact information of the reporting person or business subject to this section;</p> <p>(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; and</p> <p>(iii) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.”</p> <p>(§19.255.010(14))</p>	<p>notwithstanding the notification requirement in subsection (16) of this section.”</p> <p>(§19.255.010(10))</p> <p>-- “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 23 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part 24 364, Appendix</p>	<p>consequence of the breach, even if the financial institution has not suffered a physical injury in connection with the breach. In any legal action brought pursuant to this subsection, the prevailing party is entitled to recover its reasonable attorneys’ fees and costs incurred in connection with the legal action.”</p> <p>(§19.255.020)(3)(a))</p> <p>Special liability for vendors to financial institutions:</p> <p>“A vendor, instead of a processor or business, is liable to a financial institution for the damages . . . to the extent that the damages were proximately caused by the vendor’s negligence and if the claim is not limited or foreclosed by</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Washington								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
							B, and 12 C.F.R. Part 748, Appendices A and B, as they 25 existed on the effective date of this section, 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 the effective date of this section. The entity shall notify the attorney general pursuant to subsection (15) of this section in	another provision of law or by a contract to which the financial institution is a party.” (§19.255.020)(3)(b))

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Washington								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
							addition to providing notice to its primary federal regulator.” (§19.255.010(11))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

West Virginia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
W. Va. Code §46A-2A-101 <i>et seq.</i>	<p>Covered entities: “An individual or entity* that owns or licenses computerized data that includes personal information.” (§46A-2A-102(a))</p> <p>* “‘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.” (§46A-2A-101(2))</p> <p>Service provider requirement: Yes.</p>	<p>Personal information: A resident’s “first name or first initial and last name linked to any one or more of the following data elements . . . when the data elements are neither encrypted nor redacted: (A) Social security number; (B) Driver’s license number or state identification card number issued in lieu of a driver’s license; or (C) Financial account number, or credit card, or debit card number in combination with any required security code, access code or password that would permit access to a resident’s financial accounts.” (§46A-2A-101(6))</p>	<p>Breach definition: “‘Breach of the security of a system’ means the unauthorized access and acquisition of unencrypted* and unredacted** computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of this state.” (§46A-2A-101(1))</p> <p>“An individual or entity must give notice of the breach of the security of the system if</p>	<p>Residents: “[A]ny 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.” (§46A-2A-102(a))</p> <p>Credit reporting agency notice requirement: Yes. “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. [This requirement] does not apply to an entity who is subject to Title V of the Gramm</p>	<p>Timing: “[F]ollowing discovery or notification of the breach of the security of the system . . . the notice shall be made without unreasonable delay,” except where postponed by law enforcement or “in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.” (§46A-2A-102(a))</p> <p>Delay: Delay is permitted “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.” Notification “must be</p>	<p>Method: “‘Notice’ means: (A) Written notice to the postal address in the records of the individual or entity; (B) Telephonic notice; (C) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures, set forth in Section 7001, United States Code Title 15, Electronic Signatures in Global and National Commerce Act. (D) Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed fifty thousand dollars or that the affected class of residents to be notified exceeds one hundred thousand persons or that the individual</p>	<p>For establishing own notification method: Yes. “An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies residents of this state in accordance with its procedures in the event of a breach of security of the system.” (§46A-2A-103(a))</p> <p>For following interagency guidelines: Yes. -- “An entity that complies with the notification requirements or procedures pursuant</p>	<p>State enforcement: “[F]ailure to comply with the notice provisions of this article constitutes an unfair or deceptive act of practice . . . which may be enforced by the Attorney General pursuant to the enforcement provisions of this chapter.” (§46A-2A-104(a))</p> <p>Penalties: “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.” (§46A-2A-104(b))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

West Virginia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>“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.” (§46A-2A-102(c))</p>	<p>Exception: “[D]oes 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.” (§46A-2A-101(6))</p>	<p>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.” (§46A-2A-102(b))</p> <p>* “‘Encrypted’ means transformation of data through the use of an algorithmic process to into a form in 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 unreadable or unusable.”</p>	<p>Leach Bliley Act.” (§46A-2A-102(f))</p> <p>Government notice requirement: No.</p>	<p>made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.” (§46A-2A-102(e))</p>	<p>or the entity does not have sufficient contact information or to provide notice as described in paragraph (A), (B) or (C).” (§46A-2A-101(7))</p> <p>Substitute notice: “Substitute notice consists of any two of the following: (i) E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents; (ii) Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; or (iii) Notice to major statewide media.” (§46A-2A-101(7))</p> <p>Notice contents requirement: “The notice shall include: (1) To the extent possible, a</p>	<p>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-103(c)) -- “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.” (§46A-2A-103(b))</p>	<p>Private right of action: No. “A violation of this article by a licensed financial institution shall be enforceable exclusively by the financial institution’s primary functional regulator.” Otherwise, “the Attorney General shall have exclusive authority to bring action.” (§§46A-2A-104 (b), (c))</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

West Virginia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			<p>(§46A-2A-101(3))</p> <p>** “‘Redact’ means alteration or truncation of data 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 personal information.”</p> <p>(§46A-2A-101(8))</p> <p>Exception: “Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity</p>			<p>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;</p> <p>(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:</p> <p>(A) What types of information the entity maintained about that individual or about individuals in general;</p> <p>(B) Whether or not the entity maintained information about that individual;</p> <p>(3) The toll-free</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

West Virginia								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			<p>or subject to further unauthorized disclosure.” (§46A-2A-101(1))</p> <p>Risk of harm analysis: Yes. Notice is required only where “the individual or entity reasonably believes that [the breach] has caused or will cause identity theft or other fraud to any resident of this state.” (§§46A-2A-102(a), (b))</p>			<p>contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a fraud alert or security freeze.” (§46A-2A-102(d))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Wisconsin								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Wis. Stat. §134.98	<p>Covered entities: - “[A]n entity* whose principal place of business is located in [Wisconsin] or an entity that maintains or licenses personal information in [Wisconsin]” and that “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.” OR - “[A]n entity whose principal place of business is not located in [Wisconsin] and] knows that personal information pertaining to a resident of [Wisconsin] has been acquired by a person whom the entity has not authorized to</p>	<p>Personal information: “[A]n 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,</p>	<p>Breach definition: A breach is the “unauthorized acquisition of personal information pertaining to the subject of the personal information . . . [or] unauthorized acquisition of personal information pertaining to the resident of [Wisconsin] who is the subject of the personal information.” (§§134.98(2)(a), (b))</p> <p>Exception: Breach does not include personal information that is “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.” (§134.98(2)(cm) (2))</p>	<p>Requirement depends on entity’s connection to Wisconsin: “(a) If the entity’s principal place of business is located in Wisconsin or it maintains or licenses personal information in Wisconsin then ‘each subject of the personal information’ shall be given notice (b) If the entity’s principal place of business is outside Wisconsin then each resident of [Wisconsin] who is the subject of the personal information shall be given notice.” (§134.98(2))</p> <p>Credit agency reporting requirement: Yes. If an entity is required to notify “1,000 or more individuals that personal information pertaining to the individuals has been acquired, the entity shall without</p>	<p>Timing: Notice must be given “within a reasonable time, no to exceed 45 days after the entity learns of the acquisition of personal information.” A determination as to reasonableness of the time taken to provide notice “shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.” (§134.98(3)(a))</p> <p>Delay: “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 . . . for any period of time and the notification process required . . . shall begin at the end of that time period.”</p>	<p>Method: “[B]y mail or by a method the entity has previously employed to communicate with the subject of the personal information.” (§134.98(3)(b))</p> <p>Substitute notice: “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.” (§134.98(3)(b))</p> <p>“Upon written request by a person who has received a</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: Yes. Notification is not required for “[a]n 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 . . . [or] an entity that is described in 45 CFR 164.104 (a), if the entity complies with the requirements of 45 CFR part 164.” (§134.98(3)(m))</p>	<p>Enforcement: Not specified.</p> <p>Effect on civil claims: “Failure to comply with this [the breach law] is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.” (§134.98(4))</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Wisconsin								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>acquire the personal information.” (§134.98(2)(a))</p> <p>** An entity is “a person, other than an individual, that does any of the following:</p> <p>(a) Conducts business in [Wisconsin] and maintains personal information in the ordinary course of business.</p> <p>(b) Licenses personal information in [Wisconsin].</p> <p>(c) Maintains for a resident of [Wisconsin] a depository account [as defined in Section 815.18(2)(e).]</p> <p>(d) Lends money to a resident of [Wisconsin].” (§134.98(1)(a)(1))</p> <p>Service provider requirement: Yes. “If a person, other than an individual, that</p>	<p>access code, or password that would permit access to the individual’s financial account.</p> <p>(4) The individual’s deoxyribonucleic acid profile, as defined in s. 939.74(2d)(a) [i.e. an individual’s patterned chemical structure of genetic information identified by analyzing biological material that contains the individual’s deoxyribonucleic acid].</p> <p>(5) The individual’s unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.” (§134.98(1)(b))</p>	<p>Risk of harm analysis: Yes. Notice is not required if “[t]he acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.” (§134.98(2)(cm) (1))</p>	<p>unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis . . . of the timing, distribution, and content of the notices sent to the individuals.” (§134.98 (2)(br))</p> <p>Government notice requirement: No.</p>	(§134.98(5))	<p>notice under [the statute], the entity that provided the notice shall identify the personal information that was acquired.” (§134.98(3)(c))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Wisconsin								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	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							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Wisconsin								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	as practicable.” (§134.98(2)(bm))							

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Wyoming								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Wyoming Statutes 40-12-501 <i>et seq.</i>	<p>Covered entities: “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” (§40-12-502(a))</p> <p>Service provider requirement: Yes. “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</p>	<p>Personal identifying information: “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) [as listed below], when the data elements are not redacted.”* (§40-12-501(a) (vii))</p> <p>The listed data elements include: “(iii) Social security number; (iv) Driver’s license number; (v) Account number, credit card number or debit card number in combination with any security code, access code or password that would allow</p>	<p>Breach definition: “‘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 [Wyoming].” (§40-12-501(a)(i))</p> <p>Exception: “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</p>	<p>Residents: The affected Wyoming resident. (§40-12-502(a)).</p> <p>Credit reporting agency notice requirement: No.</p> <p>Government notice requirement: No.</p>	<p>Timing: “[W]hen [an entity] becomes aware of a breach of the security of the system, [it shall] 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</p>	<p>Method: “[N]otice 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 \$10,000 for Wyoming-based persons or businesses, and \$250,000 for all other businesses operating but not based in Wyoming; (B) that the affected class of subject persons to be notified exceeds 10,000 for Wyoming-based persons or businesses and 500,000 for all other businesses operating but not based in Wyoming; or (C) the person</p>	<p>For establishing own notification method: No.</p> <p>For following interagency guidelines: Yes. “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.” (§40-12-502(c))</p>	<p>State enforcement: “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 of 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.” (§40-12-502(f))</p> <p>Private right of action: No.</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Wyoming								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	personal identifying information was, or is reasonably believed to have been acquired by an unauthorized person.” (§40-12-502(g))	access to a financial account of the person; (vi) Tribal identification card; (vii) Federal or state government issued identification card; (viii) Shared secrets or security tokens that are known to be used for data based authentication; (ix) A username or email address, in combination with a password or security question and answer that would permit access to an online account; (x) A birth or marriage certificate; (xi) Medical information, meaning a person’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;	used or subject to further unauthorized disclosure.” (§40-12-501(a)(i)) Risk of harm analysis: Yes. “[Notice is required only] if the investigation determines that the misuse of personal identifying information about a Wyoming resident has occurred or is reasonably likely to occur.” (§40-12-502(a))		to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.” (§40-12-502(a)) Delay: “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.” (§40-12-502(b))	does not have sufficient contact information.” (§40-12-502(d)) Substitute notice: * “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, World Wide Web or a similar proprietary or common carrier electronic system site; and (B) Notification to major statewide media, including a toll-free phone number where an individual can learn whether or not that individual’s personal data is included in the security breach.” (§40-12-502(d))	“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.” (§40-12-502(h))	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Wyoming								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>(xii) Health insurance information, meaning a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person or information related to a person's application and claims history;</p> <p>(xiii) Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes;</p> <p>(xiv) An individual taxpayer identification number."</p> <p>(§6-3-901(b))</p> <p>* "'Redact' means alteration or</p>				<p>Notice contents requirement:</p> <p>"[Notice] shall be clear and conspicuous and shall include, at a minimum:</p> <p>(i) A toll-free number:</p> <p>(A) that the individual may use to contact the person collecting the date, or his agent; and</p> <p>(B) from which the individual may learn the toll free contact telephone numbers and addresses for the major credit reporting agencies.</p> <p>(ii) The types of personal identifying information that were or are reasonably believed to have been the subject of the breach;</p> <p>(iii) A general description of the breach incident;</p> <p>(iv) The approximate date of</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Wyoming								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		<p>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 [§40-12-501(a)] are accessible as part of the personal information.” (§40-12-501(a) (viii))</p> <p>Exception: “Personal identifying information 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.” (§40-12-501(b))</p>				<p>the breach of security, if that information is reasonably possible to determine at the time notice is provided;</p> <p>(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;</p> <p>(vi) Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports;</p> <p>(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. (§40-12-502(e))</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Wyoming								
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						<p>* Note: The Wyoming Act includes some internal inconsistencies regarding the definition of “substitute notice.” The requirements described in the text above are outlined in the section of the Act that specifically addresses data breach notifications. Section 40-12-501, which lists the definitions of terms “[a]s used in this act,” provides a different definition of “substitute notice.” Under this definition, “substitute notice” means:</p> <p>(A) email notice when the business has an email address for the affected person;</p> <p>(B) conspicuous posting on the business’s website; and</p> <p>(C) publication in local or statewide media.</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Gramm-Leach-Bliley Act (GLBA)								
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial institutions provide the disclosure? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
15 U.S.C. § 6801, <i>et seq.</i>	<p>Covered entities: “[F]inancial institution[s].” (§ 6801(a))</p> <p>Relevant financial institutions include: “(A) national banks, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers); (B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign</p>	<p>Nonpublic personal information: “[P]ersonally identifiable financial information-- (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.” (§6809(4))</p> <p>Exception: “Nonpublic personal information does not include publicly available information.” (§6809(4)(B))</p>	<p>“[A] financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice.” (§6802(a))</p> <p>Opt out exception: “(1) A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless - (A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the regulations prescribed under</p>	<p>Consumers: “[Any] individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.” (§6809(9))</p>	<p>Timing: “[Disclosure must be given] at the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship....” (§6803(a))</p>	<p>“[A covered] financial institution shall provide a clear and conspicuous disclosure to such consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 6804 of this title, of such financial institution’s policies with respect to- (1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with section 6802 of this title, including the categories of information that may be disclosed; (2) disclosing nonpublic personal information of persons who have ceased to be</p>	<p>Model forms safe harbor: “Any financial institution that elects to provide the model form developed by the agencies [referred to in section 6804 (a)(1)] shall be deemed to be in compliance with the disclosures required under this section.” (§6803(e))</p>	<p>State and Federal enforcement: “(a) In General. Subject to subtitle B of the Consumer Financial Protection Act of 2010 [12 U.S.C. 5511 <i>et seq.</i>], this subchapter and the regulations prescribed thereunder shall be enforced by the Bureau of Consumer Financial Protection, the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission with respect to financial institutions and other persons subject to their jurisdiction under applicable law, as follows: (1) Under section 1818 of Title 12, by the appropriate Federal banking agency, as defined</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Gramm-Leach-Bliley Act (GLBA)								
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial institutions provide the disclosure? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act [12 U.S.C.A. § 601 <i>et seq.</i> or 611 <i>et seq.</i>], and bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers); (C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System), insured State branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons		[15 U.S.C. §6804] that such information may be disclosed to such third party; (B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and (C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option. (2) This subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including marketing			customers of the financial institution; and (3) protecting the nonpublic personal information of consumers.” (§6803(a)) Information to be included: “(1) the policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third parties, other than agents of the institution, consistent with section 6802 of this title, and including (A) the categories of persons to whom the information is or may be disclosed, other than the persons to whom the information may be provided pursuant to [the general exceptions		in section 1813(q) of Title 12, in the case of-- (A) national banks, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers); (B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Gramm-Leach-Bliley Act (GLBA)								
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial institutions provide the disclosure? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	providing insurance, investment companies, and investment advisers); and (D) savings associations the deposits of which are insured by the Federal Deposit Insurance Corporation, and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).” (§6805(a))		of the financial institution’s own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 6804 of this title, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.” (§6802(b)) Limitations on the sharing of account number			in] section 6802(e) of this title; and (B) the policies and practices of the institution with respect to disclosing of nonpublic personal information of persons who have ceased to be customers of the financial institution; (2) the categories of nonpublic personal information that are collected by the financial institution; (3) the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information in accordance with section 6801 of this title; and (4) the disclosures required, if any, under section 1681a(d)(2)(A)(iii) of this title.” (§6803(c))		owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act [12 U.S.C.A. § 601 et seq. or 611 et seq.], and bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers); (C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System), insured State branches of foreign banks, and any

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Gramm-Leach-Bliley Act (GLBA)								
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial institutions provide the disclosure? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			<p>information for marketing purposes: “A financial institution shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.” (§6802(d))</p> <p>General exceptions: “[Disclosure of nonpublic personal information is permitted]: (1) as necessary to effect, administer, or enforce a transaction</p>					<p>subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers); and (D) savings associations the deposits of which are insured by the Federal Deposit Insurance Corporation, and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies, and investment advisers). (2) Under the Federal Credit Union Act [12 U.S.C.A. § 1751 et seq.], by the Board of the National Credit</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Gramm-Leach-Bliley Act (GLBA)								
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial institutions provide the disclosure? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			requested or authorized by the consumer, or in connection with— (A) servicing or processing a financial product or service requested or authorized by the consumer; (B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or (C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;					Union administration with respect to any federally insured credit union, and any subsidiaries of such an entity. (3) Under the Securities Exchange Act of 1934 [15 U.S.C.A. § 78a et seq.], by the Securities and Exchange Commission with respect to any broker or dealer. (4) Under the Investment Company Act of 1940 [15 U.S.C.A. § 80a-1 et seq.], by the Securities and Exchange Commission with respect to investment companies. (5) Under the Investment Advisers Act of 1940 [15 U.S.C.A. § 80b-1 et seq.], by the Securities and Exchange Commission with

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Gramm-Leach-Bliley Act (GLBA)								
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial institutions provide the disclosure? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			(2) with the consent or at the direction of the consumer; (3) (A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein; (B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (C) for required institutional risk control, or for resolving customer disputes or inquiries; (D) to persons holding a legal or beneficial interest relating to the consumer; or (E) to persons acting in a					respect to investment advisers registered with the Commission under such Act. (6) Under State insurance law, in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled, subject to section 6701 of this title. (7) Under the Federal Trade Commission Act [15 U.S.C.A. § 41 et seq.], by the Federal Trade Commission for any other financial institution or other person that is not subject to the jurisdiction of any agency or authority under paragraphs (1) through (6) of this

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Gramm-Leach-Bliley Act (GLBA)								
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial institutions provide the disclosure? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			<p>fiduciary or representative capacity on behalf of the consumer;</p> <p>(4) to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors;</p> <p>(5) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 [12 U.S.C. 3401 <i>et seq.</i>], to law enforcement agencies (including</p>					<p>subsection.</p> <p>(8) Under subtitle E of the Consumer Financial Protection Act of 2010, by the Bureau of Consumer Financial Protection, in the case of any financial institution and other covered person or service provider that is subject to the jurisdiction of the Bureau and any person subject to this subchapter, but not with respect to the standards under section 6801 of this title.</p> <p>(b) Enforcement of section 6801.</p> <p>(1) In general. Except as provided in paragraph (2), the agencies and authorities described in subsection (a),</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Gramm-Leach-Bliley Act (GLBA)								
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial institutions provide the disclosure? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			the Bureau of Consumer Financial Protection, a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, and chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951–1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety; (6) (A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act [15 U.S.C. 1681 <i>et seq.</i>], or (B) from a consumer report reported by a consumer reporting agency;					other than the Bureau of Consumer Financial Protection, of this section shall implement the standards prescribed under section 6801 (b) of this title in the same manner, to the extent practicable, as standards prescribed pursuant to section 1831p–1 (a) of title 12 are implemented pursuant to such section. (2) Exception. The agencies and authorities described in paragraphs (3), (4), (5), (6), and (7) of subsection (a) of this section shall implement the standards prescribed under section 6801 (b) of this title by rule with respect to the

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Gramm-Leach-Bliley Act (GLBA)								
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial institutions provide the disclosure? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			(7) in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or (8) to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for					financial institutions and other persons subject to their respective jurisdictions under subsection (a) of this section.” (§6805) Private right of action: No.

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Gramm-Leach-Bliley Act (GLBA)								
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial institutions provide the disclosure? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			examination, compliance, or other purposes as authorized by law.” (§6802(e))					

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Health Insurance Portability and Accountability Act of 1996 (HIPAA)								
Federal Statute	What entities are covered?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
45 CFR §§ 160.103, 164.400-414, 42 USC §1320d, <i>et seq.</i>	<p>Covered entities: “Covered entity means: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA.” (§160.103)</p> <p>Business associate notice requirement: “(1) A business associate* shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach. (2) For purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such</p>	<p>Protected health information: ““Protected health information”* means individually identifiable health information:** (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C.</p>	<p>Breach definition: “Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part [§164.500] which compromises the security or privacy of the protected health information.” (§164.402)</p> <p>Exception: “Breach excludes: (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not</p>	<p>Notice must be given to: - “[E]ach individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of [a] breach.” (§164.404(a)(1))</p> <p>Government notice requirement: Yes. “(a) <i>Standard:</i> A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary [of Health and Human Services]. (b) <i>Implementation specifications: Breaches involving 500 or more individuals:</i> For breaches of unsecured protected health information involving 500 or more individuals, a</p>	<p>Timing: “[A] covered entity shall provide the required notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.” (§164.404(b))</p> <p>Discovery: “[A] breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law</p>	<p>Method: “(1) <i>Written notice.</i> (i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available. (ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of</p>	<p>Safe harbor for encryption/ destruction of data: Yes. -- “<i>Unsecured protected health information</i> means protected health information that is not rendered unusable, unreadable, or indecipherable* to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5 on the HHS website.” (§164.402) -- “Protected health information (PHI) is rendered unusable, unreadable, or indecipherable . . . only if one or more of the following applies: (a) Electronic PHI has been encrypted as specified in the HIPAA Security Rule by the use</p>	<p>Federal enforcement: Penalties imposed by HHS Secretary. “(A) if it is established that the person did not know (and by exercising reasonable diligence would not have known) that such person committed a violation, they will be fined at least \$100 per violation, but not more than \$1.5 million total. (B) in the case of a violation of such provision in which it is established that the violation was due to reasonable cause and not to willful neglect, they will be fined at least \$1,000 per violation, but not more than \$1.5 million total. (C) in the case of a violation of such provision in which it is established that the violation was due to willful neglect— (i) if the violation is corrected as</p>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Health Insurance Portability and Accountability Act of 1996 (HIPAA)								
Federal Statute	What entities are covered?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).” (§164.410(a)) * Business associate: “(1) Except as provided in paragraph (2) of this definition, business associate	1232g (a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer”. (§160.103) * Health information: “Health information means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the	permitted under subpart E [§164.500] of this part; (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E [§164.500] of this part; (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an	covered entity shall provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS Web site. (c) Implementation specifications: For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.” (§164.408)	of agency).” (§164.404(a)(2)) Delay for law enforcement: “If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the	the individual. The notification may be provided in one or more mailings as information is available. (2) <i>Substitute notice.</i> In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii). (i) In the case in which there is insufficient or out-of-date contact	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 and such confidential process or key that might enable decryption has not been breached. Encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard. (i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800–111, <i>Guide to Storage Encryption Technologies for End User Devices</i> . (ii) Valid encryption	described in subsection (b)(3)(A), a penalty in an amount that is at least the amount described in paragraph (3)(C) but not to exceed the amount described in paragraph (3)(D); and (ii) if the violation is not corrected as described in such subsection, a penalty in an amount that is at least the amount described in paragraph (3)(D).” (42 U.S.C. §1320d–5(a)(1)) Private right of action: No. However, at least one state supreme court has held that the HIPAA can provide the standard of care for common law negligence claims against health care providers and does not preempt these claims. <i>See Byrne v. Avery Ctr. for</i>

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Health Insurance Portability and Accountability Act of 1996 (HIPAA)								
Federal Statute	What entities are covered?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of: (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration,	past, present, or future payment for the provision of health care to an individual.” (§160.103) Individual identifiable health information: “Individual identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for	unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.” (§164.402)(1)) Risk of harm analysis: Yes. “Except as provided [above], an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E [§164.500] is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the protected health information		oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.” (§164.412)	information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means. (ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) Include a toll-free phone	processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140–2. These include, as appropriate, standards described in NIST Special Publications 800–52, <i>Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations</i> ; 800–77, <i>Guide to IPsec VPNs</i> ; or 800–113, <i>Guide to SSL VPNs</i> , and may include others which are FIPS 140–2 validated. (b) The media on which the PHI is stored or recorded has been destroyed in one of the following ways: (i) Paper, film, or other hard copy	<i>Obstetrics & Gynecology, P.C.</i> , 314 Conn. 433 (2014).

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Health Insurance Portability and Accountability Act of 1996 (HIPAA)								
Federal Statute	What entities are covered?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by this subchapter; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity	the provision of health care to an individual; and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.” (§160.103)	involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the protected health information or to whom the disclosure was made; (iii) Whether the protected health information was actually acquired or viewed; and (iv) The extent to which the risk to the protected health information has been mitigated.” (§164.402)(2))			number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach. (3) Additional notice in urgent situations. In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.” (§164.404)(d)) Notice contents requirement: “(A) A brief description of what happened, including	media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. (ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, <i>Guidelines for Media Sanitization</i> , such that the PHI cannot be retrieved.” 74 Fed. Reg. 19009 (April 27, 2009) (as amended by 78 Fed. Red. 5695 (Jan. 25, 2013)); <i>see also</i> http://www.csrc.nist.gov	

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Health Insurance Portability and Accountability Act of 1996 (HIPAA)								
Federal Statute	What entities are covered?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<p>participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.</p> <p>(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health</p>					<p>the date of the breach and the date of the discovery of the breach, if known;</p> <p>(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);</p> <p>(C) Any steps individuals should take to protect themselves from potential harm resulting from the breach;</p> <p>(D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and</p> <p>(E) Contact procedures for</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Health Insurance Portability and Accountability Act of 1996 (HIPAA)								
Federal Statute	What entities are covered?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement. (3) A covered entity may be a business associate of another covered entity.” (§160.103)					<p>individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.” (§164.404(c)(1))</p> <p>Plain language requirement: The notification shall be written in “plain language.” (§164.404(c)(2))</p> <p>Notification to the Media: “(a) <i>Standard.</i> For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction. (b) <i>Implementation specification:</i> <i>Timeliness of notification.</i> Except</p>		

Comparison of US State and Federal Security Breach Notification Laws – Current through September 1, 2017

Health Insurance Portability and Accountability Act of 1996 (HIPAA)								
Federal Statute	What entities are covered?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
						as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. (c) <i>Implementation specifications: Content of notification.</i> The notification required by paragraph (a) of this section shall meet the requirements of §164.404(c).” (§164.406)		

Please note that this summary is intended only to provide an overview of the various notification laws and does not constitute legal advice. In addition, the requirements of these laws can differ significantly, and they are subject to change over time. If you have questions about the possible application of any of these laws, please contact a Steptoe lawyer.