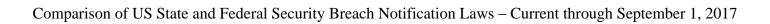


# **Comparison of US State and Federal Security Breach Notification Laws**

Current through September 1, 2017

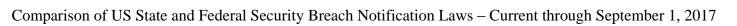
Alaska2
Arizona6
Arkansas9
California
Colorado
Connecticut
Delaware
District of Columbia
Florida
Georgia37
Guam
Hawaii
Idaho
Illinois
Indiana 55
Iowa
Kansas
Kentucky
Louisiana65
Maine
Maryland
Massachusetts
Michigan 80
Minnesota85
Mississippi
Missouri
Montana
Nebraska
Nevada101

New Hampshire105
New Jersey 108
New Mexico
New York 116
North Carolina120
North Dakota124
Ohio128
Oklahoma
Oregon136
Pennsylvania
Puerto Rico144
Rhode Island147
South Carolina151
Tennessee
Texas
Utah160
Vermont
Virginia 168
Virgin Islands (US)
Washington174
West Virginia179
Wisconsin
Wyoming187
Gramm-Leach-Bliley Act (GLBA)192
Health Insurance Portability and Accountability Act of 1996 (HIPAA)202





	Alaska										
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?			
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is			
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private			
	requirement for		analysis?			available?		right of action?			
	service		-								
	providers?										
Alaska	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:			
Stat. §45.48.010	A "covered	information:	A "breach of the	"[E]ach state resident	"An information	"An information	own notification	"If an information			
et seq.	person" who	"[I]nformation in	security" means	whose personal	collector shall make	collector shall make	method: No.	collector			
	"owns or licenses	any form on an	"unauthorized	information was	the disclosure	the disclosure		violates AS			
	personal	individual that is	acquisition, or	subject to the	required by this	required by AS	For following	45.48.010 -			
	information in any	not encrypted or	reasonable belief of	breach."	section in the most	45.48.010	interagency	45.48.090 with			
	form that includes	redacted, or is	unauthorized	(§45.48.010(a))	expeditious time	(1) by a written	guidelines: No.	regard to the			
	personal	encrypted and the	acquisition, of	C 1'4	possible and without	document sent to		personal			
	information on a state resident."	encryption key has	personal	Credit reporting	unreasonable delay,	the most recent address the		information of a			
	(§45.48.010(a))	been accessed or acquired, and that	information that compromises the	agency notice requirement: Yes.	except as [requested by law enforcement]	information		state resident, the violation is an			
	(§45.46.010(a))	consists of a	security,	"(a) If an information	and as necessary to	collector has for the		unfair or deceptive			
	"Covered person"	combination of:	confidentiality, or	collector is required	determine the scope	state resident;		act or practice under			
	is defined as "a	(A) an individual's	integrity of the	to notify more	of the breach and	(2) by electronic		AS 45.50.471 -			
	(A) person doing	name; in this	personal	than 1,000 state	restore the reasonable	means if the		45.50.561.			
	business;	subparagraph,	information	residents of a breach,	integrity of the	information		However the			
	(B) governmental	'individual's	maintained by the	the information	information system."	collector's primary		information			
	agency; or	name' means a	information	collector shall also	(§45.48.010(b))	method of		collector is not			
	(C) person with	combination of an	collector."	notify without		communication with		subject to the civil			
	more than 10	individual's	(§45.48.090(1))	unreasonable delay	Delay:	the state resident is		penalties imposed			
	employees."	(i) first name or		all consumer credit	"An information	by electronic means		under AS 45.50.551			
	(§45.48.090(2))	first initial; and	"Acquisition"	reporting agencies	collector may delay	or if making the		but is liable to the			
		(ii) last name;	includes acquisition	that compile and	disclosing the breach	disclosure by the		state for a civil			
	Service provider	and	by:	maintain files on	if an appropriate	electronic means is		penalty of up to			
	requirement:	(B) one or more of	"(A) photocopying,	consumers on a	law enforcement	consistent with the		\$500 for each state			
	Yes. "If a breach of the security of	the following information	facsimile, or other paper-based	nationwide basis and	agency determines that disclosing the	provisions regarding electronic records		resident who was not notified under			
	the information	elements:	method;	provide the agencies with the timing,	breach will interfere	and signatures		AS 45.48.010 -			
	system containing	(i) social	(B) a device,	distribution, and	with a criminal	required for notices		45.48.090, except			
	personal	security number;	including a	content of the notices	investigation.	legally required to		that the total civil			
	information on a	(ii) driver's	computer, that can	to state residents.	However, the	be in writing under		penalty may not			
	state resident that	license or state	read, write, or store	(b) This section may	information collector	15 U.S.C. 7001 et		exceed \$50,000."			
	is maintained by	ID card number;	information that is	not be construed to	shall disclose the	seq. (Electronic		(§45.48.080(b)(1))			
	an information	(iii) the	represented in	require the	breach to the state	Signatures in Global		(0 1 1 1 1 1 (1 ) (1 ) (1 )			
	recipient occurs,	Individual's	numerical form; or	information collector	resident in the most	and National		Private right of			
	the information	account number,	(C) a method not	to provide the	expeditious time	Commerce Act); or		action: Yes.			
	recipient is not	credit card	identified by (A) or	consumer reporting	possible and without	(3) if the		Alaska residents			





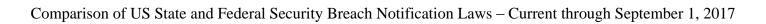
				Alaska				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?			available?		right of action?
	service							
	providers?							
	required to comply	number, or debit	(B)."	agencies identified	unreasonable delay	information		injured by such
	with [the law's	card number, if	(§45.48.090(1))	under (a) of this	after the law	collector		violations may seek
	requirement to	no access code,		section with the	enforcement agency	demonstrates that		relief under AS
	notify state	personal	"'Information	names or other	informs the	the cost of		45.50.471 -
	residents].	identification	collector' means a	personal information	information collector	providing notice		45.50.56. However,
	However,	number, or	covered person who	of the state residents	in writing that	would exceed		"damages that may
	immediately after	password is	owns or licenses	whose personal	disclosure of the	\$150,000, that the		be awarded against
	the information	required to	personal	information was	breach will no longer	affected class of		the information
	recipient discovers	access the	information in any	subject to the breach.	interfere with the	state residents to be		collector under
	the breach, the	account;	form if the personal	(c) This section does	investigation."	notified exceeds		(A) AS 45.50.531
	information	(iv) the	information	not apply to an	(§45.48.020)	300,000, or that the		are limited to
	recipient shall	Individual's	includes personal	information collector		information		actual economic
	notify the information	account number,	information on a state resident."	who is subject to the Gramm-Leach-Bliley		collector does not have sufficient		damages that do
	distributor who	credit card number, or debit	(45.48.090(4))	Financial		contact information		not exceed \$500;
	owns the personal	card number in	(43.48.090(4))	Modernization Act.		to provide notice,		and (B) AS 45.50.537
	information or	combination with	Exception:	(d) In this section,		by		are limited to
	who licensed the	an access code, a	"[T]he good faith	'consumer credit		(A) electronic mail		actual economic
	use of the personal	personal	acquisition of	reporting agency that		if the information		damages."
	information to the	identification	personal	compiles and		collector has an		(§45.48.080(b))
	information	number, or a	information by an	maintains files on		electronic mail		(3.61.6.666(6))
	recipient about the	password	employee or agent	consumers on a		address for the		
	breach and	required to	of an information	nationwide basis' has		state resident;		
	cooperate with the	access the	collector for a	the meaning given to		(B) conspicuously		
	information	account; or	legitimate purpose	'consumer reporting		posting the		
	distributor as	(v) passwords,	of the information	agency that compiles		disclosure on the		
	necessary to allow	personal ID	collector is not a	and maintains files on		Internet website of		
	the information	numbers, or other	breach of the	consumers on a		the information		
	distributor to	access codes for	security of the	nationwide basis' in		collector if the		
	comply with	financial	information system	15 U.S.C. 1681a(p)."		information		
	this section."	accounts."	if the employee or	(§45.48.040)		collector maintains		
	(§45.48.070(a))	(§45.48.090(7))	agent does not use			an Internet		
	(((50)		the personal	Government notice		website; and		
	"'[C]ooperate'		information for a	requirement:		(C) providing a		
	means sharing		purpose unrelated to	Possibly. The section		notice to major		
	with the		a legitimate purpose	of the law describing		statewide media."		
	information		of the information	the risk of harm		(§45.48.030)		
	distributor		collector and does	analysis could be				



				Alaska				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?		•	available?		right of action?
	service		J					8
	providers?							
	information		not make further	read as suggesting				
	relevant to the		unauthorized	that the state attorney				
	breach, except		disclosure of the	general must be				
	for confidential		personal	notified whenever				
	business		information."	there is a breach:				
	information or		(§45.48.050)	"[D]isclosure is not				
	trade secrets."			required if, after an				
	(§45.48.070(a))		Risk of harm	appropriate				
			analysis: Yes.	investigation and				
	"[I]f an		"[D]isclosure is not	after written				
	information		required if, after an	notification to the				
	recipient notifies		appropriate	attorney general of				
	an information		investigation and	this state, the covered				
	distributor of a		after written	person determines				
	breach under (a) of		notification to the	that there is not a				
	this section, the		attorney general of	reasonable likelihood				
	information		this state, the	that harm to the				
	distributor shall		covered person	consumers whose				
	comply with [the		determines that	personal information				
	law's requirement		there is not a reasonable	has been acquired has resulted or will result				
	to notify state residents] as if the		likelihood that harm	from the breach				
	breach occurred to		to the consumers	The notification				
	the information		whose personal	required by this				
	system maintained		information has	subsection shall not				
	by the information		been acquired has	be considered a				
	distributor."		resulted or will	public record open to				
	(§45.48.070(b))		result from the	inspection by the				
	(3.27.0.070(0))		breach. The	public." Because the				
			determination shall	section says that the				
			be documented in	determination about				
			writing and the	whether to notify				
			documentation shall	consumers should be				
			be maintained for	made after				
			five years. The	notification to the				
			notification required	state Attorney				
			by this subsection	General, it could be				
			shall not be	read as meaning that				

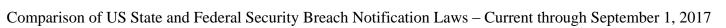


				Alaska				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	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)).				





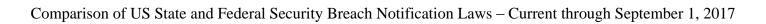
				Arizona				
State Statute	What entities are covered? Is there a	What data are covered?	Has there been a breach? Is there a risk of harm	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private
	requirement for service providers?		analysis?			available?		right of action?
Ariz. Rev. Stat. Ann. §18-545	Covered entities: "[A] person that conducts business in [Arizona] and that owns or licenses unencrypted computerized data that includes personal information." (§18-545(A))  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	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	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))  Exception: "Good faith acquisition of personal information by an employee or	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))  Credit reporting agency notice requirement: No.  Government notice requirement: No.	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))  Delay: "The notification required by [§18- 545(A)] may be delayed if a law enforcement agency advises the person that the notification	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	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))  For following interagency guidelines: Yes.	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))  Private right of action: No. The law "may only be enforced by the attorney general." (§18-545(H))
	unreasonable delay." (§18-545(B))	individual's financial account number or credit or debit card number	agent of the person for the purposes of the person is not a breach of the		will impede a criminal investigation." (§18-545(C))	notice pursuant to paragraph 1, 2 or 3 of this subsection would exceed fifty	"A person that complies with the notification requirements or	





				Arizona				
State Statute	What entities are covered? Is there a	What data are covered?	Has there been a breach? Is there a risk of harm	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private
	requirement for		analysis?			available?		right of action?
	service							
	providers?							
		in combination	security system if			thousand dollars or	security breach	
		with any required	the personal			that the affected	procedures pursuant	
		security code,	information is not			class of subject	to the rules,	
		access code or	used for a purpose			individuals to be	regulations,	
		password that	unrelated to the			notified exceeds one	procedures,	
		would permit	person or subject to			hundred thousand	guidance or	
		access to the	further wilful [sic]			persons, or the	guidelines	
		individual's financial account."	unauthorized disclosure."			person does not have sufficient	established by the	
		(§18-545(L)(6)	(§18-545(L)(1))				person's primary or functional federal	
		(§18-343(L)(6) (a))	(§16-343(L)(1))			contact information."	regulator is deemed	
		(a))	Risk of harm			(§18-545(D))	to be in compliance	
		Exception:	analysis: Yes.			(\$16-343(D))	with this section."	
		Personal	"A person is not			Substitute notice:	(§18-545(F))	
		information does	required to disclose			"Substitute notice	"This section	
		not include	a breach of the			shall consist of all of	[also] does not apply	
		"publicly available	security of the			the following:	to either of the	
		information that is	system if the person			(a) Electronic mail	following:	
		lawfully made	or a law			notice if the person	1. A person subject	
		available to the	enforcement agency,			has electronic mail	to title V of the	
		general public	after a reasonable			addresses for the	Gramm-Leach-	
		from federal, state	investigation,			individuals subject	Bliley act of 1999	
		or local	determines that a			to the notice.	(P.L. 106-102; 113	
		government	breach of the			(b) Conspicuous	Stat. 1338; 15	
		records or widely	security of the			posting of the notice	United States Code	
		distributed media."	system has not			on the web site of	sections 6801	
		(§18-545(L)(6)	occurred or is not			the person if the	through 6809).	
		(b))	reasonably likely to			person maintains	<ol><li>Covered entities</li></ol>	
			occur."			one.	as defined under	
			(§18-545(G))			(c) Notification to	regulations	
			A breach occurs			major statewide	implementing the	
			only if the security			media."	health insurance	
			or confidentiality of			(§18-545(D)(4))	portability and	
			an individual's				accountability act,	
			personal information				45 Code of Federal	
			is materially compromised and if				Regulations section 160.103 (1996)."	
			the event "causes or				(§18-545(J))	
			the event causes of				(810-343(J))	

				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))					

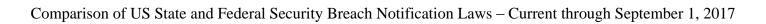




				Arkansas				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be	substitute notice	safe harbor?	there a private
	requirement		analysis?		delayed?	available?		right of action?
	for service		J			***************************************		<del>_</del>
	providers?							
Ark. Code Ann.	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:
§4-110-101 et	"Any person or	information:	A "[b]reach of the	"[A]ny resident of	"[D]isclosure shall	"[N]otice may be	own notification	"Any violation of
seq.	business that	"[A]n individual's	security of the	Arkansas whose	be made in the most	provided by one (1)	method: Yes.	this chapter is
seq.	acquires, owns, or	first name or first	system" is the	unencrypted personal	expedient time and	of the following	If a person or	punishable by
	licenses	initial and his or	"unauthorized	information was, or	manner possible and	methods	business "maintains	action of the
	computerized data	her last name in	acquisition of	is reasonably	without unreasonable	(1) Written notice;	its own notification	Attorney General
	that includes	combination with	computerized data	believed to have	delay, consistent	(2) Electronic mail	procedures as part	under the
	personal	any one (1) or	that compromises	been, acquired by an	with the legitimate	notice if the notice	of an information	provisions of Ark.
	information" of	more of the	the security,	unauthorized	needs of law	provided is	security policy for	Code Ann. § 4-88-
	Arkansas	following data	confidentiality, or	person."	enforcement as	consistent with the	the treatment of	101 et seq.
	residents.	elements, when	integrity of	(§4-110-105(a)(1))	provided in [§4-110-	provisions	personal	[regulating
	(§4-110-105(a)	either the name or	personal		105(c)] or any	regarding electronic	information and is	deceptive trade
	(1))	the data element is	information	Credit reporting	measures necessary	records and	otherwise	practices]."
		not encrypted or	maintained by a	agency notice	to determine the	signatures set forth	consistent with the	(§4-110-108)
	Service provider	redacted:	person or business."	requirement: No.	scope of the breach	in 15 U.S.C. 7001,	timing requirements	
	requirement:	(A) Social	(§4-110-103(1)(A))		and restore the	as it existed on	of this section shall	Private right of
	Yes. "Any person	security number;	T	Government notice	reasonable integrity	January 1, 2005; or	be deemed to be in	action: No.
	or business that	(B) Driver's	Exception:	requirement: No.	of the data system."	(3) Substitute	compliance with	
	maintains computerized data	license number or Arkansas	"[D]oes not include the good faith		(§4-110-105(a)(2))	notice if the person or business	the notification requirements of this	
	that includes	identification card	acquisition of		Delay: Notice may	demonstrates that:	section if the person	
	personal	number;	personal		be delayed "if a law	(i) The cost of	or business notifies	
	information that	(C) Account	information by an		enforcement agency	providing notice	the affected persons	
	the person or	number, credit	employee or agent		determines that the	would exceed two	in accordance with	
	business does not	card number, or	of the person or		notification will	hundred fifty	its policies in the	
	own shall notify	debit card number	business for the		impede a criminal	thousand dollars	event of a breach of	
	the owner or	in combination	legitimate purposes		investigation."	(\$250,000);	the security of the	
	licensee of the	with any required	of the person or		Notification "shall be	(ii) The affected	system."	
	information of any	security code,	business if the		made after the law	class of persons to	(§4-110-105(f))	
	breach of the	access code, or	personal		enforcement agency	be notified		
	security of the	password that	information is not		determines that it	exceeds five	For following	
	system	would permit	otherwise used or		will not compromise	hundred thousand	interagency	
	immediately	access to an	subject to further		the investigation."	(500,000); or	guidelines: Yes.	
	following	individual's	unauthorized		(§4-110-105(c))	(iii) The person or	"The provisions of	
	discovery if the	financial account;	disclosure."			business does not	this chapter do not	
	personal	and	(§4-110-103(1)(B))			have sufficient	apply to a person or	
	information was,	(D) Medical				contact	business that is	

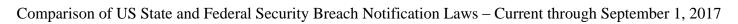


				Arkansas				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	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))	



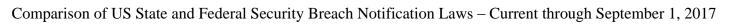


	California											
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?				
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is				
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private				
	requirement		analysis?		•	available?		right of action?				
	for service		·					J				
	providers?											
Cal. Civ. Code	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:				
§§ 1798.29,	"A person or	information:	A "breach of the	"[A] resident of	"[F]ollowing	""[N]otice' may be	own notification	"Any business that				
1798.80 et seq.	business that	"(1) An	security of the	California (1) whose	discovery or	provided by one of	method: Yes.	violates, proposes				
	conducts business	individual's	system" is the	unencrypted personal	notification of the	the following	"[A] person or	to violate, or has				
	in California, and	first name or first	"unauthorized	information was, or	breach in the security	methods:	business that	violated this title				
	that owns or	initial and last	acquisition of	is reasonably	of the data $\dots$ [t]he	(1) Written notice.	maintains its own	may be enjoined."				
	licenses	name in	computerized data	believed to have	disclosure shall be	(2) Electronic	notification	(§1798.84(e))				
	computerized data	combination with	that compromises	been, acquired by an	made in the most	notice, if the notice	procedures as part					
	that includes	any one or more	the security,	unauthorized person,	expedient time	provided is	of an information	Private right of				
	personal	of the following	confidentiality, or	or, (2) whose	possible and without	consistent with the	security policy for	action: Yes.				
	information."	data elements,	integrity of personal	encrypted personal	unreasonable delay,	provisions	the treatment of	"Any customer				
	(§1798.82(a))	when either the	information maintained by the	information was, or is reasonably	consistent with the	regarding electronic records and	personal information and is	injured by a violation of this				
	Service provider	name or the data elements are not	person or business."	believed to have	legitimate needs of law enforcement, as		otherwise	title may institute a				
	requirement:	encrypted:	(§1798.82(g))	been, acquired by an	provided in	signatures set forth in Section 7001 of	consistent with the	civil action to				
	Yes. "A person or	(A) Social	(\$1796.62(g))	unauthorized person	[§1798.82(c)], or any	Title 15 of the	timing requirements	recover damages."				
	business that	security number.	Exception:	and the encryption	measures necessary	United States Code.	of this part, shall be	(§1798.84(b))				
	maintains	(B) Driver's	"Good faith	key or security	to determine the	(3) Substitute	deemed to be in	"Any waiver of a				
	computerized data	license number	acquisition of	credential was, or is	scope of the breach	notice, if the person	compliance with the	provision of this				
	that includes	or California	personal	reasonably believed	and restore the	or business	notification	title is contrary to				
	personal	identification	information by an	to have been,	reasonable integrity	demonstrates that	requirements of this	public policy and is				
	information that	card number.	employee or agent	acquired by an	of the data system."	the cost of	section if the person	void and				
	the person or	(C) Account	of the person or	unauthorized person	(§1798.82(a))	providing notice	or business notifies	unenforceable."				
	business does not	number or credit	business for the	and the person or		would exceed two	subject persons in	(§1798.84(a))				
	own shall notify	or debit card	purposes of the	business that owns or	Non-binding	hundred fifty	accordance with its	"The rights and				
	the owner or	number, in	person or business	licenses the	guidance from the	thousand dollars	policies in the event	remedies available				
	licensee of the	combination with	is not a breach of	encrypted	California Office of	(\$250,000), or that	of a breach of	under [the breach				
	information of the	any required	the security of the	information has a	Privacy Protection	the affected class of	security of the	notification law] are				
	breach of the	security code,	system, provided	reasonable belief that	provides that notice	subject persons to	system."	cumulative to each				
	security of the data immediately	access code, or password that	that the personal information is not	the encryption key or security credential	should be given "within 10 business	be notified exceeds 500,000, or the	(§1798.82(1))	other and to any other rights and				
	following	would permit	used or subject to	could render that	days" of a	person or business	For following	remedies available				
	discovery, if the	access to an	further	personal information	days of a determination "that	does not have	interagency	under law."				
	personal	individual's	unauthorized	readable or useable."	the information was,	sufficient contact	guidelines: Yes.	(§1798.84(h))				
	information was,	financial	disclosure."	(§1798.82(a))	or is reasonably	information."	"A covered entity	(21/)0.07(11))				
	or is reasonably	account.	(§1798.82(g))	(31/20.02(4))	believed to have	(§1798.82(j))	under the federal					
	believed to have	(D) Medical	(0 / 2 - 2 - 10//	Credit reporting	been, acquired by an	(0	Health Insurance					



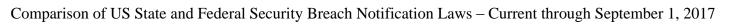


	California										
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?			
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is			
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private			
	requirement		analysis?			available?		right of action?			
	for service										
	providers?										
	been, acquired by	information.*	Non-binding	agency notice	unauthorized	Substitute notice:	Portability and				
	an unauthorized	(E) Health	guidance from the	requirement: No.	person," subject to	"Substitute notice	Accountability Act				
	person."	insurance	California Office of		the needs of law	shall consist of all	of 1996 (HIPAA)				
	(§1798.82(b))	information.**	Privacy Protection	Government notice	enforcement.	of the following:	(42 U.S.C. Sec.				
		(F) Information	suggests	requirement: Yes.	Recommended	(A) Email notice	1320d et seq.) will				
		or data collected	considering the	"Any person or	Practices on Notice	when the person or	be deemed to have				
		through the use	following factors	business that is	of Security Breach	business has an	complied with the				
		or operation of	when determining	required to issue a	Involving Personal	email address for	notice requirements				
		an automated	whether	security breach	Information,	the subject persons.	in subdivision (d) if				
		license plate	unencrypted notice-	notification pursuant	California Office of	(B) Conspicuous	it has complied				
		recognition	triggering information has	to this section to more than 500	Privacy Protection	posting, for a minimum of 30	completely with Section 13402(f) of				
		system, as defined in	been acquired, or is	California residents	(Jan. 2012)	days, of the notice	the federal Health				
		Section	reasonably believed	as a result of a single	Delay:	on the Internet Web	Information				
		1798.90.5."	to have been	breach of the security	Notice may be	site page of the	Technology for				
		OR	acquired, by an	system shall	delayed "if a law	person or business,	Economic and				
		"(2) A user name	unauthorized	electronically submit	enforcement agency	if the person or	Clinical Health Act				
		or email address,	person:	a single sample copy	determines that the	business maintains	(Public Law 111-5).				
		in combination	"(1) Indications that	of that security	notification will	one. For purposes	However, nothing				
		with a password	the information is	breach notification,	impede a criminal	of this	in this subdivision				
		or security	in the physical	excluding any	investigation."	subparagraph,	shall be construed				
		question and	possession and	personally	Notification "shall be	conspicuous	to exempt a covered				
		answer that would	control of an	identifiable	made promptly after	posting on the	entity from any				
		permit access to	unauthorized	information, to the	the law enforcement	person's or	other provision of				
		an online	person, such as a	Attorney General."	agency determines	business's Internet	this section."				
		account."	lost or stolen	(§1798.82(f))	that it will not	Web site means	(§1798.82(e))				
		(§1798.82(h))	computer or		compromise the	providing a link to					
			other device		investigation."	the notice on the					
		* Medical	containing		(§1798.82(c))	home page or first					
		information means	unencrypted notice-			significant page					
		"any information	triggering			after entering the					
		regarding an individual's	information;			Internet Web site					
		medical history,	(2) Indications that the information has			that is in larger type than the					
		mental or physical	been downloaded or			surrounding text, or					
		condition, or	copied; and			in contrasting type,					
		medical treatment	(3) Indications that			font, or color to the					
		or diagnosis by a	the information was			surrounding text of					



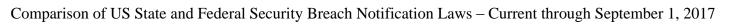


				California				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice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



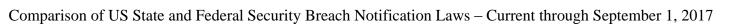


	California											
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute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



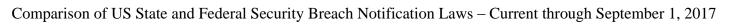


	California											
State Statute	What entities are covered? Is there a requirement	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there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



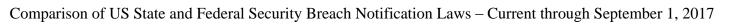


	California											
State Statute	What entities are covered? Is there a requirement	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?				
	for service providers?											
	providers:					(A) The name and						
						contact						
						information of the						
						reporting person						
						or business subject to this section.						
						(B) A list of the						
						types of personal						
						information that						
						were or are						
						reasonably						
						believed to have been the subject of						
						a breach.						
						(C) If the						
						information is						
						possible to						
						determine at the time the notice is						
						provided, then any						
						of the following:						
						(i) the date of the						
						breach,						
						(ii) the estimated						
						date of the breach, or						
						(iii) the date						
						range within						
						which the breach						
						occurred.						
						The notification						
						shall also include						
						the date of the notice.						
						(D) Whether						
						notification was						
						delayed as a result						
						of a law						



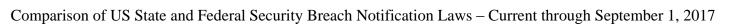


	California										
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?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



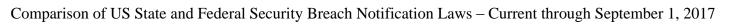


	California										
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?			
	providers?					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)]. (3) At the discretion of the person or business, the security breach notification may also include any of the following: (A) Information about what the person or business has done to protect individuals whose information has been breached.					





	California											
State Statute	What entities are covered? Is there a requirement for service	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?				
	providers?					(B) Advice on steps that the person whose information has been breached may take to protect himself or herself." (§1798.82(d))  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						

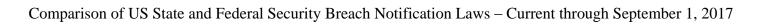




	California											
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?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

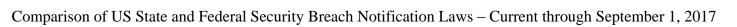


				California				
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?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



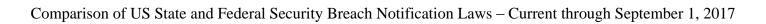


	Colorado										
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?			
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is			
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private			
	requirement for		analysis?			available?		right of action?			
	service		·								
	providers?										
Colo. Rev. Stat.	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:			
§6-1-716	"An individual or	information:	"Breach of the	Notice must be given	"Notice shall be	"'Notice' means	own notification	"The attorney			
	a commercial	"[A] Colorado	security of the	to the "affected	made in the most	(I) Written notice to	method: Yes.	general may bring			
	entity that	resident's first	system' means the	Colorado resident."	expedient time	the postal address	"[A]n individual or	an action in law or			
	conducts business	name or first	unauthorized	(§6-1-716(2)(a))	possible and without	listed in the records	a commercial entity	equity to address			
	in Colorado and	initial and last	acquisition of		unreasonable delay,	of the individual or	that maintains its	violations of this			
	that owns or	name in	unencrypted	Credit reporting	consistent with the	commercial entity;	own notification	section and for other			
	licenses	combination with	computerized data	agency notice	legitimate needs of	(II) Telephonic	procedures as part	relief that may be			
	computerized data	any one or more of	that compromises	requirement: Yes.	law enforcement and	notice;	of an information	appropriate to			
	that includes	the following data	the security,	If a "commercial	consistent with any	(III) Electronic	security policy for	ensure compliance			
	personal	elements that	confidentiality, or	entity is required to	measures necessary	notice, if a primary	the treatment of	with this section or			
	information about	relate to the	integrity of personal	notify more than one	to determine the	means of	personal	to recover direct			
	a resident of	resident, when the	information	thousand Colorado	scope of the breach	communication by	information and	economic damages			
	Colorado."	data elements are	maintained by an individual or a	residents of a breach	and to restore the	the individual or	whose procedures	resulting from a violation, or both.			
	(§6-1-716(2)(a))	not encrypted, redacted, or secure	commercial entity."	of the security of the system pursuant to	reasonable integrity of the computerized	commercial entity with a Colorado	are otherwise consistent with the	The provisions of			
	Service provider	by any other	(§6-1-716(1)(a))	this section, the	data system."	resident is by	timing requirements	this section are not			
	requirement: Yes.	method rendering	(80-1-710(1)(a))	individual or	(§6-1-716(2)(a))	electronic means or	of this section shall	exclusive and do not			
	"An individual or	the name or the	Exception:	commercial entity	(90-1-710(2)(a))	the notice provided	be deemed to be in	relieve an individual			
	a commercial	element	"Good faith	shall also notify,	Delay:	is consistent with	compliance with the	or a commercial			
	entity that	unreadable or	acquisition of	without unreasonable	Notice may be	the provisions	notice requirements	entity subject to this			
	maintains	unusable:	Personal	delay, all consumer	delayed "if a law	regarding electronic	of this section if the	section from			
	computerized data	(A) Social security	information by an	reporting agencies	enforcement agency	records and	individual or the	compliance with all			
	that includes	number;	employee or agent	that compile and	determines that the	signatures or	commercial entity	other applicable			
	personal	(B) Driver's	of the person or	maintain files on	notice will impede a	(IV) Substitute	notifies affected	provisions of law."			
	information that	license number or	business for the	consumers on a	criminal investigation	notice, if the	Colorado customers	(§6-1-716(4))			
	the individual or	identification card	purposes of the	nationwide basis, as	and the law	individual or the	in accordance with				
	the commercial	number;	person or business	defined by 15 U.S.C.	enforcement agency	commercial entity	its policies in the	Private right of			
	entity does not	(C) Account	is not a breach of	sec. 1681a (p), of the	has notified the	required to provide	event of a breach of	action: No.			
	own or license	number or credit	the security of the	anticipated date of	individual or	notice demonstrates	security of the				
	shall give notice to	or debit card	system, provided	the notification to the	commercial entity	that the cost of	system."				
	and cooperate with	number, in	that the personal	residents and the	that conducts	providing notice	(§6-1-716(3)(a))				
	the owner or	combination with	information is not	approximate number	business in Colorado	will exceed two					
	licensee of the	any required	used or subject to	of residents who are	not to send notice	hundred fifty	For following				
	information of any	security code,	further unauthorized	to be notified."	required by this	thousand dollars,	interagency				
	breach of the	access code, or	disclosure."	(§6-1-716(2)(d))	section."	the affected class of	guidelines: Yes.				
	security of the	password that	(§6-1-716(1)(a))		(§6-1-716(2)(c))	persons to be	"An individual or a				



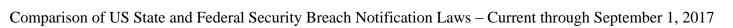


	Colorado										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice 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 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))				





				Connecticut				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?			available?		right of action?
	service		J					g
	providers?							
Conn. Gen. Stat.	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:
§§36a-701b, 4e-	"Any person who	information:	A "breach of	Any Connecticut	"[F]ollowing the	"Any notice	own notification	"Failure to comply
70; [2015 Conn.	conducts business	"[A]n individual's	security" is the	resident "whose	discovery of the	required by the	method: Yes.	with the
Legis. Serv. P.A.	in [Connecticut],	first name or first	"unauthorized	personal information	breach notice	provisions of this	"Any person that	requirements of this
15-142 (S.B.	and who, in the	initial and last	access to or	was breached or is	shall be made without	section may be	maintains such	section shall
949)]	ordinary course of	name in	unauthorized	reasonably believed	unreasonable delay	provided by one of	person's own	constitute an unfair
/ j	such person's	combination with	acquisition of	to have been	but not later than	the following	security breach	trade practice for
	business, owns,	any one, or more,	electronic files,	breached."	ninety days after the	methods:	procedures as part	purposes of section
	maintains or	of the following	media, databases, or	(§36a-701b(b)(1))	discovery of such	(1) Written notice;	of an information	42-110b and shall
	licenses	data:	computerized data,	.,,,,	breach, unless a	(2) telephone	security policy for	be enforced by the
	computerized data	(A) Social	containing personal	Credit reporting	shorter time is	notice;	the treatment of	Attorney General."
	that includes	Security number;	information when	agency notice	required under	(3) electronic	personal	(§36a-701b(g))
	personal	(B) Driver's	access to the	requirement: No.	federal law, subject to	notice, provided	information and	
	information."	license number or	personal		the provisions of	such notice is	otherwise complies	Private right of
	(§36a-701b(b)(1))	state identification	information has not	Government notice	[§36a-701b(d)] and	consistent with the	with the timing	action: No.
		card number; or	been secured by	requirement: Yes.	the completion of an	provisions regarding	requirements of this	
	Service provider	(C) Any account	encryption or by	"The person who	investigation by such	electronic records	section, shall be	
	requirement:	number, credit or	any other method or	conducts business in	person to determine	and signatures set	deemed to be in	
	Yes. "Any person	debit card number,	technology that	this state, and who, in	the nature and scope	forth in 15 USC	compliance with the	
	that maintains	in combination	renders the personal	the ordinary course of	of the incident, to	7001;	security breach	
	computerized data	with any required	information	such person's	identify the	(4) substitute notice,	notification	
	that includes	security code,	unreadable or	business, owns,	individuals affected,	provided such	requirements of this	
	personal	access code, or	unusable."	licenses or maintains	or to restore the	person demonstrates	section, provided	
	information that	password that	(§36a-701b(a))	computerized data	reasonable integrity	that the cost of	such person notifies,	
	the person does	would permit	D'ala ella anno	that includes personal	of the data system."	providing notice in	as applicable,	
	not own shall	access to an individual's	Risk of harm analysis: Yes.	information, shall, not later than the time	(§36a-701b(b)(1))	accordance with	residents of this	
	notify the owner	financial account."				subdivision (1), (2)	state, owners and	
	or licensee of the		"Such notification	when notice is	•	or (3) of this	licensees in	
	information of any breach of the	(§36a-701b(a))	shall not be required if, after an	provided to the resident, also provide		subsection would exceed two hundred	accordance with such person's	
	security of the data	Exception:	,	notice of the breach		fifty thousand	policies in the event	
	immediately	"Personal	appropriate investigation and	of security to the		dollars, that the	of a breach of	
	following its	information' does	consultation with	Attorney General."		affected class of	security and in the	
	discovery, if the	not include	relevant federal,	(§36a-701b(b)(2)(A))		subject persons to	case of notice to a	
	personal	publicly available	state and local	(\$30a-7010(0)(2)(A))		be notified exceeds	resident, such	
	information of a	information that is	agencies responsible			five hundred	person also notifies	
	resident of this	lawfully made	for law			thousand persons or	the Attorney	



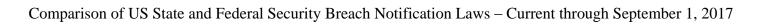


				Connecticut				
State Statute	What entities are covered? Is there a requirement for	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	service providers?							
	state was breached	available to the	enforcement, the			the person does not	General not later	
	or is reasonably believed to have been breached." (§36a-701b(c))	general public from federal, state or any local government	person reasonably determines that the breach will not likely result in harm			have sufficient contact information." (§36a-701b(e))	than the time when notice is provided to the resident." (§36a-701b(f))	
	Contractors:	records or widely distributed	to the individuals whose personal			Substitute notice:	For following	
	Connecticut law also places special	media." (§36a-701b(a))	information has been acquired and			"Substitute notice shall consist of the	interagency guidelines: Yes.	
	requirements on state contractors.	(3504 7010(4))	accessed." (§36a-701b(b)(1))			following: (A) Electronic mail	"Any person that maintains such	
	A "Contractor" is defined as "an					notice when the person, business or	[person's own] security breach	
	individual, business or other					agency has an electronic mail	procedure pursuant to the rules,	
	entity that is receiving confidential					address for the affected persons;	regulations, procedures or	
	information from a state contracting					(B) conspicuous posting of the notice on the web site of	guidelines established by the primary or	
	agency or agent of the state pursuant					the person, business or agency if the	functional regulator, as defined in 15	
	to a written agreement to					person maintains one; and	USC 6809(2) [of the Gramm Leach	
	provide goods or services to the					(C) notification to major state-wide	Bliley Act] shall be deemed to be in	
	state." (§4e-70(a)(1))					media, including newspapers, radio	compliance with the security breach	
	Contractors must take special					and television." (§36a-701b(e))	notification requirements of this section, provided	
	precautions with residents' data.					Notice contents requirement:	such person notifies, as applicable, such	
	Any contract between the state					If a breach exposes Social Security	residents of this state, owners, and	
	or a state agency and a contractor					Numbers, the notice to residents must	licensees required to be notified under	
	must require that					include "appropriate	and in accordance	



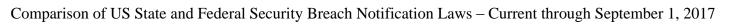
				Connecticut				
State Statute	What entities are covered? Is	What data are covered?	Has there been a breach? Is there	Who receives notice?	When must notice be given? May	How must notice be given? Is	Is there an exemption or	Enforcement? Penalties? Is
	there a	00,01000	a risk of harm	11011001	notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?		notice be delayed.	available?	saic nai boi .	right of action?
	service		anarysis.			available.		right of action.
	providers?							
	the contractor					identity theft	with the policies or	
	"[n]otify the state					prevention services	the rules,	
	contracting agency					and, if applicable,	regulations,	
	and the Attorney					identity theft	procedures or	
	General as soon as					mitigation services.	guidelines	
	practical after the					Such service or	established by the	
	contractor					services shall be	primary or	
	becomes aware of					provided at no cost	functional regulator	
	or has reason to					to such resident for	in the event of a	
	believe that any					a period of not less	breach of security of	
	confidential					than twelve months.	the system."	
	information that					[The covered entity]	(§36a-701b(f))	
	the contractor					shall provide all		
	possesses or					information		
	controls has been					necessary for such		
	subject to a					resident to enroll in		
	confidential					such service or		
	information					services and shall		
	breach."					include information		
	(§4e-70(b)(6))					on how such		
	F '44					resident can place a		
	Every written agreement with a					credit freeze on such resident's		
	contractor must					credit file."		
	also:					(§36a-		
	"(1) Include a					701b(b)(2)(B))		
	proposed timetable					7010(b)(2)( <b>D</b> ))		
	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,							

hat entities covered? Is there a irement for service roviders?	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	Is there an exemption or	Enforcement? Penalties? Is
roviders?				nouce be delayed?	substitute notice available?	safe harbor?	there a private right of action?
further							
stigation, the ractor believes reach has rred; and							
pecify how ost of any ication about, vestigation a confidential mation breach be rtioned when tate racting agency ontractor is the ect of such a ch."							
th Insurers: ctive Oct. 1, t, health eers and ed companies be subject to ctional data acy ections, and connecticut rance missioner will authority to ree those isions.							
peoos iccommunitation in the control of the control	etor believes ach has ed; and ecify how at of any attion about, estigation confidential attion breach ecim agency tractor is the tof such a "O(e)(1)-(2))  Insurers: ve Oct. 1, health es and companies subject to anal data ecim and mecticut ace issioner will atthority to et those	ector believes ach has ed; and ecify how at of any attion about, estigation confidential attion breach ecting agency tractor is the et of such a ""  O(e)(1)-(2))  Insurers:  ve Oct. 1, health es and companies es subject to enal data ey dions, and ennecticut ece issioner will atthority to et those enos.	ector believes ach has ed; and ecify how st of any ation about, estigation confidential ation breach ecting agency tractor is the et of such a"  O(e)(1)-(2))  In Insurers:  ve Oct. 1, health is and companies esubject to smal data y dions, and necticut ece issioner will authority to et those enos.	eter believes ach has ed; and sed; and	ctor believes ach has ed; and carried and companies subject to snad companies subject to snad data of companies subject to snad metatical data of companies subject to snad metatical data of companies subject to snad companies sna	actor believes ach has ed; and continued by the state of any attornation about, stigation confidential attornation breach attor	ach has ded; and ded;





				Delaware				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?		·	available?		right of action?
	service		·					
	providers?							
Del. Code Ann.	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:
tit. 6, §12B-101	"Any person who	information:	A "breach of	"[A]ny resident of	"Notice must be	"Notice' means	own notification	"Pursuant to the
et seq.; H.B. 180	conducts business	"[A] Delaware	security" means	this State whose	made without	any of the	method: Yes.	enforcement duties
(effective April	in this State and	resident's first	"[t]he unauthorized	personal information	unreasonable delay	following:	"[A] person that	and powers of the
14, 2018)	who owns or	name or first	acquisition of	was breached or is	but not later than 60	(a) Written notice.	maintains its own	Director of
	licenses	initial and last	computerized data	reasonably believed	days after	(b) Telephonic	notice procedures as	Consumer
	computerized data	name in	that compromises	to have been	determination of the	notice.	part of an	Protection of the
	that includes	combination with	the security,	breached."	breach of security."	(c) Electronic	information security	Department of
	personal	any 1 or more of	confidentiality, or	(§12B-102(a))	(§12B-102(c))	notice, if the notice	policy for the	Justice Chapter 25
	information."	the following data	integrity of personal	G 111	n.	provided is	treatment of	of Title 29, the
	(§12B-102(a))	elements that	information."	Credit reporting	Delay:	consistent with the	personal	Attorney General
	*"'Person' means	relate to that	(§12B-101(1)(a))	agency notice	Notice required may be delayed if:	provisions regarding electronic records	information, and	may bring an action
		individual:	E	requirement: No.	_		whose procedures	in law or equity to
	an individual; corporation;	(1) Social Security number.	Exception:"Good faith	Government notice	"(1) A shorter time is required under	and signatures set forth in § 7001 of	are otherwise consistent with the	address the violations of this
	business trust:	(2) Driver's	acquisition of	requirement: Yes.	federal law.	Title 15 of the	timing requirements	chapter and for
	estate trust;	license number or	personal	"If the affected	(2) A law	United States Code	of this chapter is	other relief that may
	partnership;	state or federal	information by an	number of Delaware	enforcement agency	or if the person's	deemed to be in	be appropriate to
	limited liability	identification card	employee or agent	residents to be	determines that the	primary means of	compliance with the	ensure proper
	company;	number.	of any person for	notified exceeds 500	notice will impede a	communication with	notice requirements	compliance with
	association; joint	(3) Account	the purposes of such	residents, the person	criminal investigation	the resident is by	of this chapter if the	this chapter or to
	venture;	number, credit	person is not a	required to provide	and such law	electronic means.	person notifies	recover direct
	government;	card number, or	breach of security,	notice shall, not later	enforcement agency	(d) Substitute notice	affected Delaware	economic damages
	governmental	debit card number,	provided that the	than the time when	has made a request of	if the person	residents in	resulting from a
	subdivision,	in combination	personal	notice is provided to	the person that the	required to provide	accordance with its	violation, or both.
	agency, or	with any required	information is not	the resident, also	notice be delayed.	notice under this	policies in the event	The provisions of
	instrumentality;	security code,	used for an	provide notice of the	Any such delayed	chapter	of a breach of	this chapter are not
	public corporation;	access code, or	unauthorized	breach of security to	notice must be made	demonstrates that	security."	exclusive and do not
	or any other legal	password that	purpose or subject	the Attorney	after such law	the cost of	(§12B-103(a))	relieve entity person
	or commercial	would permit	to further	General."	enforcement agency	providing notice		subject to this
	entity."	access to a	unauthorized	(§12B-102(d))	determines that notice	will exceed	For following	chapter from
	g,	resident's financial	disclosure."		will not compromise	\$75,000, the	interagency	compliance with all
	Service provider	account.	(§12B-101(1)(a))		the criminal	affected number of	guidelines: Yes.	other applicable
	requirement:	(4) Passport	"The unauthorized		investigation and so	Delaware residents	"Under this chapter,	provisions of law."
	Yes. "A person	number.	acquisition of		notifies the person of	to be notified	a person that is	(§12B-104(a))
	that maintains computerized data	5. A username or email address, in	computerized data that compromises		such determination.	exceeds 100,000 residents, or that the	regulated by state or federal law.	
	computerized data	eman address, in	mat compromises		(3) When a person	residents, or that the	rederal law,	

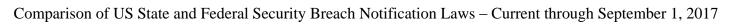




	Delaware										
State Statute	What entities are covered? Is there a	What data are covered?	Has there been a breach? Is there a risk of harm	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private			
	requirement for		analysis?		notice be delayed.	available?	Suit hui boi .	right of action?			
	service		unuiy sis t			u vanasie v		right of detion.			
	providers?										
	that includes	combination with	the security,		otherwise required	person does not	including the Health	Private right of			
	personal	a password or	confidentiality, or		to provide notice,	have sufficient	Insurance	action: No. But			
	information that	security question	integrity of personal		could not, through	contact information	Portability and	"[n]othing in this			
	the person does	and answer that	information is not a		reasonable diligence,	to provide notice."	Accountability Act	chapter may be			
	not own or license	would permit	breach of security to		identify within 60	(§12B-101(3))	of 1996 (P.L. 104–	construed to modify			
	shall give notice to	access to an online	the extent that		days that the personal		191, as amended)	any right which a			
	and cooperate with	account.	personal		information of certain	Substitute notice:	and the Gramm	person may have at			
	the owner or	6. Medical history,	information		residents of this State	"Substitute notice	Leach Bliley Act	common law, by			
	licensee of the	medical treatment	contained therein is		was included in a	consists of all of the	(15 U.S.C. § 6801 et	statute, or			
	information of any	by a healthcare	encrypted, unless		breach of security,	following:	seq., as amended),	otherwise."			
	breach of security	professional,	such unauthorized		such person must	(1) Electronic notice	and that maintains	(§12B-104(b))			
	immediately	diagnosis of	acquisition includes,		provide the notice	if the person has	procedures for a				
	following	mental or physical condition by a	or is reasonably believed to include,		required by § 12B–	email addresses for the members of the	breach of security				
	determination of the breach of	health care	the encryption key		102(a) to such residents as soon as	affected class of	pursuant to the laws, rules.				
	security."	professional, or	and the person that		practicable after the	Delaware residents.	regulations,				
	(§12B-102(b))	deoxyribonucleic	owns or licenses the		determination that the	(2) Conspicuous	guidance, or				
	(§12D-102(0))	acid profile.	encrypted		breach of security	posting of the notice	guidelines				
		7. Health	information has a		included the personal	on the web site page	established by its				
		insurance policy	reasonable belief		information of such	of the person if the	primary or				
		number,	that the encryption		residents, unless such	person maintains	functional state or				
		subscriber	key could render		person provides or	one.	federal regulator is				
		identification	that personal		has provided	(3) Notification to	deemed to be in				
		number, or any	information		substitute notice in	major statewide	compliance with				
		other unique	readable or		accordance with §	media, including	this chapter if the				
		identifier used by	useable."		12B-101(3)d."	newspapers, radio,	person notifies				
		a health insurer to	(§12B-101(1)(b))		(§12B-102(c))	and television and	affected Delaware				
		identify the				publication on the	residents in				
		person.	Risk of harm			major social media	accordance with the				
		8. Unique	analysis: Yes.			platforms of the	maintained				
		biometric data	"Any person who			person providing	procedures when a				
		generated from	conducts business in			notice."	breach of security				
		measurements or	this State and who			(§12B-101(3)(d))	occurs."				
		analysis of human	owns or licenses				(§12B-103(b))				
		body	computerized data			Breaches That					
		characteristics for	that includes			Permit Access to					
		authentication	personal			Email Accounts:					
		purposes.	information shall			"In the case of a					



				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?
		9. An individual taxpayer identification number." (§12B-101(4)(a))  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))	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))			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))		

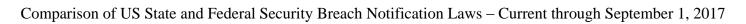




				District of Colum	nbia			
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
D.C. O.C. 1	providers?		D 116° '/'	D 11 4	m· ·	36.4	77	T 1 C
D.C. Off 1 Code §28-3851 et seq.	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))  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	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	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))  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 personal information is not used improperly or subject to further unauthorized disclosure."	Residents: Notice must be given to "any District of Columbia resident whose personal information was included in the breach." (§28-3852(a))  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))  Government notice requirement: No.	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))  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))	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	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))  For following	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."
	security of the system in the most	individual's financial or credit	(§28-3851(1))		(320 0001(4))	the person or business does not	interagency guidelines: Yes.	(§28-3853(b))

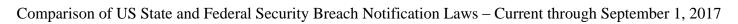


				District of Colur	nbia			
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute 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 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))



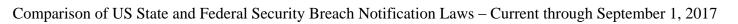


				Florida				
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	providers?							-
Fla. Stat. Ann. §501.171	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))  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	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	Breach definition: "Breach of security' or 'breach' means unauthorized access of data in electronic form containing personal information." (§501.171(1)(a))  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))  Risk of harm analysis: Yes. "Notice to the affected individuals is not required if, after an appropriate	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))  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	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))	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))  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 range of the breach of	For establishing own notification method: No.  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	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
	later than 10 days following the determination of the breach of security or reason to believe the	or credit or debit card number, in combination with any required security code, access code, or	investigation and consultation with relevant federal, state, or local law enforcement	Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices."	Delay: "If a federal, state, or local law enforcement agency determines that notice to individuals	security.  2. A description of the personal information that was accessed or reasonably believed	event of a breach of security. Under this paragraph, a covered entity that timely provides a copy of such notice	any violation, and thereafter, \$50,000 for each subsequent 30-day period or portion thereof for up to





				Florida				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?			available?		right of action?
	service							
	providers?							
	breach occurred.	password that is	agencies, the	(§501.171(5))	required under this	to have been	to the department is	180 days.
	Upon receiving	necessary to	covered entity		subsection would	accessed as a part of	deemed to be in	2. If the violation
	notice from a	permit access to	reasonably	Government notice	interfere with a	the breach of	compliance with the	continues for more
	third-party agent, a	an individual's	determines that the	requirement: Yes.	criminal	security.	notice requirement."	than 180 days, in
	covered entity	financial account;	breach has not and	"(a) A covered entity	investigation, the	3. Information that	(§501.171(4)(g))	an amount not to
	shall provide	(IV) Any	will not likely result	shall provide notice	notice shall be	the individual can		exceed \$500,000.
	notices required	information	in identity theft or	to the [Florida	delayed upon the	use to contact the		The civil penalties
	under	regarding an	any other financial	Department of Legal	written request of the	covered entity to		for failure to notify
	[§§501.171(3) and	individual's	harm to the	Affairs] of any	law enforcement	inquire about the		provided in this
	501.171(4)]. A	medical history,	individuals whose	breach of security	agency for a specified	breach of security		paragraph apply per
	third-party agent	mental or	personal	affecting 500 or more	period that the law	and the personal		breach and not per
	shall provide a	physical	information has	individuals in this	enforcement agency	information that the		individual affected
	covered entity with all	condition, or medical	been accessed.	state. Such notice must be provided to	determines is	covered entity maintained about		by the breach."
	information that		Such a determination must	the department as	reasonably necessary.  A law enforcement	the individual."		(§501.171(9))
	the covered entity	treatment or diagnosis by a	be documented in	expeditiously as	agency may, by a	(§501.171(4)(e))		Private right of
	needs to comply	health care	writing and	practicable, but no	subsequent written	(8301.171(4)(6))		action: No.
	with its notice	professional;	maintained for at	later than 30 days	request, revoke such	Substitute notice:		"This section does
	requirements.	(V) An	least 5 years. The	after the	delay as of a	"A covered entity		not establish a
	(b) An agent may	individual's	covered entity shall	determination of the	specified date or	required to provide		private cause of
	provide notice as	health insurance	provide the written	breach or reason to	extend the period set	notice to an		action."
	required under	policy number or	determination to the	believe a breach	forth in the original	individual may		(§501.171(10))
	[§§501.171(3) and	subscriber	department within	occurred. A covered	request made under	provide substitute		(0
	501.171(4)] on	identification	30 days after the	entity may receive 15	this paragraph to a	notice in lieu of		
	behalf of the	number and any	determination."	additional days to	specified date if	direct notice if such		
	covered entity;	unique identifier	(§501.171(4)(c))	provide notice as	further delay is	direct notice is not		
	however, an	used by a health		required in	necessary."	feasible because the		
	agent's failure to	insurer to		[§501.171(4)] if good	(§501.171(4)(b))	cost of providing		
	provide proper	identify the		cause for delay is		notice would exceed		
	notice shall be	individual.		provided in writing to		\$250,000, because		
	deemed a violation	b. A user name or		the department within		the affected		
	of this section	e-mail address, in		30 days after		individuals exceed		
	against the	combination with		determination of the		500,000 persons, or		
	covered entity."	a password or		breach or reason to		because the covered		
	(§501.171(6))	security question		believe a breach		entity does not have		
		and answer that		occurred.		an e-mail address or		
		would permit		(b) The written		mailing address for		
		access to an online		notice to the		the affected		

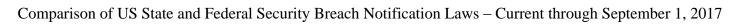




	Florida											
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?				
	providers?											
	providers	account." (§501.171(1)(g) (1))  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))		department must include:  1. A synopsis of the events surrounding the breach at the time notice is provided.  2. The number of individuals in this state who were or potentially have been affected by the breach.  3. Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services.  4. A copy of the 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.		individuals. Such substitute notice shall include the following:  1. A conspicuous notice on the Internet website of 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))						
		(2))		address of the								

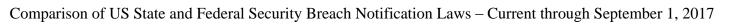


	Florida											
State Statute	What entities are covered? Is there a requirement for	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is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





				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 et	Covered entities: "Any information	Personal information:	Breach definition: A "breach of the	Residents: Notification must be	Timing: "The notice shall be	Method: "Notice' means:	For establishing own notification	Enforcement: Not specified.
seq., §46-5-214	broker or data	"[A]n individual's	security of the	given to "any resident	made in the most	(A) Written notice;	method: Yes.	specified.
seq., 310 3 211	collector that	first name or first	system" is the	of [Georgia] whose	expedient time	(B) Telephone	"[A]n information	Private cause of
	maintains	initial and last	"unauthorized	unencrypted personal	possible and without	notice;	broker or data	action: No.
	computerized data	name in	acquisition of an	information was, or is	unreasonable delay,	(C) Electronic	collector that	
	that includes	combination with	individual's	reasonably believed	consistent with the	notice, if the notice	maintains its own	
	personal	any one or more of	computerized data	to have been,	legitimate needs of	provided is	notification	
	information."	the following data	that compromises	acquired by an	law enforcement, as	consistent with the	procedures as part	
	(§10-1-912(a))	elements, when	the security,	unauthorized person."	provided in [§10-1-	provisions regarding	of an information	
		either the name or	confidentiality, or	(§10-1-912(a))	912(c)], or with any	electronic records	security policy for	
	Information	the data elements	integrity of personal		measures necessary	and signatures set	the treatment of	
	broker:	are not encrypted	information of such	Credit reporting	to determine the	forth in Section	personal	
	An "information	or redacted:	individual	agency notice	scope of the breach	7001 of Title 15 of	information and is	
	broker" means	(A) Social security	maintained by an	requirement: Yes.	and restore the	the United States	otherwise consistent	
	"any person or	number;	information broker	"In the event that an	reasonable integrity,	Code; or	with the timing	
	entity who, for	(B) Driver's	or data collector."	information broker or	security, and	(D) Substitute	requirements of this	
	monetary fees or	license number or	(§10-1-911(1))	data collector	confidentiality of the	notice, if the	article shall be	
	dues, engages in	state identification	T	discovers	data system."	information broker	deemed to be in	
	whole or in part in	card number;	Exception: "Good faith	circumstances	(§10-1-912(a))	or data collector	compliance with the	
	the business of collecting,	(C) Account		requiring notification	Dalam	demonstrates that	notification	
	assembling,	number, credit card number, or	acquisition of personal	pursuant to this Code section of more than	<b>Delay</b> : Notification "may be	the cost of providing notice	requirements of this article if it notifies	
	evaluating,	debit card number,	information by an	10,000 residents of	delayed if a law	would exceed	the individuals who	
	compiling,	if circumstances	employee or agent	[Georgia] at one time,	enforcement agency	\$50,000.00, that the	are the subjects of	
	reporting,	exist wherein such	of an information	the information	determines that the	affected class of	the notice in	
	transmitting,	a number could be	broker or data	broker or data	notification will	individuals to be	accordance with its	
	transferring, or	used without	collector for the	collector shall also	compromise a	notified exceeds	policies in the event	
	communicating	additional	purposes of such	notify, without	criminal	100,000, or that the	of a breach of the	
	information	identifying	information broker	unreasonable delay,	investigation. The	information broker	security of the	
	concerning	information,	or data collector is	all consumer	notification required	or data collector	system."	
	individuals for the	access codes, or	not a breach of the	reporting agencies	by this Code section	does not have	(§10-1-911(4))	
	primary purpose	passwords;	security of the	that compile and	shall be made after	sufficient contact		
	of furnishing	(D) Account	system, provided	maintain files on	the law enforcement	information to	For following	
	personal	passwords or	that the personal	consumers on a	agency determines	provide written or	interagency	
	information to	personal	information is not	nation-wide basis, as	that it will not	electronic notice to	guidelines: No.	
	nonaffiliated third	identification	used or subject to	defined by 15 U.S.C.	compromise the	such individuals."		
	parties."	numbers or other	further unauthorized	Section 1681a, of the	investigation."	(§10-1-911(4))		

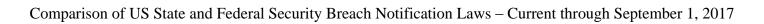




				Georgia				
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	<b>providers?</b> (§10-1-911(3))	access codes; or	disclosure."	timing, distribution,	(§10-1-912(c))	Substitute notice:		
	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))  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))  Person: "Person" means "any individual, partnership,	(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))  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))	(§10-1-911(1))  Risk of harm analysis: No, except as the definition of "breach" may incorporate elements of such a test.	and content of the notices." (§10-1-912(d))  Government notice requirement: No.		"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))		

				Georgia				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?			available?		right of action?
	service							
	providers?							
	corporation,							
	limited liability							
	company, trust,							
	estate,							
	cooperative,							
	association, or other entity."							
	(§10-1-911(5))							
	(§10-1-711(3))							
	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							

				Georgia				
State Statute	What entities are covered? Is there a requirement for service	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?
	providers? an unauthorized							
	person." (§10-1-912(b))							
	Telecommunicati ons 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.							



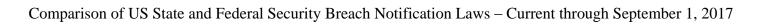


				Guam				
State Statute	What entities	What data are	Has there been a	Who receives	When must	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	notice be given?	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		May notice be	substitute notice	safe harbor?	there a private
	requirement for		analysis?		delayed?	available?		right of action?
	service		J					<b>g</b>
	providers?							
9 GCA § 48-10 et	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	Local
seq.	"An individual or	information:	A "breach of the	Any affected	An individual or	"Notice means:	own notification	enforcement:
seq.	entity that owns or	"[F]irst name, or	security of a	resident of Guam.	entity maintaining a	(1) Written notice	method: Yes.	"(a) A violation of
	licenses	first initial, and last	system" is the	(§48.30(a))	computerized	to the postal	"An entity that	this Chapter that
	computerized data	name in	"unauthorized	(3 1010 (11))	system with	address in the	maintains its own	results in injury or
	that includes	combination with	access and	Credit reporting	personal	records of the	notification	loss to residents of
	personal	and linked to any	acquisition of	agency	information "shall	individual or entity;	procedures as part	Guam may be
	information."	one or more of the	unencrypted and	requirement: No.	notify the owner or	(2) Telephone	of an information	enforced by the
	(§48.30(a))	following data	unredacted		licensee of the	notice;	privacy or security	Office of the
		elements that relate	computerized data	Government	information of any	(3) Electronic	policy for the	Attorney General.
	Individual:	to a resident of	that compromises	notice	breach of the	notice; or	treatment of	(b) Except as
	An individual	Guam, when the	the security or	requirement: No.	security of the	(4) Substitute	personal	provided by § 48.40
	"means a natural	data elements are	confidentiality of		system as soon as	notice, if the	information and	of this Chapter, the
	person."	neither encrypted	personal		practicable	individual or the	that are consistent	Office of the
	(§48.20(e))	nor redacted:	information		following	entity required to	with the timing	Attorney General
	T 414	(1) Social Security	maintained by an		discovery."	provide notice	requirements of this	shall have exclusive
	Entity:	number;	individual or entity		(§48.30(c))	demonstrates that	Chapter shall be	authority to bring
	An entity "includes	(2 )Driver's license	as part of a database		Delen	the cost of	deemed to be in	action and may
	corporations, business trusts,	number or Guam identification card	of personal information		<b>Delay</b> : "Notice required by	providing notice will exceed Ten	compliance with the notification	obtain either actual damages for a
	estates,	number issued in	regarding multiple		this section may be	Thousand Dollars	requirements of this	violation of this
	partnerships,	lieu of a driver's	individuals and that		delayed if a law	(\$10,000), or that	Chapter if it notifies	Chapter or a civil
	limited	license; or	causes, or the		enforcement agency	the affected class of	residents of Guam	penalty not to
	partnerships,	(3) Financial	individual or entity		determines and	residents to be	in accordance with	exceed One
	limited liability	account number, or	reasonably believes		advises the	notified exceeds	its procedures in the	Hundred Fifty
	partnerships,	credit card or debit	has caused or will		individual or entity	five thousand	event of a breach of	Thousand Dollars
	limited liability	card number, in	cause, identity theft		that the notice will	(5,000) persons, or	security of the	(\$150,000) per
	companies,	combination with	or other fraud to		impede a criminal	that the individual	system."	breach of the
	associations,	any required	any resident of		or civil	or the entity does	(§48.40(a))	security of the
	organizations, joint	security code,	Guam."		investigation, or	not have sufficient		system or series of
	ventures,	access code, or	(§48.20(a))		homeland or	contact information	For following	breaches of a
	governments,	password that			national security.	or consent to	interagency	similar nature that
	governmental	would permit	Exception:		Notice required by	provide notice as	guidelines: Yes.	are discovered in a
	subdivisions,	access to a	"Good faith		this section must be	described in	"(1) A financial	single
	agencies, or	resident's financial	acquisition of		made without	paragraphs 1, 2, or	institution that	investigation."
	instrumentalities, or	accounts."	personal		unreasonable delay	3."	complies with the	(§48.50)
	any other legal	(§48.20(f))	information by an		after the law	(§48.20(g))	notification	



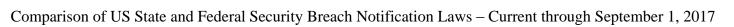
				Guam				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	entity, whether for profit or not-for-profit." (§48.20(b))  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	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))	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))  Risk of harm analysis: No.		enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security." (§48.30(d))	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))	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))	Private right of action: No.

	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))										





				Hawaii				
State Statute	What entities are covered? Is	What data are covered?	Has there been a breach? Is there	Who receives notice?	When must notice be given? May	How must notice be given? Is	Is there an exemption or	Enforcement? Penalties? Is
	there a requirement for service		a risk of harm analysis?		notice be delayed?	substitute notice permitted?	safe harbor?	there a private right of action?
	providers?							
Hawaii Rev. Stat.	Covered entities:	Personal	Breach definition:	Affected persons:	Timing:	Method:	For establishing	State enforcement:
§487N-1 et seq.	"Any business that	information:	A "security breach"	Notice must be	"The disclosure	"[N]notice to	own notification	"Any business that
	owns or licenses	"[A]n individual's	is "an incident of	given to the "affected	notification shall be	affected persons	method: No.	violates any
	personal	first name or first	unauthorized access	person."	made without	may be provided by		provision of this
	information of	initial and last	to and acquisition of	(§487N-2(a))	unreasonable delay,	one of the following	For following	chapter shall be
	residents of	name in	unencrypted or	G 114	consistent with the	methods:	interagency	subject to penalties
	Hawaii, any	combination with	unredacted records	Credit reporting	legitimate needs of	(1) Written notice to	guidelines: Yes.	of not more than
	business that conducts business	any one or more of	or data containing	agency and	law enforcement as	the last available address the business	"The following shall be deemed in	\$2,500 for each violation. The
	in Hawaii that	the following data elements, when	personal information where	government notice requirements: Yes.	provided in [§487N-2(c)], and consistent	or government	compliance with	attorney general or
	owns or licenses	either the name or	illegal use of the	"In the event a	with any measures	agency has on	[the Hawaii statute]:	the executive
	personal	the data elements	personal	business provides	necessary to	record;	(1) A financial	director of the office
	information in any	are not encrypted:	information has	notice to more than	determine sufficient	(2) Electronic mail	institution that is	of consumer
	form (whether	(1) Social security	occurred, or is	one thousand persons	contact information,	notice, for those	subject to the	protection may
	computerized,	number;	reasonably likely to	at one time pursuant	determine the scope	persons for whom a	Federal Interagency	bring an action
	paper, or	(2) Driver's	occur and that	to this section, the	of the breach, and	business or	Guidance on	pursuant to this
	otherwise), or any	license number or	creates a risk of	business shall notify	restore the reasonable	government agency	Response Programs	section."
	government	Hawaii	harm to a person.	in writing, without	integrity, security,	has a valid	for Unauthorized	(§487N-3(a))
	agency that	identification card	Any incident of	unreasonable delay,	and confidentiality of	electronic mail	Access to Consumer	
	collects personal	number; or	unauthorized access	the State of Hawaii's	the data system."	address and who	Information and	Private right of
	information for	(3) Account	to and acquisition of	office of consumer	(§487N-2(a))	have agreed to	Customer Notice	action: Yes.
	specific	number, credit or	encrypted records or	protection and all	n.	receive	published in the	"[A]ny business that
	government	debit card number,	data containing	consumer reporting	Delay:	communications	Federal Register on	violates any
	purposes." (§487N-2(a))	access code, or password that	personal information along	agencies that compile and maintain files on	Notice "shall be delayed if a law	electronically if the notice provided is	March 29, 2005 by the Board of	provision of this chapter shall be
	(946/1N-2(a))	would permit	with the	consumers on a	enforcement agency	consistent with the	Governors of the	liable to the injured
	Service provider	access to an	confidential process	nationwide basis, as	informs the business	provisions regarding	Federal Reserve	party in an amount
	requirement:	individual's	or key constitutes a	defined in 15 U.S.C.	or government	electronic records	System, the Federal	equal to the sum of
	Yes. "Any	financial account."	security breach."	section 1681a(p), of	agency that	and signatures for	Deposit Insurance	any actual damages
	business located in	(§487N-1)	(§487N-1)	the timing,	notification may	notices legally	Corporation, the	sustained by the
	Hawaii or any	,	/ · · · · · · · · · · · · · · · · · · ·	distribution, and	impede a criminal	required to be in	Office of the	injured party as a
	business that	Exception:	Exception:	content of the	investigation or	writing set forth in	Comptroller of the	result of the
	conducts business	Personal	"Good faith	notice."	jeopardize national	15 U.S.C. section	Currency, and the	violation. The court
	in Hawaii that	information "does	acquisition of	(§487N-2(f))	security and requests	7001;	Office of Thrift	in any action
	maintains or	not include	personal		a delay; provided that	(3) Telephonic	Supervision, or	brought under this
	possesses records	publicly available	information by an		such request is made	notice, provided that	subject to 12 C.F.R.	section may award
	or data containing	information that is	employee or agent		in writing, or the	contact is made	Part 748, and any	reasonable



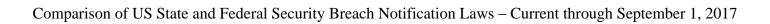


	Hawaii											
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice permitted?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?				
	requirement for	lawfully made available to the general public from federal, state, or local government records." (§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		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					
	following discovery of the breach, consistent with the legitimate needs of law enforcement." (§487N-2(b))		information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person." (§487N-1)		communicates to the business or government agency its determination that notice will no longer impede the investigation or jeopardize national security."  (§487N-2(c))	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))	Portability and Accountability Act of 1996." (§487N-2(g))					



	Hawaii											
req	hat entities covered? Is there a quirement 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?				
						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))  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						

				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))		

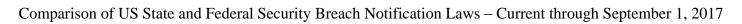




				Idaho				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Id. Code Ann.	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:
§28-51-104 et	"A city, county or	information:	"Breach of the	The "affected Idaho	"Notice must be made	"Notice' means:	own notification	"In any case in
seq.	state agency,	"Idaho resident's	security of the	resident."	in the most expedient	(a) Written notice to	method: Yes.	which an agency's,
	individual or a	first name or first	system' means the	(§28-51-105(1))	time possible and	the most recent	"An agency,	commercial entity's
	commercial entity	initial and last	illegal acquisition of		without unreasonable	address the agency,	individual or a	or individual's
	that conducts	name in	unencrypted	Credit reporting	delay, consistent with	individual or	commercial entity	primary regulator
	business in Idaho	combination with	computerized data	agency requirement:	the legitimate needs	commercial entity	that maintains its	has reason to believe
	and that owns or	any one (1) or	that materially	No.	of law enforcement	has in its records;	own notice	that an agency,
	licenses	more of the	compromises the		and consistent with	(b) Telephonic	procedures as part of	individual or
	computerized data	following data	security,	Government notice	any measures	notice;	an information	commercial entity
	that includes	elements that	confidentiality, or	requirement: Yes.	necessary to	(c) Electronic	security policy for	subject to that
	personal information about	relate to the resident, when	integrity of personal information for one	"When an agency becomes aware of a	determine the scope of the breach, to	notice, if the notice provided is	the treatment of personal	primary regulator's jurisdiction under
	a resident of	either the name or	(1) or more persons	breach of the security	identify the	consistent with the	information, and	section 28-51-
	Idaho."	the data elements	maintained by an	of the system, it shall,	individuals affected,	provisions regarding	whose procedures	104(6), Idaho Code,
	(§28-51-105(1))	are not encrypted:	agency, individual	within twenty-four	and to restore the	electronic records	are otherwise	has violated section
	(§20-31-103(1))	(a) Social security	or a commercial	(24) hours of such	reasonable integrity	and signatures set	consistent with the	28-51-105, Idaho
	Service provider	number:	entity."	discovery, notify the	of the computerized	forth in 15 U.S.C.	timing requirements	Code, by failing to
	requirement: Yes.	(b) Driver's	(§28-51-104(2))	office of the Idaho	data system."	section 7001; or	of section 28-51-	give notice in
	"An agency,	license number or	(320 01 10 (2))	attorney general."	(§28-51-105(1))	(d) Substitute notice,	105, Idaho Code, is	accordance with that
	individual or a	Idaho	Exception:	(§28-51-105(1))	( ) //	if the agency,	deemed to be in	section, the primary
	commercial entity	identification card	A breach does not		Delay:	individual or the	compliance with the	regulator may bring
	that maintains	number; or	include "[g]ood		Notice "may be	commercial entity	notice requirements	a civil action to
	computerized data	(c) Account	faith acquisition of		delayed if a law	required to provide	if the agency,	enforce compliance
	that includes	number, or credit	personal information		enforcement agency	notice demonstrates	individual or the	with that section and
	personal	or debit card	by an employee or		advises the agency,	that the cost of	commercial entity	enjoin that agency,
	information that	number, in	agent of an agency,		individual or	providing notice	notifies affected	individual or
	the agency,	combination with	individual or a		commercial entity	will exceed twenty-	Idaho residents in	commercial entity
	individual or the	any required	commercial entity		that the notice will	five thousand	accordance with its	from further
	commercial entity	security code,	for the purposes of		impede a criminal	dollars (\$25,000), or	policies in the event	violations. Any
	does not own or	access code, or	the agency,		investigation. Notice	that the number of	of a breach of	agency, individual
	license shall give	password that	individual or the		must be made in	Idaho residents to be	security of the	or commercial entity
	notice to and	would permit	commercial entity."		good faith, without	notified exceeds	system."	that intentionally
	cooperate with the owner or licensee	access to a resident's financial	(§28-51-104(2))		unreasonable delay and as soon as	fifty thousand (50,000), or that the	(§28-51-106(1))	fails to give notice in accordance with
	of the information	account."			possible after the law	agency, individual		section 28-51-105,
	of any breach of	(§28-51-104(5))			enforcement agency	or the commercial		Idaho Code, shall be
	of ally breach of	(820-31-104(3))		l	emorcement agency	or the commercial	l	Tuano Coue, shall be

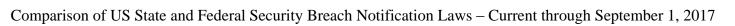


				Idaho				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	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 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))
								action: No.



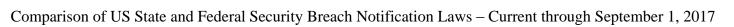


				Illinois				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
815 Ill. Comp. Stat. 530/1 et seq.	Covered entities: "Any data collector that owns or licenses personal information concerning an Illinois resident." (815 ILCS 530/10(a))  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)  The requirements also expressly	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	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)  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)	Residents: Illinois residents. (815 ILCS 530/10(a))  Credit reporting agency notice requirement: No.  Government notice requirement: No.	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))  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))	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."	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))  For following interagency guidelines: Yes. "Any covered entity or business	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
	apply to any "[s]tate agency	number, or an account number or				(815 ILCS 530/10(c))	associate that is subject to and in	impose an additional civil



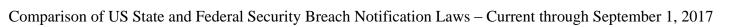


				Illinois				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	that collects personal information concerning an Illinois resident." (815 ILCS 530/12)  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))	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 or biometric data. OR (2) user name or email address, in combination with	Risk of harm analysis: No, except as definition of "breach" may incorporate elements of such a test.			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))	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	penalty of up to \$10,000 for each violation. (815 ILCS 530/20; 505/7)  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)





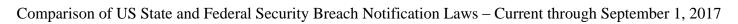
		Illinois				
What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
password or curity question and answer that ould permit occus to an online occunt, when there the user ame or email ddress or assword or curity question and answer are not acrypted or dacted or are acrypted or dacted but the eys to unencrypt or unredact or herwise read the ata elements have been obtained rough the breach of security."  Medical formation means any information garding an dividual's edical history, ental or physical ondition, or edical treatment of diagnosis by a calthcare of society and the or of				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 of 'per	days of notifying the Secretary." (815 ILCS 530/50)	
—pecto ocception de la contra del contra de la contra del la contra	assword or urity question I answer that uld permit tess to an online tount, when her the user he or email lifess or sword or urity question I answer are not trypted or acted or are trypted or acted but the test to unencrypt unredact or erwise read the a elements have the obtained tough the breach the security." 5 ILCS 530/5) Itedical formation means the properties of the security	assword or urity question I answer that uld permit tess to an online tount, when ner the user ne or email thress or stword or urity question I answer are not trypted or acted or are trypted or acted but the test to unencrypt tunredact or erwise read the a elements have en obtained tough the breach tough the breach to obtained to unencrypt touries or to obtained to unencrypt touries or to obtained to unencrypt touries or tourity question to end to obtained to unencrypt touries or tourity question to end to obtained to unencrypt touries or tourity question to end to obtained to unencrypt touries or tourity question to end to obtained to unencrypt touries or tourity question to end to obtained to unencrypt touries or tourity question to end to obtained to unencrypt touries or tourity question to end to obtained to unencrypt touries or tourity question to end to obtained to unencrypt touries or to	Anat data are covered?  It sthere a risk of harm analysis?  It assword or urity question answer that uld permit less to an online count, when her the user me or email litress or sword or urity question answer are not expeted or are expeted or acted but the sto unencrypt corrected or acted but the store and the store acted but the stor	That data are covered?    Has there been a breach? Is there a risk of harm analysis?   Who receives he given? May notice be delayed?	That data are covered?  It here been a breach? Is there a risk of harm analysis?  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 rewise read the a elements have en obtained ough the breach security;"  It cledical ormation means by information mans in vidual's dicial bristory, intal or physical diction, or dicial treatment diagnosis by a lthicare feessional,	And data are covered?  Is there a breach? Is there a risk of harm analysis?  Is there an office be delayed?  Is there an exemption or safe harbor?  Include, but need not be limited to information as defined in [815]  ILCS 530/5) in paragraph (1) of the definition of personal information?  ILCS 530/5) tedical or means the red activity information and website address for the Federal Trade Commission, and website address for the Federal Trade Commission, and website address for the Federal Trade Commission, and security, "61 ILCS 530/5] in paragraph (1) of the definition of personal information and defresses for the Federal Trade Commission, and website address for the Federal Trade Commission, and (C) a statement that the individual can obtain information arding an information arding an information of information arding an information arting an information are informa





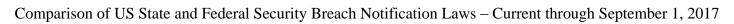
				Illinois				
State Statute	What entities are covered? Is there a	What data are covered?	Has there been a breach? Is there a risk of harm	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private
	requirement for service		analysis?			available?		right of action?
	providers?							
	providers.	information				may be provided in		
		provided to a				electronic or other		
		website or mobile				form directing the		
		application." (815				Illinois resident		
		ILCS 530/5)				whose personal		
						information has		
		**Health				been breached to		
		insurance				promptly change his		
		information means				or her user name or		
		"an individual's				password and		
		health insurance				security question or		
		policy number or subscriber				answer, as applicable, or to		
		identification				take other steps		
		number, any				appropriate to		
		unique identifier				protect all online		
		used by a health				accounts for which		
		insurer to identify				the resident uses the		
		the individual, or				same user name or		
		any medical				email address and		
		information in an				password or		
		individual's health				security question		
		insurance				and answer.		
		application and				The notification		
		claims history,				shall not, however,		
		including any				include information		
		appeals records." (815 ILCS 530/5)				concerning the number of Illinois		
		(813 ILCS 330/3)				residents affected		
		Exception:				by the breach."		
		"[D]oes not				(815 ILCS		
		include publicly				530/10(a))		
		available						
		information that is						
		lawfully made						
		available to the						
		general public						
		from federal,						

				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)						





				Indiana				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?			available?		right of action?
	service							
	providers?							
Ind. Code §24-	Covered entities:	Personal	Breach definition:	Residents:	Timing: "A person	Method:	For establishing	State enforcement:
4.9	A "data base	information:	"Breach of the	Any "Indiana resident	required to make a	"Except as provided	own notification	"(a) A person that is
	owner," defined as	"(1) a Social	security of data'	whose:	disclosure or	in [§24-4.9-3-4(b)	method: Yes, as	required to make a
	"a person that	Security number	means unauthorized	(1) unencrypted	notification under this	("substitute	long as the privacy	disclosure or
	owns or licenses	that is not	acquisition of	personal information	chapter shall make	notice")], a data	policy is at least as	notification in
	computerized data	encrypted or	computerized data	was or may have	the disclosure or	base owner required	stringent as the	accordance with IC
	that includes	redacted; or	that compromises	been acquired by an	notification as soon	to make a disclosure	disclosure required	24-4.9-3 and that
	personal	(2) an individual's	the security,	unauthorized person;	as possible after:	under this chapter	by the Indiana	fails to comply with
	information."	first and last	confidentiality, or	or	(1) delay is no longer	shall make the	statute or the federal	any provision of this
	(§24-4.9-2-3)	names, or first	integrity of personal	(2) encrypted	necessary to restore	disclosure using one	statutes listed	article commits a
		initial and last	information	personal information	the integrity of the	(1) of the following	below.	deceptive act that is
	Service provider	name, and one or	maintained by a	was or may have	computer system or	methods:	(§24-4.9-3-4(c))	actionable only by
	requirement:	more of the	person."	been acquired by an	to discover the scope	(1) Mail.		the attorney general
	Yes. "A person	following data	(§24-4.9-2-2(a))	unauthorized person	of the breach; or	(2) Telephone.	For following	under this chapter.
	that maintains	elements that are		with access to the	(2) the attorney	(3) Facsimile (fax).	interagency	(b) A failure to
	computerized data	not encrypted or	"Breach includes	encryption key."	general or a law	(4) Electronic mail,	guidelines: Yes.	make a required
	but that is not a	redacted:	the unauthorized	(§24-4.9-3-1(a))	enforcement agency	if the data base	"A data base	disclosure or
	data base owner	(A) A driver's	acquisition of	·	notifies the person	owner has the	owner that	notification in
	shall notify the	license number;	computerized data	Credit reporting	that delay will no	electronic mail	maintains its own	connection with a
	data base owner if	(B) A state	that have been	agency notice	longer impede a	address of the	disclosure	related series of
	the person	identification	transferred to	requirement: Yes.	criminal or civil	affected Indiana	procedures as part	breaches of the
	discovers that	card number;	another medium,	"A data base owner	investigation or	resident."	of an information	security of a system
	personal	(C) A credit card	including paper,	required to make a	jeopardize national	(§24-4.9-3-4)(a))	privacy, security	constitutes one (1)
	information was or	number; or	microfilm, or a	disclosure under	security."	G 1 44 4 4	policy, or	deceptive act."
	may have been	(D) A financial	similar medium,	[§24-4.9-3-1(a)] to	(§24-4.9-3-3(b))	Substitute notice:	compliance plan	(§24-4.9-4-1)
	acquired by an	account number	even if the	more than one	" A	"If a data base	under	Penalties:
	unauthorized person."	or debit card number in	transferred data are no longer in a	thousand (1,000) consumers shall also	"A person required to make a disclosure or	owner required to make a disclosure	(1) The federal USA Patriot Act	"The attorney
	(§24-4.9-3-2)	combination with	computerized	disclose to each	notification under this	under this chapter is	(P.L. 107-56);	general may bring
	(824-4.9-3-2)	a security code,	format."	consumer reporting	chapter shall make	required to make the	(2) Executive	an action under this
		password, or		agency (as defined in	the disclosure or	disclosure to more	Order 13224;	chapter to obtain
		access code that	(§24-2.9-2-2(a))	15 U.S.C. 1681a(p))	notification without	than five hundred	(3) The federal	any or all of the
		would permit	Exception:	information	unreasonable delay.	thousand (500,000)	Driver's Privacy	following:
		access to the	Breach does not	necessary to assist the	For purposes of this	Indiana residents, or	Protection Act (18	(1) An injunction to
		person's	include the "[g]ood	consumer reporting	section, a delay is	if the data base	U.S.C. 2781 et	enioin future
		account."	faith acquisition of	agency in preventing	reasonable if the	owner required to	seq.);	violations of this
		(§24-4.9-2-10)	personal	fraud, including	delay is:	make a disclosure	(4) The federal	section.
		(827-7.7-2-10)	information by an	personal information	(1) necessary to	under this chapter	Fair Credit	(2) A civil penalty
	1	l	information by an	personal information	(1) necessary to	under tills chapter	ran Cicuit	(2) A CIVII Pellatty

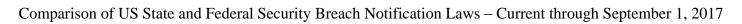




				Indiana				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		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)	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))  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."	of an Indiana resident affected by the breach of the security of a system." (§24-4.9-3-1(b))  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))	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))	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))	Reporting Act (15 U.S.C. 1681 et seq.); (5) The federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or (6) The federal Health Insurance Portability and Accountability Act (HIPAA) (P.L.104-191); 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	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)  Private right of action: No. Violations are "actionable only by the attorney general." (\$24-4.9-4-1)

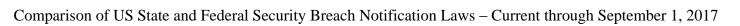


				Indiana				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?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





				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 et seq.	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))  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	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,	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))  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	Affected consumers: To "any consumer whose personal information was included in the information that was breached." (§715C.2(1))  Consumers: A "consumer" means any Iowa resident. (§715C.1(2))  Credit reporting agency notice requirement: No.  Government notice requirement: No.	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))  Delay: "The consumer notification requirements of this section may be delayed if a law enforcement agency determines that the notification will impede a criminal	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	For establishing own notification method: No.  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 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))  "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))  Private right of action: No, although the attorney general may seek damages on behalf of person
	or commercial entity."	credit card number, or debit	threat to the security,		investigation and the agency has made a	thousand dollars, that the affected	state or federal law that provides greater	injured by a violation.

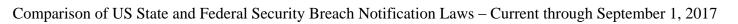




	Iowa											
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice 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 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))				



	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))					

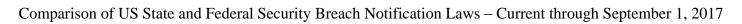




	Kansas										
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?			
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is			
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private			
	requirement for		analysis?			available?		right of action?			
	service		·								
	providers?										
Kansas Stat. §50-	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:			
7a01 <i>et seq</i> .	"A person that	information:	A security breach	Affected Kansas	After an	"'Notice' means:	own notification	"For violations of			
	conducts business	"[A] consumer's	means "the	residents.	investigation,	(1) Written notice;	method: Yes.	this section, except			
	in [Kansas], or a	first name or first	unauthorized access	(§50-7a02(a))	"[n]otice must be	(2) electronic	"[A]n individual or	as to insurance			
	government,	initial and last	and acquisition of		made in the most	notice, if the notice	a commercial entity	companies licensed			
	governmental	name linked to any	unencrypted or	Credit reporting	expedient time	provided is	that maintains its	to do business in			
	subdivision or	one or more of the	unredacted	agency notice	possible and without	consistent with the	own notification	[Kansas], the			
	agency that owns	following data	computerized data	requirement: Yes.	unreasonable delay,	provisions regarding	procedures as part	attorney general is			
	or licenses	elements that	that compromises	If notice must be	consistent with the	electronic records	of an information	empowered to bring			
	computerized data that includes	relate to the consumer, when	the security, confidentiality or	given to "more than 1.000 consumers at	legitimate needs of law enforcement and	and signatures set forth in 15 U.S.C. §	security policy for the treatment of	an action in law or equity to address			
	personal	the data elements	integrity of personal	one time, the person	consistent with any	7001; or	personal	violations of this			
	information."	are neither	information	shall also notify,	measures necessary	(3) substitute notice.	information, and	section and for other			
	(§50-7a02(a))	encrypted or	maintained by an	without unreasonable	to determine the	if the individual or	whose procedures	relief that may be			
	(\$30-7402(a))	redacted:	individual or a	delay, all consumer	scope of the breach	the commercial	are otherwise	appropriate. The			
	Service provider	(1) Social security	commercial entity	reporting agencies	and to restore the	entity required to	consistent with the	provisions of this			
	requirement:	number;	and that causes, or	that compile and	reasonable integrity	provide notice	timing requirements	section are not			
	Yes. "An	(2) driver's license	such individual or	maintain files on	of the computerized	demonstrates that	of this section, is	exclusive and do not			
	individual or a	number or state	entity reasonably	consumers on a	data system."	the cost of	deemed to be in	relieve an individual			
	commercial entity	identification card	believes has caused	nationwide basis	(§50-7a02(a))	providing notice	compliance with the	or a commercial			
	that maintains	number; or	or will cause,	of the timing,		will exceed	notice requirements	entity subject to this			
	computerized data	(3) financial	identity theft to any	distribution and	Delay:	\$100,000, or that	of this section if the	section from			
	that includes	account number or	consumer."	content of the	Notice "may be	the affected class of	individual or the	compliance with all			
	personal	credit or debit card	(§50-7a01(h))	notices."	delayed if a law	consumers to be	commercial entity	other applicable			
	information that	number, alone or		(§50-7a02(f))	enforcement agency	notified exceeds	notifies affected	provisions of law."			
	the individual or	in combination	Exception:		determines that the	5,000, or that the	consumers in	(§50-7a02(g))			
	the commercial	with any required	"Good faith	Government notice	notice will impede a	individual or the	accordance with its	"For violations of			
	entity does not own or license	security code, access code or	acquisition of personal	requirement: No.	criminal investigation."	commercial entity does not have	policies in the event of a breach of	the law by an insurance company			
	shall give notice to	password that	information by an		(§50-7a02(c))	sufficient contact	security of the	licensed to do			
	the owner or	would permit	employee or agent		(\$30-7a02(c))	information to	system."	business in			
	licensee of the	access to a	of an individual or a			provide notice."	(§50-7a02(d))	[Kansas], the			
	information of any	consumer's	commercial entity			(§50-7a01(c))	(350 / 1102(11))	insurance			
	breach of the	financial account."	for the purposes of			(320 / 401(0))	For following	commissioner shall			
	security of the data	(§50-7a01(g))	the individual or the			Substitute notice:	interagency	have the sole			
	following	(0 1 1 1 1 1 6 )	commercial entity is			"Substitute' notice	guidelines: Yes.	authority to enforce			
	discovery of a		not a breach of the			means:	"An individual or a	the provisions of			
	breach, if the		security of the			(1) E-mail notice if	commercial entity	this section."			



	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.			

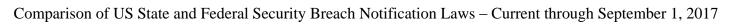




Kentucky										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?		
KRS §365.732	Covered entities: Any "information holder," defined as "any person or business entity that conducts business in [Kentucky]." (§365.732(1)(b))  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	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: 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))	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))  Exception: "Good faith acquisition of personally	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))  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))	Timing: Notification shall be made "in in the most expedient time possible and without unreasonable delay." (§365.732(2))  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))	Method:  "[N]otice may be provided by one (1) of the following methods:  (a) Written notice; (b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. sec. 7001; or (c) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the information holder does not have sufficient contact information." (§365.732(5))	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))  For following interagency guidelines: Yes. Does not apply to "any person who is subject to the provisions of Title	Penalties: Not specified.  Private right of action: No.		



	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))		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))  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))	Government notice requirement: No.		Substitute notice: "Substitute notice shall consist of all of the following:  1. E-mail notice, when the information holder has an e-mail address for the subject persons;  2. Conspicuous posting of the notice on the information holder's Internet Web site page, if the information holder maintains a Web site page; and  3. Notification to major statewide media."  (§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))				

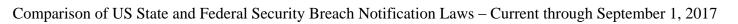




Louisiana									
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?	
La. Rev. Stat. Ann. §51:3071 et seq.; La. Admin. Code tit. 16, pt. III, §701.	providers?  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))  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))  Service provider requirement: Yes. "Any agency or person that maintains computerized data that includes	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))  Exception: Does not "include publicly available information that is lawfully made available to the	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))  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 system, provided that the personal information is not used for, or is subject to, unauthorized	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))  Credit reporting agency notice requirement: No.  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	Timing: Notice to residents "shall be made in the most expedient time possible and without unreasonable delay." (R.S. 51:3074(C))  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))	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))	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))  For following interagency guidelines: Yes. "A financial institution that is	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))  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)	

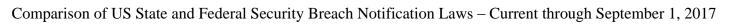


	Louisiana										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice 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)				





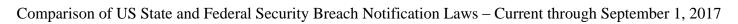
	Maine										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?			
Maine Rev. Stat. Ann. tit. 10, §1346 et seq.	Covered entities: "[A]n information broker that maintains computerized data that includes personal information." (§1348(1)(A))  Information broker: 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))	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	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))  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	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))  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	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))  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))	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))	For establishing own notification method: No.  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))	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))  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))			





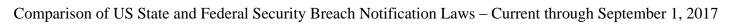
	Maine										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?			
	* 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))  Exception: Information broker "does not include a governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes." (§1347(3))	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))  Exception: Personal information "does not include information from 3rd-party claims databases maintained by property and casualty insurers or publicly available information that is	disclosure to another person." (§1347(1))  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))	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))  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))		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))		Private right of action: No.			

				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))						



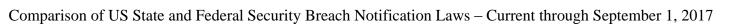


	Maryland										
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?			
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is			
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private			
	requirement for		analysis?			available?		right of action?			
	service		J					8			
	providers?										
Maryland Code	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:			
Ann., Com. Law.	"[A] business*	information:	A "breach of the	"[A]n individual	Notice "shall be	"The [required]	own notification	A violation is			
§14-3501 et seq.;	that owns or	Personal	security of a	residing in	given as soon as	notification may	method: No.	considered an			
H.B. 974	licenses	Information means	system' means the	[Maryland]."	reasonably	be given:		"unfair or deceptive			
(effective January	computerized data	"(i) [a]n	unauthorized	(§14-3504(b)(1))	practicable, but not	(1) By written	For following	trade practice" and			
1, 2018)	that includes	individual's first	acquisition of		later than 45 days	notice sent to the	interagency	is enforced pursuant			
	personal	name or first	computerized data	Credit reporting	after the business	most recent address	guidelines: Yes.	to Maryland's			
	information of an	initial and last	that compromises	agency notice	concludes the	of the individual in	"(1) A business	Consumer			
	individual residing	name in	the security,	requirement: Yes.	investigation required	the records of the	that complies with	Protection Act (§13-			
	in the State"	combination with	confidentiality, or	"If a business is	under	business;	the requirements for	101 et seq.), which			
	(§14-3504(b)(1))	any one or more of	integrity of the	required under § 14–	[§14-3504(b)(1)]."	(2) By electronic	notification	authorizes actions			
	*"D	the following data	personal	3504 of this subtitle	(§14-3504(b)(3))	mail to the most	procedures, the	by the Attorney			
	*"Business'	elements, when	information	to give notice of a	Delam	recent electronic	protection or	General.			
	means a sole	the name or the	maintained by a business."	breach of the security of a system to 1,000	Delay:	mail address of the individual in the	security of personal	(§14-3508)			
	proprietorship,	data elements are	(§14-3504(a)(1))	or more individuals,	"(1) The [required] notification may	records of the	information, or the destruction of	Private right of			
	partnership, corporation,	not encrypted, redacted, or	(§14-3304(a)(1))	the business also	be delayed:	business, if:	personal	action: Yes.			
	association, or any	otherwise	Exception:	shall notify, without	(i) If a law	(i)the recipient	information under	Maryland's			
	other business	protected by	Breach "does not	unreasonable delay,	enforcement agency	has expressly	the rules,	Consumer			
	entity, whether or	another method	include the good	each consumer	determines that the	consented to	regulations,	Protection Act (§13-			
	not organized to	that renders the	faith acquisition of	reporting agency that	notification will	receive electronic	procedures, or	101 et seq.) states			
	operate at a profit	information	personal	compiles and	impede a criminal	notices; or	guidelines	that "any person			
	[and] includes a	unreadable or	information by an	maintains files on	investigation or	(ii) the business	established by the	may bring an action			
	financial	unusable:	employee or agent	consumers on a	jeopardize	conducts its	primary or	to recover for injury			
	institution	1. A Social	of a business for the	nationwide basis, as	homeland or	business primarily	functional federal or	or loss sustained by			
	organized,	Security number,	purposes of the	defined by 15 U.S.C.	national security; or	through Internet	State regulator of	him as the result of			
	chartered,	an Individual	business provided	§ 1681a(p), of the	(ii) To determine the	account	the business shall be	a [prohibited]			
	licensed, or	Taxpayer	that the personal	timing, distribution,	scope of the breach	transactions or the	deemed to be in	practice."			
	otherwise	Identification	information is not	and content of the	of the security of a	Internet;	compliance	(See §14-3508)			
	authorized under	Number, a	used or subject to	notices This	system, identify the	(3) By telephonic	(2) A business that				
	the laws of	passport number,	further unauthorized	section does not	individuals affected,	notice, to the most	is subject to and in				
	[Maryland], any	or other	disclosure."	require the inclusion	or restore the	recent telephone	compliance with				
	other state, the	identification	(§14-3504(a)(2))	of the names or other	integrity of the	number of the	Gramm-Leach-				
	United States, or	number issued by	D: 1 61	personal identifying	system.	individual in the	Bliley, the Fair and				
	any other country,	the federal	Risk of harm	information of	(2) If notification is	records of the	Accurate				
	and the parent or	government;	analysis: Yes "A business that	recipients of notices	delayed [it] shall be	business; or	Transactions Act,				
	subsidiary of a financial	(2. A driver's		of the breach of the	given as soon as	(4) By substitute	the Interagency				
	manciai	license number or	owns or licenses	security of a system."	reasonably	notice if:	Guidelines				



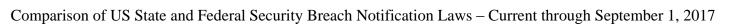


	Maryland										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?			
	institution." (§14-3501(b))  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))	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	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 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))	(§14-3506)  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))	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))	(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))  Substitute notice: "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))	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))				



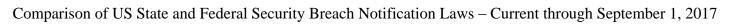


				Maryland				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; OR (ii) A user name or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account." (§14-3501(e)(1))  Exception: "Personal information' does not include: (i) Publicly	"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))			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 numbers and addresses for		





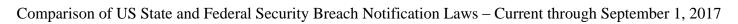
			Maryland				
State Statute What ent are covere there a requirement service	1? Is covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
provide	s?						
	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		





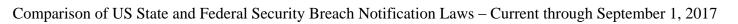
				Maryland				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	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))		





				Massachusett	S			
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Penalties? Is
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	there a private
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	right of action?
	requirement for		analysis?		v	available?		
	service		J					
	providers?							
Massachusetts	Covered entities:	Personal	Breach definition:	Notice must be	Timing:	Method:	For establishing	State enforcement:
Gen Laws ch.	"A person* or	information:	"Breach of	given to:	Notice shall be given	"Notice' shall	own notification	"The attorney
93H, §1, et seq.	agency that owns	Personal	security' [means]	The attorney	"as soon as	include:-	method: No.	general may bring
	or licenses data	information means	the unauthorized	general;	practicable and	(i) written notice;		an action pursuant
	that includes	"a resident's first	acquisition or	the director of	without unreasonable	(ii) electronic	For following	to section 4 of
	personal	name and last	unauthorized use of	consumer affairs and	delay."	notice, if notice	interagency	chapter 93A [the
	information about	name or first	unencrypted data or,	business regulation	(§3(b))	provided is	guidelines: Yes.	Massachusetts
	a resident of the	initial and last	encrypted*	and;		consistent with the	"[A] person who	Consumer
	commonwealth,	name in	electronic data and	the affected	Delay:	provisions regarding	maintains	Protection Act]
	shall provide	combination with	the confidential	Massachusetts	Delay is permitted "if	electronic records	procedures for	against a person or
	notice when	any 1 or more of	process or key that	resident.	a law enforcement	and signatures set	responding to a	otherwise to remedy
	such person or	the following data	is capable of	(§3(b))	agency determines	forth in § 7001 (c)	breach of security	violations of this
	agency (1) knows or has	elements that relate to such	compromising the security,	Credit reporting	that provision of such notice may impede a	of Title 15 of the United States Code;	pursuant to federal laws, rules,	chapter and for other relief that may
	reason to know of	resident:	confidentiality, or	agency and	criminal investigation	and chapter 110G;	regulations,	be appropriate."
	a breach of	(a) A Social	integrity of personal	government notice	and has notified the	or	guidance, or	(§6)
	security or	Security number;	information,	requirement: Yes.	attorney general, in	(iii) substitute	guidelines, is	(80)
	(2) when the	(b) A driver's	maintained by a	"The notice to be	writing, thereof and	notice, if the person	deemed to be in	Private right of
	person or agency	license number or	person or agency, or	provided to the	informs the person or	or agency required	compliance with	action: No.
	knows or has	state-issued	employee or agent	attorney general and	agency of such	to provide notice	this chapter if the	
	reason to know	identification card	thereof, that creates	said director, and	determination. If	demonstrates that	person notifies	
	that the personal	number;	a substantial risk of	consumer reporting	notice is delayed due	the cost of	affected	
	information of	(c) A financial	identity theft or	agencies or state	to such determination	providing written	Massachusetts	
	such resident was	account number,	fraud against a	agencies if any, shall	and as soon as the	notice will exceed	residents in	
	acquired or used	or credit or debit	resident of the	include, but not be	law enforcement	\$250,000, or that	accordance with the	
	by an	card number, with	commonwealth."	limited to, the nature	agency determines	the affected class of	maintained or	
	unauthorized	or without any	(§1(a))	of the breach of	and informs the	Massachusetts	required procedures	
	person or used for	required security	However, even if	security or	person or agency that	residents to be	when a breach	
	an unauthorized	code, access code,	there has not been a	unauthorized	notification no longer	notified exceeds	occurs; provided	
	purpose"	personal	"breach of security"	acquisition or use, the	poses a risk of	500,000 residents,	further that the	
	(§3(b))	identification	as defined by the	number of residents	impeding an	or that the person or	person also notifies	
	* Person:	number or password that	statute (with its "substantial risk of	of the commonwealth affected by such	investigation, notice shall be provided, as	agency does not have sufficient	the attorney general and the director of	
	"Person' means a	would permit	identity theft or	incident at the time of	soon as practicable	contact information	the office of	
	natural person,	access to a	fraud" threshold),	notification, and any	and without	to provide notice."	consumer affairs	
	corporation,	resident's financial	notification is still	steps the person or	unreasonable delay.	(§1(a))	and business	
	association,	account."	required if a person	agency has taken or	The person or agency	(0-(4))	regulation of the	
	partnership or	(§1(a))	that owns or	plans to take relating	shall cooperate with		breach as soon as	





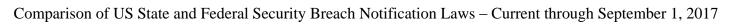
				Massachusett	S			
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Penalties? Is
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	there a private
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	right of action?
	requirement for		analysis?			available?		
	service							
	providers?							
	other legal entity."	Exception:	licenses data that	to the incident. Upon	law enforcement in	Substitute notice:	practicable and	
	(§1(a))	Personal	includes personal	receipt of [the]	its investigation of	"Substitute notice"	without	
		information does	information about a	notice, the director of	any breach of	shall consist of all	unreasonable delay	
	Service provider	not include	resident of the	consumer affairs and	security or	of the following:	following the	
	requirement:	information that	commonwealth	business regulation	unauthorized	(i) electronic mail	breach. The notice	
	Yes. "A person or	"is lawfully	"knows or has	shall identify any	acquisition or use,	notice, if the person	to be provided to	
	agency that	obtained from	reason to know that	relevant consumer	which shall include	or agency has	the attorney general	
	maintains or	publicly available	the personal	reporting agency or	the sharing of	electronic mail	and the director of	
	stores, but does	information or	information of such	state agency, as	information relevant	addresses for the	the office of	
	not own or license data that includes	from federal, state or local	resident was acquired or used by	deemed appropriate by said director, and	to the incident; provided however,	members of the affected class of	consumer affairs and business	
	personal	government	an unauthorized	forward the names of	that such disclosure	Massachusetts	regulation shall	
	information about	records lawfully	person or used for	the identified	shall not require the	residents;	consist of, but not	
	a resident of the	made available to	an unauthorized	consumer reporting	disclosure of	(ii) clear and	be limited to, any	
	commonwealth,	the general	purpose."	agencies and state	confidential business	conspicuous posting	steps the person or	
	shall provide	public."	(§3(b))	agencies to the	information or trade	of the notice on the	agency has taken or	
	notice, as soon as	(§1(a))	(6- (-7)	notifying person or	secrets."	home page of the	plans to take	
	practicable and	(0 ( ))	* Encrypted:	agency. Such person	(§4)	person or agency if	relating to the	
	without		Encrypted [means]	or agency shall, as		the person or	breach pursuant to	
	unreasonable		"transformation of	soon as practicable		agency maintains a	the applicable	
	delay, when such		data through the use	and without		website; and	federal law, rule,	
	person or agency		of a 128-bit or	unreasonable delay,		(iii) publication in	regulation, guidance	
	(1) knows or has		higher algorithmic	also provide notice,		or broadcast	or guidelines;	
	reason to know of		process into a form	in accordance with		through media or	provided further	
	a breach of		in which there is a	this chapter, to the		medium that	that if said person or	
	security or		low probability of	consumer reporting		provides notice	agency does not	
	(2) when the		assigning meaning	agencies and state		throughout the	comply with	
	person or agency knows or has		without use of a confidential process	agencies identified by the director of		commonwealth." (§1(a))	applicable federal laws, rules,	
	reason to know		or key, unless	consumer affairs and		(81(a))	regulations,	
	that the personal		further defined by	business regulation."		Notice contents	guidance or	
	information of		regulation of the	(§3(b))		requirement:	guidelines, then it	
	such resident was		department of	(85(0))		"The notice to be	shall be subject to	
	acquired or used		consumer affairs			provided to the	the provisions of	
	by an		and business			resident shall	this chapter."	
	unauthorized		regulation."			include, but not be	(§5)	
	person or used for		(§1(a))			limited to, the		
	an unauthorized					consumer's right to		



State Statute  What entities are covered? Is there a requirement for service providers?  Durpose, 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 person or agency, is not a  What entities are covered? Has there been a breach? Is there a risk of harm analysis?  When must notice be given? Is substitute notice available?  When must notice be given? Is substitute notice available?  State Statute  Who receives notice?  When must notice be given? Is substitute notice available?  State Statute  Who receives notice?  When must notice be given? Is substitute notice available?  State Statute  Who receives notice?  When must notice be given? Is substitute notice available?  State Statute  State Statute  Who receives notice?  When must notice be given? Is substitute notice available?  Substitute notice available?  State Statute  State Statute  State Statute  Is there an exemption or safe harbor?  Substitute notice available?  State Statute  Substitute notice available?  State Statute  Substitute notice available?	Penalties? Is there a private
purpose, to the owner or licensor in accordance with this chapter. In addition to provided herein, such person or agency, or employee or agent cooperate with the owner or licensor of such	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, or employee or agent cooperate with the owner or licensor of such person or agency, is not a such person or agency, is not a  providers?  Exception:  "A good faith but unauthorized consumer requests a security freeze and the necessary information of personal information by a person or agency, or employee or agent thereof, for the security freeze, and any fees required to be paid to any of the consumer reporting	
purpose, to the owner or licensor "A good faith but unauthorized this chapter. In acquisition of personal information by a providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such such person or agency, is not a such person or agency, is not a    Description: "A good faith but unauthorized consumer requests a security freeze and the necessary information to be 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	
owner or licensor in accordance with this chapter. In addition to personal information by a person or agency, or such person or agency shall cooperate with the owner or licensor of such  owner or licensor in accordance with tunauthorized 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  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	
in accordance with this chapter. In addition to personal information by a person or agency, or employee or agent security freeze, and cooperate with the owner or licensor of such consumer requests a security freeze and the necessary information to be person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not 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	
this chapter. In addition to personal information by a person or agency, or employee or agent cooperate with the owner or licensor of such such person or agency, is not 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	
addition to providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such  addition to personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a  the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting	
providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such  providing notice information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a  information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting	
as provided herein, such person or agency, or employee or agent thereof, for the agency shall cooperate with the owner or licensor of such agency, is not a provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting	
such person or agency shall cooperate with the owner or licensor of such of such  such person or agency shall thereof, for the lawful purposes of such person or agency, is not a  requesting the security freeze, and any fees required to be paid to any of the consumer reporting	
agency shall cooperate with the owner or licensor of such  thereof, for the lawful purposes of such person or agency, is not a  thereof, for the lawful purposes of such person or agency, is not a  security freeze, and any fees required to be paid to any of the consumer reporting	
cooperate with the owner or licensor of such lawful purposes of such lawful purposes of such person or agency, is not a lawful purposes of be paid to any of the consumer reporting	
owner or licensor of such person or agency, is not a be paid to any of the consumer reporting	
of such agency, is not a consumer reporting	
information. Such breach of security agencies, provided	
cooperation shall unless the personal however, that said	
include, but not be information is used notification shall	
limited to, in an unauthorized not include the	
informing the manner or subject to nature of the breach	
owner or licensor further unauthorized or unauthorized	
of the breach of disclosure." acquisition or use or	
security or (§1(a)) the number of	
unauthorized residents of the	
acquisition or use, the date or Risk of harm analysis: No. commonwealth affected by said	
of such incident security" occurs unauthorized access only when there is a or use."	
thereof, and any steps the person or steps the person of t	
agency has taken fraud," notice must	
or plans to take be given whenever a	
relating to the person that owns or	
incident, except licenses personal	
that such information about	
cooperation shall state residents	
not be deemed to "knows or has	
require the reason to know that	
disclosure of the personal	
confidential informationwas	

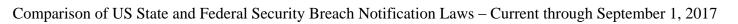


				Massachusett	ts			
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice 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))					



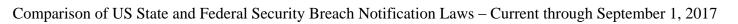


	Michigan									
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?		
Michigan Comp. Laws § 445.63, et seq.	providers?  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))  Person: "Person' means an individual, partnership, corporation, limited liability company, association, or other legal entity." (§3(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	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))	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))  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;	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))  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	Timing:  "A person or agency shall provide any notice required under this section without unreasonable delay." (§12(4))  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	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 at the recipient at the recipient at of the recipient at the recipient at the recipient at the recipient if 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	For establishing own notification method: No.  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	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)) "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))  Criminal penalties for false reporting:		
	the database that shall provide a notice to the		(iii) The employee or other individual did not misuse any	consumers on a nationwide basis." Requirement does	breach and restore the reasonable integrity of the database.	the person or agency reasonably believes that it has	adopted by the national credit union	"A person that provides notice of a security breach in		





				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 93 days or a fine of 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.





				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?
						subdivision (a) or (b) if the notice by telephone does not result in a live conversation between the individual representing the person or agency and the recipient within 3 business days after the initial attempt to provide telephonic notice. (d) Substitute notice, if the person or agency demonstrates that the cost of providing notice under subdivision (a), (b), or (c) will exceed \$250,000.00 or that the person or agency has to provide notice to more than 500,000 residents of this state." (§12(5))  Substitute notice: "Substitute notice must provide a telephone number or web address that an individual can		



				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?
						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))  * 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,		

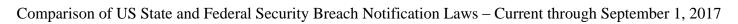
	Michigan											
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice 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))						



	Minnesota										
State Statute	What entities are covered? Is	What data are covered?	Has there been a breach? Is there	Who receives notice?	When must notice be given? May	How must notice be given? Is	Is there an exemption or	Penalties? Is there a private			
		covereu:	a risk of harm	nouce:		substitute notice	safe harbor?				
	there a				notice be delayed?		sale narbor:	right of action?			
	requirement for		analysis?			available?					
	service providers?										
Minn. Stat.	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:			
§325E.61	"Any person or	information:	A "breach of the	"[A]ny resident of	"The disclosure must	""[N]otice' may be	own notification	The Attorney			
	business that	"[A]n individual's	security of the	[Minnesota] whose	be made in the most	provided by one of	method: Yes.	General is given			
	conducts business	first name or first	system" is the	unencrypted personal	expedient time	the following	If a person or	enforcement power			
	in [Minnesota],	initial and last	"unauthorized	information was, or is	possible and without	methods:	business "maintains	to seek civil			
	and that owns or	name in	acquisition of	reasonably believed	unreasonable delay,	(1) written notice to	its own notification	penalties not to			
	licenses data that	combination with	computerized data	to have been,	consistent with the	the most recent	procedures as part	exceed \$25,000 and			
	includes personal	any one or more of	that compromises	acquired by an	legitimate needs of	available address	of an information	injunctive relief			
	information."	the following data	the security,	unauthorized person."	law enforcement, as	the person or	security policy for	under Minn. Stat.			
	(Subdiv. 1(a))	elements, when	confidentiality, or	(Subdiv. 1(a))	provided in [Subdiv.	business has in its	the treatment of	§8.31 (establishing			
		the data element is	integrity of personal		1(c)], or with any	records;	personal	the Attorney			
	Exception:	not secured by	information	Credit reporting	reasonable measures	(2) electronic	information and is	General's authority			
	The law "does not	encryption or	maintained by the	agency notice	necessary to	notice, if the	otherwise consistent	to investigate and			
	apply to any	another method of	person or the	requirement: Yes.	determine the scope	person's primary	with the timing	prosecute certain			
	'financial	technology that	business."	"If a person discovers	of the breach, identify	method of	requirements" under	illegal acts).			
	institution' as	makes electronic	(Subdiv. 1(d))	circumstances	the individuals	communication with	the law, then the	(Subdiv. 6)			
	defined by United States Code, title	data unreadable or unusable, or was	Exception:	requiring notification under this section of	affected, and restore the reasonable	the individual is by electronic means, or	person or business "shall be deemed to	Private right of			
	15. section	secured and the	"Good faith	more than 500	integrity of the data	if the notice	be in compliance	action: Yes.			
	6809(3)."	encryption key,	acquisition of	persons at one time,	system."	provided is	with the notification	"In addition to the			
	(Subdiv. 4)	password, or other	personal	the person shall also	(Subdiv. 1(a))	consistent with the	requirements of this	remedies otherwise			
	(Suburv. 1)	means necessary	information by an	notify, within 48	(Bubulli I(u))	provisions regarding	section if the person	provided by law,			
	Service provider	for reading or	employee or agent	hours, all consumer	Delay:	electronic records	or business notifies	any person injured			
	requirement:	using the data was	of the person or	reporting agencies	Delay is permitted if	and signatures in	subject persons in	by a violation [of			
	Yes. "Any person	also acquired:	business for the	that compile and	"a law enforcement	United States Code,	accordance with its	the state consumer			
	or business that	(1) Social Security	purposes of the	maintain files on	agency affirmatively	title 15, section	policies in the event	protection law] may			
	maintains data that	number;	person or business	consumers on a	determines that the	7001; or	of a breach of	bring a civil action			
	includes personal	(2) driver's license	is not a breach of	nationwide basis as	notification will	(3) substitute notice,	security of the	and recover			
	information that	number or	the security system,	defined by [15 USC	impede a criminal	if the person or	system."	damages, together			
	the person or	Minnesota	provided that the	1681a], of the timing,	investigation."	business	(Subdiv. 1(h))	with costs and			
	business does not	identification card	personal	distribution, and	(Subdiv. 1(c))	demonstrates that		disbursements,			
	own shall notify	number;	information is not	content of the		the cost of	For following	including costs of			
	the owner or	(3) account	used or subject to	notices."		providing notice	interagency	investigation and			
	licensee of the	number or credit	further unauthorized	(Subdiv. 2)		would exceed	guidelines: No, but	reasonable			
	information of any	or debit card	disclosure."			\$250,000, or that	the statute does not	attorney's fees, and			
	breach of the	number, in	(Subdiv. 1(d))			the affected class of	apply to "any	receive other			
	security of the data	combination with				subject persons to	'financial	equitable relief as			



	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)			

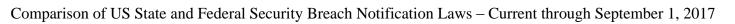




				Mississippi				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?		·	available?		right of action?
	service		·					
	providers?							
Miss. Code §75-	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:
24-29	"[A] any person	information:	"Breach of	"[A]ny individual	"[D]isclosure shall be	"Any notice	own notification	"Failure to comply
	who conducts	"Personal	security' means	who is a resident of	made without	required by the	method: Yes.	with the
	business in	information'	unauthorized	[Mississippi] whose	unreasonable delay."	provisions of this	"Any person who	requirements of this
	[Mississippi] and	means an	acquisition of	personal information	(§75-24-29(3))	section may be	conducts business in	section shall
	who, in the	individual's first	electronic files,	was, or is reasonably		provided by one (1)	[Mississippi] that	constitute an unfair
	ordinary course of	name or first	media, databases or	believed to have	Delay:	of the following	maintains its own	trade practice and
	the person's	initial and last	computerized data	been, intentionally	Delay is permitted	methods:	security breach	shall be enforced by
	business functions,	name in	containing personal	acquired by an	"for a reasonable	(a) written notice;	procedures as part	the Attorney
	owns, licenses or	combination with	information of any	unauthorized person	period of time if a	(b) telephone	of an information	General."
	maintains personal	any one or more of	resident of this state	through a breach of	law enforcement	notice;	security policy for	(§75-24-29(8))
	information of any	the following data	when access to the	security."	agency determines	(c) electronic notice,	the treatment of	D
	resident of	elements:	personal	(§75-24-29(2)(b)(iv))	that the notification	if the person's	personal	Private right of action: No.
	[Mississippi]."	(i) Social security	information has not	Credit reporting	will impede a	primary means of communication with	information, and	"[N]othing in this
	(§75-24-29(1))	number; (ii) Driver's	been secured by encryption or by	agency notice	criminal investigation or national security	the affected	otherwise complies with the timing	section may be
	Service provider	license number or	any other method or	requirement: No.	and the law	individuals is by	requirements of this	construed to create a
	requirement:	state identification	technology that	requirement. No.	enforcement agency	electronic means or	section, shall be	private right of
	Yes. "Any person	card number; or	renders the personal	Government notice	has made a request	if the notice is	deemed to be in	action."
	who conducts	(iii) An account	information	requirement: No.	that the notification	consistent with the	compliance with the	(§75-24-29(8))
	business in this	number or credit	unreadable or	requirement. 140.	be delayed. Any	provisions regarding	security breach	(\$13 24 25(0))
	state that	or debit card	unusable."		such delayed	electronic records	notification	
	maintains	number in	(§75-24-29(2)(a))		notification shall be	and signatures set	requirements of this	
	computerized data	combination with	(0.2		made after the law	forth in 15 USCS	section if the person	
	which includes	any required	Risk of harm		enforcement agency	7001; or	notifies affected	
	personal	security code,	analysis: Yes.		determines that	(d) substitute notice,	individuals in	
	information that	access code or	"Notification shall		notification will not	provided the person	accordance with the	
	the person does	password that	not be required [of a		compromise the	demonstrates that	person's policies in	
	not own or license	would permit	person who		criminal investigation	the cost of	the event of a	
	shall notify the	access to an	conducts business in		or national security	providing notice in	breach of security."	
	owner or licensee	individual's	Mississippi] if, after		and so notifies the	accordance with	(§75-24-29(7))	
	of the information	financial account."	an appropriate		person of that	paragraph (a), (b) or		
	of any breach of	(§75-24-29(2)(b))	investigation, the		determination."	(c) of this	For following	
	the security of the		person reasonably		(§75-24-29(5))	subsection would	interagency	
	data as soon as	Exception:	determines that the			exceed Five	guidelines: Yes.	
	practicable	"[P]ersonal	breach will not			Thousand Dollars (\$	"Any person that	
	following its	information' does	likely result in harm			5,000.00), that the	maintains such a	
	discovery, if the	not include	to the affected			affected class of	security breach	

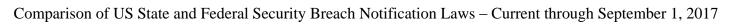


	Mississippi											
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute 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))					



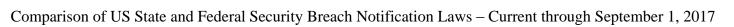


	Missouri										
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Penalties? Is			
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	there a private			
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	right of action?			
	requirement for		analysis?		v	available?		8			
	service		J								
	providers?										
Mo. Rev. Stat. §	Covered entities:	Personal	Breach definition:	Consumers:	Timing:	Method:	For establishing	State enforcement:			
407.1500	"Any person that	information:	"Breach of	Notification must be	"The disclosure	"[N]notice to	own notification	"The attorney			
	owns or licenses*	Personal	security' or 'breach'	given to the "affected	notification shall be:	affected consumers	method: Yes.	general shall have			
	personal	information means	[means]	consumer.*"	(a) Made without	shall be provided by	"A person that	exclusive authority			
	information of	"an individual's	unauthorized access	(§407.1500.2(1))	unreasonable delay;	one of the following	maintains its own	to bring an action to			
	residents of	first name or first	to and unauthorized		(b) Consistent with	methods:	notice procedures as	obtain actual			
	Missouri or any	initial and last	acquisition of	* Consumer means	the legitimate needs	(a) Written notice;	part of an	damages for a			
	person** that	name in	personal	"an individual who is	of law enforcement,	(b) Electronic notice	information security	willful and knowing			
	conducts business	combination with	information	a resident of	as provided in this	for those consumers	policy for the	violation of this			
	in Missouri that owns or licenses	any one or more of the following data	maintained in computerized form	[Missouri]." (§407.1500.1(2))	section; and (c) Consistent with	for whom the person has a valid	treatment of personal	section and may seek a civil penalty			
	personal	elements that	by a person that	(8407.1300.1(2))	any measures	email address and	information, and	not to exceed one			
	information in any	relate to the	compromises the		necessary to	who have agreed to	whose procedures	hundred fifty			
	form of a resident	individual if any	security,	Credit reporting	determine sufficient	receive	are otherwise	thousand dollars per			
	of Missouri."	of the data	confidentiality, or	agency and	contact information	communications	consistent with the	breach of the			
	(§407.1500.2(1))	elements are not	integrity of the	government notice	and to determine the	electronically, if the	timing requirements	security of the			
	(3 ( - / /	encrypted,	personal	requirement: Yes.	scope of the breach	notice provided is	of this section, is	system or series of			
	* "Owns or	redacted, or	information."	"In the event a person	and restore the	consistent with the	deemed to be in	breaches of a			
	licenses' includes,	otherwise altered	(§407.1500.1(1))	provides notice to	reasonable integrity,	provisions of 15	compliance with the	similar nature that			
	but is not limited	by any method or		more than one	security, and	U.S.C. Section 7001	notice requirements	are discovered in a			
	to, personal	technology in such	Exception:	thousand consumers	confidentiality of the	regarding electronic	of this section if the	single			
	information that a	a manner that the	"Good faith	at one time pursuant	data system."	records and	person notifies	investigation."			
	business retains as	name or data	acquisition of	to this section, the	(§407.1500.2(1))	signatures for	affected consumers	(§407.1500.3(4))			
	part of the internal	elements are	personal	person shall notify,		notices legally	in accordance with				
	customer account	unreadable or	information by a	without unreasonable	Delay:	required to be in	its policies in the	Private right of			
	of the business or	unusable:	person or that	delay, the attorney	Delay is permitted if	writing;	event of a breach of	action: No.			
	for the purpose of	(a) Social Security	person's employee	general's office and	"a law enforcement	(c) Telephonic	security of the				
	using the	number;	or agent for a	all consumer	agency informs the	notice, if such	system."				
	information in	(b) Driver's	legitimate purpose	reporting agencies	person that	contact is made	(§407.1500.3(1))				
	transactions with the person to	license number or other unique	of that person is not a breach of security,	that compile and maintain files on	notification may impede a criminal	directly with the affected consumers;	For following				
	whom the	identification	provided that the	consumers on a	investigation or	or	interagency				
	information	number created or	personal	nationwide basis, as	jeopardize national or	(d) Substitute	guidelines: Yes.				
	relates."	collected by a	information is not	defined in 15 U.S.C.	homeland security,	notice, if:	"A person that is				
	(§407.1500.1(7))	government body;	used in violation of	Section 1681a(p), of	provided that such	a. The person	regulated by state or				
	(3.07.12.00.1(7))	(c) Financial	applicable law or in	the timing,	request by law	demonstrates that	federal law and that				
	** "Person"	account number,	a manner that harms	distribution, and	enforcement is made	the cost of	maintains				
	means "any	credit card	or poses an actual	content of the	in writing or the	providing notice	procedures for a				





	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?				
	individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental subdivision, governmental agency, governmental instrumentality, public corporation, or any other legal or commercial entity." (§407.1500.1(8))  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	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))  Encryption: Encryption means "the use of an algorithmic process to	threat to the security, confidentiality, or integrity of the personal information." (§407.1500.1(1))  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))	notice." (§407.1500.2(8))	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))	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))  Substitute notice: "Substitute notice shall consist of all the following: (a) Email notice	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,					
	any person that conducts business	transform data into a form in which				when the person has an electronic mail	issued on March 29, 2005, by the					

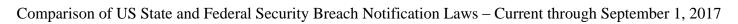




	Missouri										
State Statute	What entities are covered? Is there a requirement for	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is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

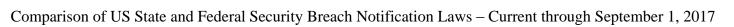


				Missouri				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Penalties? Is there a private right of action?
		professional." (§407.1500.1(6))  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))				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))		





	Montana											
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?				
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is				
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private				
	requirement for		analysis?		v	available?		right of action?				
	service		·									
	providers?											
Mont. Code Ann.	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	Enforcement: Not				
§30-14-1701 et	"Any person, or	information:	"[B]reach of the	"[A]ny resident of	"[F]ollowing	"[N]otice may be	own notification	specified.				
seq., § 33-19-231	business that	"[A]n individual's	security of the data	Montana whose	discovery or	provided by one of	method: Yes.	_				
	conducts business	first name or first	system' means	unencrypted personal	notification of the	the following	"[A] person or	Private right of				
	in Montana and	initial and last	unauthorized	information was or is	breach [t]he	methods:	business that	action: No.				
	that owns or	name in	acquisition of	reasonably believed	disclosure must be	(i) written notice;	maintains its own					
	licenses	combination with	computerized data	to have been acquired	made without	(ii) electronic	notification					
	computerized data	any one or more of	that materially	by an unauthorized	unreasonable delay,	notice, if the notice	procedures as part					
	that includes	the following data	compromises the	person." (§30-14-	consistent with the	provided is	of an information					
	personal	elements, when	security,	1704(1))	legitimate needs of	consistent with the	security policy for					
	information."	either the name or	confidentiality, or	~	law enforcement	provisions regarding	the treatment of					
	(§30-14-1704(1))	the data elements	integrity of personal	Credit reporting	or consistent with any	electronic records	personal					
	a	are not encrypted:	information	agency notice	measures necessary	and signatures set	information and that					
	Service provider	(A) social security	maintained by the	requirement: No.	to determine the	forth in 15 U.S.C.	does not					
	requirement:	number;	person or business	G	scope of the breach	7001;	unreasonably delay					
	Yes. "Any person	(B) driver's	and causes or is	Government notice	and to restore the	(iii) telephonic	notice is considered					
	or business that maintains	license number or state identification	reasonably believed to cause loss or	requirement: No.	integrity of the data system."	notice; or	to be in compliance with the notification					
	computerized data	card number;	injury to a Montana		(§30-14-1704(1))	(iv) substitute notice, if the person	requirements of this					
	that includes	(C) account	resident."		(830-14-1704(1))	or business	section if the person					
	personal	number or credit	(§30-14-1704(4)(a))		Delay:	demonstrates that:	or business notifies					
	information that	or debit card	(\$30-14-1704(4)(a))		Delay is permitted "if	(A) the cost of	subject persons in					
	the person or	number, in	Exception:		a law enforcement	providing notice	accordance with its					
	business does not	combination with	"Good faith		agency determines	would exceed	policies in the event					
	own shall notify	any required	acquisition of		that the notification	\$250,000;	of a breach of					
	the owner or	security code,	personal		will impede a	(B) the affected	security of the data					
	licensee of the	access code, or	information by an		criminal investigation	class of subject	system."					
	information of any	password that	employee or agent		and requests a delay	persons to be	(§30-14-1704(6))					
	breach of the	would permit	of the person or		in notification." Such	notified exceeds						
	security of the data	access to an	business for the		notification "must be	500,000; or	For following					
	system	individual's	purposes of the		made after the law	(C) the person or	interagency					
	immediately	financial account."	person or business		enforcement agency	business does not	guidelines: No.					
	following	(§30-14-1704(4)	is not a breach of		determines that it will	have sufficient						
	discovery if the	(b)(i))	the security of the		not compromise the	contact						
	personal		data system,		investigation."	information."						
	information was or	Exception:	provided that the		(§30-14-1704(3))	(§30-14-1704(5)(a))						
	is reasonably	Personal	personal									
	believed to have	information "does	information is not									



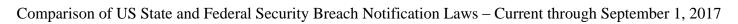


	Montana											
State Statute	What entities are covered? Is there a requirement for	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?				
	service providers?											
	been acquired by an unauthorized person." (§30-14-1704(2))  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	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))	used or subject to further unauthorized disclosure." (§30-14-1704(4)(a))  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))			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))						
	information was or is reasonably											

	Montana										
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?			
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is			
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private			
	requirement for		analysis?		•	available?		right of action?			
	service		ľ					8			
	providers?										
	believed to have										
	been acquired by										
	an unauthorized										
	person."										
	(§ 33-19-231)										
	* "'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))										
	(§ 55-17-104(10))										
	** "(a) 'Insurance-										
	support										
	organization'										
	means a person										
	who assembles or										
	collects										
	information about										
	natural persons for										
	the purpose of										
	providing the										
	information to an										

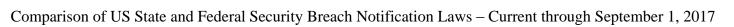
				Montana				
State Statute	What entities are covered? Is there a	What data are covered?	Has there been a breach? Is there a risk of harm	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice	Is there an exemption or safe harbor?	Enforcement?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

				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))							





				Nebraska				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?		ľ	available?		right of action?
	service		ľ					
	providers?							
Neb. Rev. Stat.	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:
87-801 et seq.	"An individual or	information:	"Breach of the	Notice must be given	"Notice shall be	"Notice means:	own notification	"[T]he Attorney
_	a commercial	"Personal	security of the	to the "affected	made as soon as	(a) Written notice;	method: Yes.	General may issue
	entity that	information means	system means the	Nebraska resident."	possible and without	(b) Telephonic	"An individual or a	subpoenas and seek
	conducts business	either of the	unauthorized	(§87-803(1))	unreasonable delay,	notice;	commercial entity	and recover direct
	in Nebraska and	following:	acquisition of		consistent with the	(c) Electronic	that maintains its	economic damages
	that owns or	(a) A Nebraska	unencrypted	Credit reporting	legitimate needs of	notice, if the notice	own notice	for each affected
	licenses	resident's first	computerized data	agency notice	law enforcement and	provided is	procedures which	Nebraska resident
	computerized data	name or first	that compromises	requirement: No.	consistent with any	consistent with the	are part of an	injured by a
	that includes	initial and last	the security,		measures necessary	provisions regarding	information security	violation of the act."
	personal	name in	confidentiality, or	Government notice	to determine the	electronic records	policy for the	(§87-806)
	information about	combination with	integrity of personal	requirement: Yes.	scope of the breach	and signatures set	treatment of	
	a resident of	any one or more of	information	"If notice of a breach	and to restore the	forth in 15 U.S.C.	personal	Private right of
	Nebraska."	the following data	maintained by an	of security of the	reasonable integrity	7001, as such	information and	action: No.
	(§87-803(1))	elements that	individual or a	system is required by	of the computerized	section existed on	which are otherwise	
	G	relate to the	commercial entity."	[§87-803(1)], the	data system."	January 1, 2006;	consistent with the	
	Service provider	resident if either	(§87-802(1))	individual or	(§87-803(1))	(d) Substitute	timing requirements	
	requirement:	the name or the	E	commercial entity	Dalam	notice, if the	of [the law], is	
	Yes. "[A]	data elements are	Exception: "Good faith	shall also, not later than the time when	<b>Delay</b> : Notice may be	individual or	deemed to be in	
	commercial entity that maintains	not encrypted, redacted, or	acquisition of	notice is provided to	delayed if "a law	commercial entity required to provide	compliance with the notice requirements	
	computerized data	otherwise altered	personal	the Nebraska	enforcement agency	notice demonstrates	of [the law] if the	
	that includes	by any method or	information by an	resident, provide	determines that the	that the cost of	individual or the	
	personal	technology in such	employee or agent	notice of the breach	notice will impede a	providing notice	commercial entity	
	information that	a manner that the	of an individual or a	of security of the	criminal	will exceed seventy-	notifies affected	
	the individual or	name or data	commercial entity	system to the	investigation. Notice	five thousand	Nebraska residents	
	commercial entity	elements are	for the purposes of	Attorney General."	shall be made in good	dollars, that the	and the Attorney	
	does not own or	unreadable:	the individual or the	(§87-803(2))	faith, without	affected class of	General in	
	license shall give	(i) Social security	commercial entity is	(30.000(=))	unreasonable delay,	Nebraska residents	accordance with its	
	notice to and	number;	not a breach of the		and as soon as	to be notified	notice procedures in	
	cooperate with the	(ii) Motor vehicle	security of the		possible after the law	exceeds one	the event of a	
	owner or licensee	operator's license	system if the		enforcement agency	hundred thousand	breach of the	
	of the information	number or state	personal		determines that	residents, or that the	security of the	
	of any breach of	identification card	information is not		notification will no	individual or	system."	
	the security of the	number;	used or subject to		longer impede the	commercial entity	(§87-804(1))	
	system when it	(iii) Account	further unauthorized		investigation."	does not have		
	becomes aware of	number or credit	disclosure."		(§87-803(4))	sufficient contact	For following	
	a breach if use of	or debit card	(§87-802(1))			information to	interagency	

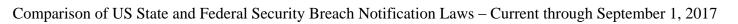




				Nebraska				
State Statute	What entities are covered? Is	What data are covered?	Has there been a breach? Is there	Who receives notice?	When must notice be given? May	How must notice be given? Is	Is there an exemption or	Enforcement? Penalties? Is
	there a	00101041	a risk of harm	11011001	notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?		notice be delayed.	available?	saic harbor.	right of action?
	service		didiy 515.			avanabie.		right of action.
	providers?							
	personal	number, in	Exception:			provide notice."	guidelines: Yes.	
	information about	combination with	"Acquisition of			(§87-802(4))	"An individual or a	
	a Nebraska	any required	personal			(307 002(1))	commercial entity	
	resident for an	security code,	information			Substitute notice:	that is regulated by	
	unauthorized	access code, or	pursuant to a search			"Substitute notice	state or federal law	
	purpose occurred	password that	warrant, subpoena,			under [§87-	and that maintains	
	or is reasonably	would permit	or other court order			802(4)(d)] requires	procedures for a	
	likely to occur.	access to a	or pursuant to a			all of the following:	breach of the	
	Cooperation	resident's financial	subpoena or order			(i) Electronic mail	security of the	
	includes, but is not	account;	of a state agency is			notice if the	system pursuant to	
	limited to, sharing	(iv) Unique	not a breach of the			individual or	the laws, rules,	
	with the owner or	electronic	security of the			commercial entity	regulations	
	licensee	identification	system."			has electronic mail	guidances, or	
	information	number or routing	(§87-802(1))			addresses for the	guidelines	
	relevant to the	code, in				members of the	established by its	
	breach, not	combination with	Risk of harm			affected class of	primary or	
	including	any required	analysis: Yes.			Nebraska residents;	functional state or	
	information	security code,	Notice must be			(ii) Notification by a	federal regulator is	
	proprietary to the	access code, or	given "if the			paid advertisement	deemed to be in	
	individual or	password; or	[individual's or			in a local newspaper	compliance with	
	commercial	(v) Unique	entity's]			that is distributed in	[the law] if the	
	entity."	biometric data,	investigation			the geographic area	individual or	
	(§87-803(3))	such as a	determines that the			in which the	commercial entity	
		fingerprint, voice	use of information			individual or	notifies affected Nebraska residents	
		print, or retina or iris image, or other	about a Nebraska resident for an			commercial entity is located, which	and the Attorney	
		unique physical	unauthorized			advertisement shall	General in	
		representation; or	purpose has			be of sufficient size	accordance with the	
		(b) A user name or	occurred or is			that it covers at least	maintained	
		email address, in	reasonably likely to			one-quarter of a	procedures in the	
		combination with	occur."			page in the	event of a breach of	
		a password or	(§87-803(1))			newspaper and shall	the security of the	
		security question	(307 003(1))			be published in the	system."	
		and answer, that				newspaper at least	(§87-804(2))	
		would permit				once a week for	(00.00.(-//	
		access to an online				three consecutive		
		account."				weeks;		
		(§87-802(5))				(iii) Conspicuous		

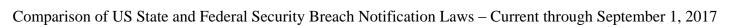


				Nebraska				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	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))		





What data are covered?  S: 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	Has there been a breach? Is there a risk of harm analysis?  Breach definition: A "breach of the security of the system data" is the "unauthorized acquisition of computerized data that materially	Residents: Any Nevada resident "whose unencrypted personal information was, or is reasonably believed to have	When must notice be given? May notice be delayed?  Timing: Following discovery or notification of the breach, "disclosure	How must notice be given? Is substitute notice available?  Method: "[T]he notification required by this	Is there an exemption or safe harbor?  For establishing own notification method: Yes.	Enforcement? Penalties? Is there a private right of action?  State enforcement: "If the Attorney
information: "[A] natural person's first name or first initial and last name in combination with any one or more of	A "breach of the security of the system data" is the "unauthorized acquisition of computerized data	Any Nevada resident "whose unencrypted personal information was, or is reasonably	Following discovery or notification of the breach, "disclosure	"[T]he notification required by this	own notification	"If the Attorney
information: "[A] natural person's first name or first initial and last name in combination with any one or more of	A "breach of the security of the system data" is the "unauthorized acquisition of computerized data	Any Nevada resident "whose unencrypted personal information was, or is reasonably	Following discovery or notification of the breach, "disclosure	"[T]he notification required by this	own notification	"If the Attorney
elements, when the name and data elements are not encrypted: (1) Social security number. (2) Driver's license number or ail identification card number. (3) Account r number, credit card number or debit card number, in combination with any required security code, access code or	compromises the security, confidentiality or integrity of personal information maintained by the data collector." (§603A.020)  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."	been, acquired by an unauthorized person." (§603A.220(1))  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."	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))  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 incomplete the notification will impede a criminal investigation. The notification section must be made after the law enforcement agency determines that the notification will not	section may be provided by one of the following methods: (a) Written notification. (b) Electronic notification, if the notification provided is consistent with the provisions of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq. (c) Substitute notification, if the data collector demonstrates that the cost of providing notification would exceed \$250,000, the affected class of subject persons to be notified exceeds 500,000 or the data collector does not have sufficient contact	"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))  For following interagency guidelines: Yes. A data collector	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)  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
	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."	encrypted: (1) Social security number. (2) Driver's license number or identification card number. (3) Account or number, credit card number or debit card number, in combination with any required security code, access code or s, password that would permit access to the person's financial account." (§603A.040)  maintained by the data collector." (§603A.020)  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	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)  maintained by the data collector." (§603A.020)  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 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 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."	maintained by the data collector. "(§603A.020) (§603A.020) (getrmines that notification is required to be given pursuant to the pursuant to the provisions of this section to more than information by an 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) (getrmines 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 unrelated to the data account." (§603A.040) (getrmines that notification is required to be given pursuant to the provisions of this section to more than (restore the reasonable integrity of the system data." (§603A.220(1))  Delay:  Notification "may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification is distributed and the content of the notification."	mintained by the data collector." (Social security number. (Social security number. (Social security number or license number or ail industrication card number. (Social security number or license number or license number or debit card number. (Social security number or license number or license number or license number or debit card number, or line with any required security code, access code or password that would permit access to the person's financial account." (Social security (\$603A.020)  Exception:  Breach "does not include the good faith acquisition of personal information by an debit card number, of the data collector shall also notify, without unreasonable delay, any consumer reporting agency that compiles and would permit access to the person's financial account." (Social security (\$603A.020)  Exception:  Breach "does not include the good faith acquisition of personal information by an debit card number, of the data collector of 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 disclosure." (Social security (\$603A.020)  Exception:  Breach "does not include the good faith acquisition of personal 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 disclosure." (Social security (\$603A.020)  Exception:  Exception:  Breach "does not include the good faith acquisition of persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency that compiles and maintains files on collector 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 notification will not contact information."  (Social security to the section	encrypted: (1) Social security number. (2) Driver's license number or identification card number. (3) Account faith acquisition of number, credit card number or debit card number or debit card number or in combination with any required security code, access code or password that would permit access to the person's financial account." (\$603A.020)    Maintained by the data collector determines that notification is not used for a purpose or manial account." (\$603A.020)    Maintained by the data collector determines that notification is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure." (\$603A.020)    Maintained by the data collector determines that notification is not usate of the meressary to determine the scope of the breach and restore the reasonable integrity of the 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 notification is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure." (\$603A.020)    Maintained by the determines that notification is not used for a purpose unrelated to the data collector of the data collector of the distributed and the continent of the unreasonable delay, any consumer reporting agency that complies and notational restore the reasonable integrity of the system data."   Maintained by the determines that necessary to determine the scope of the breach and restore the reasonable integrity of the system data."   With the fillectronic Signatures in Global and National comments in the complication."   Commerce Act, 15 Commerce Ac

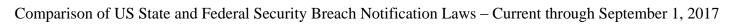




				Nevada				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	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)) "Operators" S.B. 538 also imposes certain notice requirements on "operators," which "means a person who: (a) Owns or	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)	Risk of harm analysis: No, except as definition of "breach" may incorporate elements of such a test.	Government notice requirement: No.	(§603A.220(3))	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 maintains an Internet website. (3) Notification to major statewide media." (§603A.220(4)(c))	with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§6801 et seq., shall be deemed to be in Compliance with the Notification requirements of this section." (§603A.220(5)(b))	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)  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

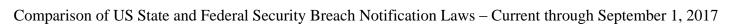
				Nevada				
State Statute	What entities are covered? Is there a	What data are covered?	Has there been a breach? Is there a risk of harm	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private
	requirement for		analysis?			available?		right of action?
	service		·					8
	providers?							
	operates an							court may order a
	Internet website or							person who is
	online service for							convicted of
	commercial							unlawfully
	purposes;							obtaining or
	(b) Collects and maintains covered							benefiting from personal
	information from							information
	consumers who							obtained as a result
	reside in this State							of such breach to
	and use or visit the							pay restitution to the
	Internet website or							data collector for
	online service; and							the reasonable costs
	(c) Purposefully							incurred by the data
	directs its							collector in
	activities toward							providing the
	this State,							[required]
	consummates							notification
	some transaction with this State or a							including, without limitation, labor,
	resident thereof or							materials, postage
	purposefully avails							and any other costs
	itself of the							reasonably related
	privilege of							to providing such
	conducting							notification."
	activities in this							(§603A.910)
	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							

				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."							





State Statute   What entities are covered?   Steep cove					New Hampshi	re			
requirement for service providers?  N.H. Rev. Stat. Ann. §359-C:19 of sex seq. (a) gustiness in [New Hampshire] who owns or licenses computerized data that includes personal information." (§359-C:20(I)(a)) and last name in combination with an individual, sorporation, trust, partnership, incorporated as association, limited liability of company, or other form of entity, or increases a manufacture form of entity, or other form of entity, or increase in dark and a calculated and the service provided entities:  Ann. §359-C:19 (No. H. Rev. Stat. Ann. §359-C:19 (No. H. Rev. Security to the data elements an individual's first that compromises the security of the following data elements, when every the data elements, when every the data elements an individual, corporated or unincorporated or unincorporated association, limited liability of company, or other form of entity, or other form of entity or other form of entity or other form of entity, or other form of entity or individuals."  State enforcem "The fisclosure shall (8359-C:20(II)(a) as possible, after the determination required under this section shall be provided by one of the following entity of the following methods: (§359-C:20(II)) (§359-C:20(III	State Statute	are covered? Is		breach? Is there	Who receives	When must notice be given? May	be given? Is	exemption or	Enforcement? Penalties? Is
N.H. Rev. Stat. Ann. §359-C:19 N.H. Rev. Stat. Ann. §359-C:19 Net Hampshire] who owns or licenses computerized data that includes personal information information information, information						notice be delayed?		sale narbor:	
N.H. Rev. Stat. Ann. §359-C:19 et seq.  N.H. Rev. Stat. Ann. §359-C:20(I)(a)  Information:  "Personal information		_		anarysis:			avanable:		right of action:
N.H. Rev. Stat. Ann, §359-C:19  Information:  "Security breach" "Every seq.    Covered entities: "Any persons" dindividuals: "Security breach" "The disclosure shall be meate to affected individuals as quickly as possible, after the determination required under this any one or more of the data elements an individual, corporated or unincorporated association, limited liability company, or other government of form of entity, or fo									
Ann. §359-C:19 et seq.  "Any person* doing business in [New Hampshire] who owns or licenses computerized data that includes personal information." (§359-C:20(I)(a))  "The disclosure shall be made to affected individuals as quickly as possible, after the determination required under this section shall be made to affected individuals as quickly as possible, after the determination required under this section shall be made to affected individuals as quickly as possible, after the determination required under this section." (§359-C:20(I)(a))  "The notice required under this section shall be provided by one of the following methods: (a) Written notice. (a) Written notice. (b) Electronic notice, if the agency or business' primary the treatment of a law enforcement agency, or national or unincorporated a sosociation, limited liability company, or other government form of entity, or of the form of entity, or identification in formation:  "The notice required under this section shall be made to affected individuals as quickly as possible, after the determination required under this section shall be made to affected individuals as quickly as possible, after the determination required under this section shall be made to affected individuals as quickly as possible, after the determination required under this section shall be made to affected individuals as quickly as possible, after the determination required under this section shall be provided by one of the following methods:  (§359-C:20(I)(a))  "The disclosure shall be made to affected individuals as quickly as possible, after the determination required under this section shall be made to affected individuals as quickly as possible, after the determination required under this section."  (§359-C:20(I)(b))  (§359-C:20(b))  Delay:  Delay	N H Rev Stat		Porconal	Breach definition:	"Δ ffected	Timing:	Method:	For actablishing	State enforcement:
doing business in [New Hampshire] who owns or licenses computerized data that includes personal information." (§359-C:20(I)(a))  Private right of acquisition of combination with an information information an individual, corporated or unincorporated or unincorporated association, [Imited liability company, or other form of entity, or identification in an electronic form of entity, or form of entity, or identification in an electronic information, information, and information, and information in [New Hampshire]. (§359-C:20(I)(a))  ### with a compromises the security or computerized data* that includes a cquisition of computerized data* that includes a composition individual, section individual, section, information or licenses.  #### with a compromises the security or confidentiality of personal or information and information information information information information information.  ### with a compromises the security or confidentiality of personal or information information information information information information information with a clements an individual, section individual as quickly as possible, after the determination required under this as quickly as possible, after the determination required under this as section. **Notice pursuant to the determination required under this as section. **Notice pursuant to the determination required under this as section. **Notice pursuant to the determination required under this as section. **Notice pursuant to the determination required under this as section. **Notice pursuant to the determination required under this as section. **Notice pursuant to the determination required under this as section. **Notice pursuant or the determination required under this as section. **Notice pursuant or the determination required under this as section. **Notice pursuant or the determination or the determination. The determination required under this as section. **Notice pur						U U			
[New Hampshire] who owns or licenses computerized data that includes personal information information information with information in an individual, partnership, incorporated or license association, limited liability company, or other form of entity, or identification is legal as the company, or other form of entity, or identification is legal as the computerized data that compromises the security of acquisition of acquisition of acquisition of acquisition of acquisition of acquisition of computerized data that compromises the security or combination of acquisition of acquisition of acquisition of computerized data that compromises the security or confidentiality of personal information individual, partnership, company, or other form of entity, or identification is acquisition of acquisition of acquisition of acquisition of acquisition of computerized data acquisition of computerized data that compromises the security or consumers of a breach of security pursuant to this partnership, acquisition of acquisition of computerized data that compromises the security or consumers of a breach of security pursuant to the following as equivalent the following methods:  (a) Written notice.  (b) Electronic  (b) Electronic  (b) Electronic  (b) Electronic  (b) Electronic  (c) Telephonic  (c) Telephonic  (d) Written notice.  (b) Electronic  (b) Electronic  (b) Electronic  (b) Electronic  (c) Telephonic  (d) Written notice.  (d) Written notice.  (e) S359-C:20(b)  (b) Delay:  (c) Telephonic  (d) Written notice.  (d) Written notice.  (e) Electronic  (d) Written notice.  (e) Electronic  (d) Breach of security policy for the treatment of prosonal and information and affected									Hampshire attorney
who owns or licenses of licenses of means an individual's first computerized data that includes that includes a that includes information." (§359-C:20(I)(a)) the following data elements, when an individual, corporation, trust, partnership, incorporated or incorporated or incorporated association, limited liability or company, or other form of entity, or incorporated incorporated incorporated individual's first agency notice agency notice required under this agency or required under this section."  (§359-C:20(b))  (§359-C	1. 2.4.				(300) 0120(0)(0))		-		
licenses computerized data that includes personal personal information." (§359-C:20(I)(a))  **"Person' means an individual, corporated runincorporated partnership, incorporated association, limited liability of company, or other form of entity, or licenses computerized data*					Credit reporting		provided by one of		shall enforce [the
computerized data that includes that includes personal information." any one or more of the following data elements, when an individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other government form of entity, or significant or company, or other government form of entity, or significant or combination with an includes that tacompromises the security or confidentiality of personal information with any one or more of the following data elements, when either the name or the data elements are not encrypted:*  (§359-C:20(b))  (b) Electronic of an information security policy for the treatment of personal information in notice, if the agency or business' primary means of communication with agency, or national or homeland security agency or business' primary means of the data elements all also notify, without unreasonable delay, all consumer reporting agencies that the notification will impede a criminal investigation or bother government information stored in formation is an individual, elements, when either the name or the data elements are not the data elements are not elements, when either the name or the data elements are not elements, when either the name or the data elements are not elements, when either the name or the data elements are not elements, when either the name or the data elements are not elements, when either the name or the data elements are not encrypted:*  (§359-C:20(b))  (§359-C:20(b))  (§359-C:20(b))  (b) Electronic of a private right of security por the treatment of sagency or national or homeland security agency determines that the notification will impede a criminal investigation or h			individual's first						
personal information." (systy-C:20(I)(a)) combination with any one or more of (systy-C:20(I)(a)) the following data elements, when either the name or an individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or integrated information information information information information information break of a consumers of a consumers of a breach of security ports of a consumers of a breach of security ports of a consumer of a consumer of the following data elements, when either the name or the data elements an individual, corporation, trust, partnership, encrypted:*  (2) Driver's limited liability of personal information information information information information information information security policy for the treatment of personal information security policy for the treatment of personal information information security alaw enforcement shall also notify, without unreasonable delay, all consumer reporting agencies that to comple and maintain files on company, or other form of entity, or identification information stored information socurity alaw enforcement shall also notify, without unreasonable delay, all consumer reporting agencies that to comple and maintain files on other government information stored information security alaw enforcement shall also notify, without unreasonable delay, all consumer reporting agencies that to comple and maintain files on other government information stored information stored information security alaw enforcement alaw enforc			name or initial and		requirement: Yes.			procedures	(§359-C:21(II))
information." (§359-C:20(I)(a))  *"'Person' means an individual, corporation, trust, partnership, incorporated or informated association, limited liability company, or other form of entity, or information infor		that includes							
(§359-C:20(I)(a)) the following data elements, when an individual, corporation, trust, partnership, incorporated unincorporated unincorporated information limited liability company, or other form of entity, or incorporate in the data element information information maintained by a person doing business in [New the data elements an individual, elements, when either the name or the data elements an individual, corporation, trust, partnership, incorporated or unincorporated or limited liability company, or other form of entity, or incorporated in a law enforcement alement of person in processing information maintained by a person doing business in [New the data elements an individual, elements, when either the name or the data elements an individual, are not either the name or the data elements an individual, corporated or the data elements an individual, corporated in information with alaw enforcement alements or business' primary means of a breach of security pursuant to this section, the person shall also notify, without unreasonable delay, all consumer reporting agencies that the notification or jeopardize national or homeland security agency determines that the notification will information with affected individuals is by electronic means. (§359-C:20(III)(e)) damages and for will impede a criminal investigation or jeopardize national or homeland or homeland or homeland or homeland or personal information with alements or personal information with alements or personal information with alements or low the treatment of personal information with alements or low the data elements alements or personal information with alements or low the data elements alements or low the sale without unreasonable delay, all consumer reporting agencies that the notification or jeopardize national or homeland or homeland or low the treatment of in law enforcement alements or low the treatment of informatio		1				(§359-C:20(b))	` '		O
elements, when either the name or the data elements an individual, corporation, trust, partnership, incorporated unincorporated association, limited liability company, or other form of entity, or identification is an individual, and individual, corporated and individual, either the name or the data elements an individual, and individual, corporation, trust, partnership, either the name or the data elements an individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or identification in a electronic in a mintained by a person doing pursuant to this section, the person shall also notify, without unreasonable delay, all consumer reporting agencies that the notification in stored in an electronic in a law enforcement agency, or national or homeland security agency determines that the notification with alaw enforcement agency, or national or homeland security agency determines that the notification with affected individuals information or homeland security agency determines that the notification will information with affected individuals information with affected individuals information is by electronic means. (§359-C:20(III)(e))  (by any violation and the law. (§359-C:20(III)(e))  (c) Telephonic notice, provided that a log of each such notification is kept by the person or other government information stored in a law enforcement agency, or national or homeland security agency determines that the notification or jeopardize national or homeland security agency determines that the notification or jeopardize national or homeland security agency determines that the notification or jeopardize national or homeland or homeland security alog of each such notification is kept by th									
* "Person' means an individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or identification in an electronic an individual, and individual, corporation, trust, partnership, encrypted:*  (§ 359-C:19(V))  (§ 359-C:20(III)(e))  (§ 359-C:20(III)(e))  (§ 359-C:20(III)(e))  (§ 359-C:20(III)(e))  (§ 359-C:20(III)(e))  (§ 359-C:20(III)(e))  (§ 359-C:21(I))		(§359-C:20(I)(a))							
an individual, corporation, trust, partnership, encrypted:*  (§359-C:19(V))  (§359-C:20(III)(e))  (§359-C:21(I))  (§359-C:21(I))  (§359-C:21(I))  (§359-C:21(I))  (§359-C:21(I))  (§359-C:21(I))		# (((D) )							
corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or									
partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or incorporated in a leactronic incorporated or unincorporated association in an electronic incorporated in a leactronic incorporated association, limited liability company, or other form of entity, or incorporated in a leactronic incorporated association, incorporated association, limited liability company, or other form of entity, or incorporated in a leactronic incorporated association, incorporated association, limited liability company, or other form of entity, or incorporated association, limited liability company, or other form of entity, or incorporated association, limited liability company, or other form of entity, or incorporated association, limited liability company, or other form of entity, or incorporated association, limited liability company, or other form of entity, or incorporated association, limited liability company, or other form of entity, or incorporated ata' means delay, all consumer reporting agencies that the notification will impede a criminal investigation or jeopardize national or homeland security."    (§ 359-C:20(III)(e)   damages and form such that the notification will impede a criminal investigation or jeopardize national or homeland security."    (§ 359-C:20(III)(e)   damages and form such that the notification will impede a criminal investigation or jeopardize national or homeland security."		,							
incorporated or unincorporated Number.  (2) Driver's limited liability company, or other form of entity, or identification in an electronic incorporated or unincorporated association, limited liability company, or other form of entity, or identification in an electronic incorporated or unincorporated unincorporated on unincorporated or unincorporate or unincorporated or unincorporate or unincorporate or u							_		
unincorporated association, (2) Driver's limited liability company, or other form of entity, or limited liability association (2) Driver's limited liability company, or other form of entity, or limited liability association (2) Driver's limited liability company, or other form of entity, or limited liability association (2) Driver's license number or other government information stored in an electronic limited liability company, or other form of entity, or license number or other government license number or other government limited liability company, or other form of entity, or license number or other government license number or other g				(8339-C:19(V))				(§359-C:20(III)(e))	<u> </u>
association, limited liability company, or other form of entity, or limited liability of license number or limited liability company, or other form of entity, or license number or license numb				* "Computerized				For following	
limited liability company, or other form of entity, or license number or other government in an electronic license number or other government information stored in an electronic license number or other government information stored in an electronic license number or other government information stored in an electronic license number or other government information stored in an electronic license number or other government information stored in an electronic license number or other government information stored in an electronic license number or other government license number or other government information stored in an electronic license number or other government license n				*					
company, or other form of entity, or identification in an electronic in an									
form of entity, or dentification in an electronic nationwide basis, as security." business who engaged in trade or <b>Burden of proo</b>									(355) 0.21(1))
									Burden of proof
any agency, number. format." defined by 15 U.S.C. (§359-C:20(II)) notifies affected commerce that is requirement:									
authority, board, (3) Account (§359-C:19(I)) section 1681a(p), of persons. subject to RSA 358- "The burden sha			(3) Account	(§359-C:19(I))	section 1681a(p), of		persons.	subject to RSA 358-	"The burden shall
court, department, number, credit the anticipated date (d) Substitute A:3, I which be on the person		court, department,			the anticipated date			A:3, I which	be on the person
		division,	card number, or		of the notification to		notice, if the person	maintains	responsible for the
			,				demonstrates that	1	determination [of
									whether 'misuse of
									the information has
governmental security code, information by an will be notified, and would exceed pursuant to the occurred or is				information by an					
			· /						reasonably likely to
political password that of a person for the notice." affected class of regulations, occur'] to		-							-
subdivision of the state."    Subdivision of the state."   Subdivision of the subject individuals   guidances, or   demonstrate   guidances, or   demonstrate   compliance."			•		(8339-C:20(VI))				
					Covernment notice				(§359-C:21(III))
(§359-C:19(III)) Individual's shall not be Government notice exceeds 1,000, or a state of lederal (§359-C:21(III)), financial account." considered a requirement: Yes.		(8333-C:13(III))							(8339-C:21(III))
(§359- security breach, "Any person engaged have sufficient deemed to be in									
C:19(IV)(a)) provided that the in trade or commerce contact information compliance with					, , , , ,				

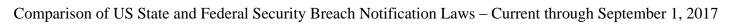




				New Hampshi	re			
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	Service provider requirement: Yes. An 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))	* "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))	personal information is not used or subject to further unauthorized disclosure." (§359-C:19(V))  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))	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."		or consent to provide notice pursuant to subparagraphs I(a)-I(c)." (§359-C:20(III))  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))  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	this subdivision if it acts in accordance with such laws, rules, regulations, guidances, or guidelines." (§359-C:20(V))	

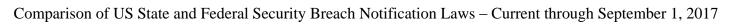


				New Hampshi	ire			
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice 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))		





	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 et seq.	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))  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 shall notify that business or public entity of any breach of security of the computerized records immediately	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	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)  Exception: "Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a	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))  * "Customer" means "an individual who provides personal information to a business." (§56:8-161)  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	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))  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	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	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))  For following interagency	State enforcement: "It shall be an unlawful practice and a violation of P.L.1960, c.39 (C.56:8-1 et seq.) [the New Jersey Consumer Fraud Act] to willfully, knowingly or recklessly violate [the breach notification law]." (§56:8-166) "It shall be an unlawful practice and a violation of P.L.1960, c.39 (C.56:8-1 et seq.) [the New Jersey Consumer Fraud Act] to violate the provisions of [the specific health insurance provisions]." (§56:8-198)  Private right of action: No.			
	following discovery, if the personal information was,	personal information is personal information if the	breach of security, provided that the personal information is not	that compile or maintain files on consumers on a nationwide basis	made a request that the notification be delayed. The notification required	sufficient contact information." (§56:8-163(d))	guidelines: No.				



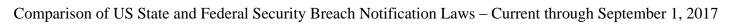


	New Jersey										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?			
	or is reasonably believed to have been, accessed by an unauthorized person." (§56:8-163(b))  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	means to link the dissociated data were accessed in connection with access to the dissociated data." (§56:8-161)  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)	used for a purpose unrelated to the business or subject to further unauthorized disclosure." (§56:8-161)  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))	of the timing, distribution and content of the notices." (§56:8-163(f))  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))	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))	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))					

	New Jersey										
State Statute	What entities are covered? Is	What data are covered?	Has there been a breach? Is there	Who receives notice?	When must notice be given? May	How must notice be given? Is	Is there an exemption or	Enforcement? Penalties? Is			
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private			
	requirement for		analysis?			available?		right of action?			
	service		·								
	providers?										
	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."										
	(§56:8-197(a))										
	The law "shall										
	only apply to end										
	user computer										
	systems and										
	computerized records										
	transmitted across										
	public networks."										
	(§56:8-197 (b))										
	"Health										
	insurance carrier"										
	is defined as "an										
	insurance										
	company, health										
	service										
	corporation,										

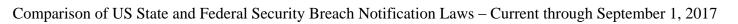
	New Jersey										
State Statute	What entities are covered? Is there a	What data are covered?	Has there been a breach? Is there a risk of harm	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private			
	requirement for		analysis?			available?		right of action?			
	service										
	providers?										
	hospital service										
	corporation,										
	medical service										
	corporation, or health										
	maintenance										
	organization										
	authorized to issue										
	health benefits										
	plans in [New										
	Jersey]."										
	(§56:8-196)										
	"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:										
	(1) Social Security										
	Number;										
	(2) driver's license										
	number or State										
	identification card										
	number;										
	<ul><li>(3) address; or</li><li>(4) identifiable</li></ul>										
	health										
	information.										
	Dissociated data										
	that, if linked,										
	would constitute										
	personal										
	information is										

	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)										





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)	Covered entities:  "[Any] person that owns or licenses elements that include personal identifying information of a New Mexico resident."  (§6.A)  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	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	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)  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	Residents:  "[E]ach New Mexico resident whose personal identifying information is reasonably believed to have been subject to a security breach." (§6.A)  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	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."  Delay: "The notification required by the Data Breach Notification Act and 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)	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	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)  For following interagency guidelines: Yes.  "The provisions of the Data Breach Notification Act shall not apply to a person subject to the federal	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-		

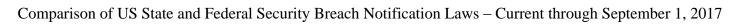




	New Mexico										
State Statute	What entities are covered? Is there a requirement for	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is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

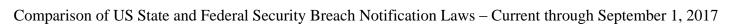


	New Mexico										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute 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)					



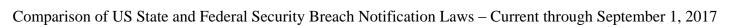


	New York										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?			
N.Y. Gen. Bus. Law § 899-aa	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))  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	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))  Private information: "Private information" means "personal information or consisting of any information 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	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	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))  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)))  *"Consumer reporting agency' shall mean any person which, for monetary fees, dues, or on a cooperative	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))  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 that such notification shall be made after such law enforcement agency determines that such notification	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.	For establishing own notification method: No.  For following interagency guidelines: No.	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,			





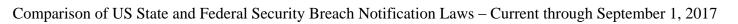
	New York										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice 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 notices 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			





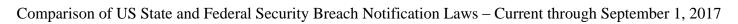
				New York				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?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



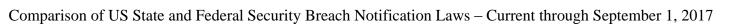


				North Carolin	na			
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?			available?		right of action?
	service							
	providers?							
N.C. Gen. Stat.	Covered entities:	Personal	Breach definition:	The "affected	Timing:	Method:	For establishing	State enforcement:
§75-60 et seq.	"Any business that	information:	A "security breach"	person."	"[F]ollowing	"[N]otice to	own notification	Violations are
	owns or licenses	"Personal	is an "incident of	(§75-65(a))	discovery or	affected persons	method: No.	treated as "[u]nfair
	personal	information'	unauthorized access		notification of the	may be provided by		methods of
	information of	[means a] person's	to and acquisition of	Person: "Person"	breach [t]he	one of the following	For following	competition in or
	residents of North	first name or first	unencrypted and	means "[a]ny	disclosure	methods:	interagency	affecting commerce,
	Carolina or any	initial and last	unredacted records	individual,	notification shall be	(1) Written notice.	guidelines: Yes.	and unfair or
	business that	name in	or data containing	partnership,	made without	(2) Electronic	"A financial	deceptive acts or
	conducts business	combination with	personal	corporation, trust,	unreasonable delay,	notice, for those	institution that is	practices in or
	in North Carolina	identifying	information where	estate, cooperative,	consistent with the	persons for whom it	subject to and in	affecting
	that owns or	information* as	illegal use of the	association,	legitimate needs of	has a valid e-mail	compliance with the	commerce" for
	licenses personal	defined in G.S. 14-	personal	government, or	law enforcement, as	address and who	Federal Interagency	which the Attorney
	information in any	113.20(b)."	information has	governmental	provided in [§75-	have agreed to	Guidance Response	General may seek
	form (whether	(§75-61(10)	occurred or is	subdivision or	65(c)], and consistent	receive	Programs for	both civil and
	computerized,	ψ ((T)	reasonably likely to	agency, or other	with any measures	communications	Unauthorized	criminal penalties.
	paper, or	* "The term	occur or that creates	entity."	necessary to	electronically if the	Access to Consumer	(§§75-65(i), 75-1.1,
	otherwise)."	'identifying information'	a material risk of	(§75-61(9))	determine sufficient contact information,	notice provided is consistent with the	Information and	13, 15.2)
	(§75-65(a))	includes the	harm to a consumer.	Cuadit wanauting		provisions regarding	Customer Notice, issued on March 7,	Duizoto night of
	Service provider	following:	Any incident of unauthorized	Credit reporting agency notice	determine the scope of the breach and	electronic records	2005, by the Board	Private right of action: Yes, but
	requirement:	(1) Social security	access to and	requirement: Yes.	restore the reasonable	and signatures for	of Governors of the	only if an
	Yes. "Any	or employer	acquisition of	"In the event a	integrity, security,	notices legally	Federal Reserve	"individual is
	business that	taxpayer	encrypted records or	business provides	and confidentiality	required to be in	System, the Federal	injured as a result of
	maintains or	identification	data containing	notice to more than	of the data system."	writing set forth in	Deposit Insurance	the violation" of the
	possesses records	numbers.	personal	1,000 persons at one	(§75-65(a))	15 U.S.C. § 7001.	Corporation, the	Act.
	or data containing	(2) Drivers	information along	time pursuant to this	(\$75 05(a))	(3) Telephonic	Office of the	(§75-65(i))
	personal	license, State	with the	section, the business	Delay:	notice provided that	Comptroller of the	(3,70 00(1))
	information of	identification card,	confidential process	shall notify, without	Notification may be	contact is made	Currency, and the	
	residents of North	or passport	or key shall	unreasonable delay,	delayed "if a law	directly with the	Office of Thrift	
	Carolina that the	numbers.	constitute a security	the Consumer	enforcement agency	affected persons.	Supervision; or a	
	business does not	(3) Checking	breach."	Protection Division	informs the business	(4) Substitute	credit union that is	
	own or license, or	account numbers.	(§75-61(14))	of the Attorney	that notification may	notice, if the	subject to and in	
	any business that	(4) Savings		General's Office and	impede a criminal	business	compliance with the	
	conducts business	account numbers.	Exception: "Good	all consumer	investigation or	demonstrates that	Final Guidance on	
	in North Carolina	(5) Credit card	faith acquisition of	reporting agencies	jeopardize national or	the cost of	Response Programs	
	that maintains or	numbers.	personal	that compile and	homeland security,	providing notice	for Unauthorized	
	possesses records	(6) Debit card	information by an	maintain files on	provided that such	would exceed two	Access to Member	
	or data containing	numbers.	employee or agent	consumers on a	request is made in	hundred fifty	Information and	





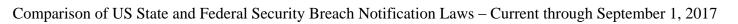
	North Carolina										
State Statute	What entities are covered? Is there a	What data are covered?	Has there been a breach? Is there a risk of harm	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private			
	requirement for		analysis?		·	available?		right of action?			
	service		v					8			
	providers?										
	personal	(7) Personal	of the business for	nationwide basis, as	writing or the	thousand dollars	Member Notice,				
	information that	Identification	a legitimate purpose	defined in 15 U.S.C.	business documents	(\$250,000) or that	issued on April 14,				
	the business does	(PIN) Code** as	is not a security	§ 1681a(p), of the	such request	the affected class of	2005, by the				
	not own or license	defined in G.S. 14-	breach, provided	timing, distribution,	contemporaneously	subject persons to	National Credit				
	shall notify the	113.8(6).	that the personal	and content of the	in writing, including	be notified exceeds	Union				
	owner or licensee	(8) Electronic	information is not	notice."	the name of the law	500,000, or if the	Administration; and				
	of the information	identification	used for a purpose	(§75-65(f))	enforcement officer	business does not	any revisions,				
	of any security	numbers,	other than a lawful		making the request	have sufficient	additions, or				
	breach	electronic mail	purpose of the	Government notice	and the officer's law	contact information	substitutions				
	immediately	names or	business and is not	requirement: Yes.	enforcement agency	or consent to satisfy	relating to any of				
	following	addresses, Internet	subject to further	"In the event a	engaged in the	subdivisions (1),	the said interagency				
	discovery of the	account numbers,	unauthorized	business provides	investigation.	(2), or (3) of this	guidance, shall be				
	breach, consistent	or Internet	disclosure."	notice to an affected	[Notice] shall be	subsection, for only	deemed to be in				
	with the legitimate	identification	(§75-61(14))	person pursuant to	provided without	those affected	compliance with this section."				
	needs of law	names. (9) Digital	Diale of house	this section, the	unreasonable delay after the law	persons without sufficient contact	(§75-65(h))				
	enforcement as provided in		Risk of harm analysis: Yes.	business shall notify			(8/3-03(n))				
	[(§75-65(c)]."	signatures. (10) Any other	Notification is only	without unreasonable delay the Consumer	enforcement	information or consent, or if the					
	(§75-65(b))	numbers or	required "where	Protection Division	agency communicates to the	business is unable to					
	(873-03(0))	information that	illegal use of the	of the Attorney	business its	identify particular					
		can be used to	personal	General's Office of	determination that	affected persons, for					
		access a person's	information has	the nature of the	notice will no longer	only those					
		financial	occurred or is	breach, the number of	impede the	unidentifiable					
		resources.	reasonably likely to	consumers affected	investigation or	affected persons."					
		(11) Biometric	occur or that creates	by the breach, steps	jeopardize national	(§75-65(e))					
		data.	a material risk of	taken to investigate	or homeland	(3/2 05(0))					
		(12) Fingerprints.	harm to a consumer.	the breach, steps	security."	Substitute notice:					
		(13) Passwords.	Any incident of	taken to prevent a	(§75-65(c))	"Substitute notice					
		(14) Parent's legal	unauthorized access	similar breach in the		shall consist of all					
		surname prior to	to and acquisition of	future, and		the following:					
		marriage."	encrypted records or	information regarding		a. E-mail notice					
		(§14-113.20(b))	data containing	the timing,		when the business					
			personal	distribution, and		has an electronic					
		** "Personal	information along	content of the		mail address for the					
		identification	with the	notice."		subject persons.					
		code' means a	confidential process	(§75-65(e1))		b. Conspicuous					
		numeric and/or	or key shall			posting of the notice					
		alphabetical code	constitute a security			on the Web site					





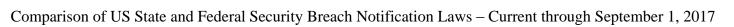
	North Carolina											
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?				
		assigned to the cardholder of a financial transaction card by the issuer to permit authorized electronic use of that FTC." (§14-113.8(6))  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))	breach." (§71-61(14))			page of the business, if one is maintained. c. Notification to major statewide media." (§75-65(e)(4))  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.						

				North Caroli	na			
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))		





				North Dakota	ì			
State Statute	What entities are covered? Is	What data are covered?	Has there been a breach? Is there	Who receives notice?	When must notice be given? May	How must notice be given? Is	Is there an exemption or	Enforcement? Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?		,	available?		right of action?
	service		J					8
	providers?							
N.D. Cent. Code	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:
§51-30-01 et seq.	"Any person that	information:	A "[b]reach of the	Any North Dakota	"[F]ollowing	"Notice under this	own notification	"The attorney
	owns or licenses	"Personal	security of the	resident "whose	discovery or	chapter may be	method: Yes.	general may enforce
	computerized data	information'	system" is the	unencrypted personal	notification of the	provided by one of	If a person	this chapter. The
	that includes	means an	"unauthorized	information was, or is	breach in the security	the following	"maintains its own	attorney general, in
	personal "	individual's first	acquisition of	reasonably believed	of the data [t]he	methods:	notification	enforcing this
	information." (§51-30-02)	name or first initial and last	computerized data when access to	to have been, acquired by an	disclosure must be made in the most	<ol> <li>Written notice;</li> <li>Electronic notice,</li> </ol>	procedures as part of an information	chapter, has all the powers provided in
	(831-30-02)	name in	personal	unauthorized person."	expedient time	if the notice	security policy for	chapter 51-15
	Service provider	combination with	information has not	(§51-30-02)	possible and without	provided is	the treatment of	[which prohibits
	requirement:	any of the	been secured by	(\$51.50.02)	unreasonable delay,	consistent with the	personal	'any deceptive act
	Yes. "Any person	following data	encryption or by	Credit reporting	consistent with the	provisions regarding	information and is	or practice'] and
	that maintains	elements, when	any other method or	agency notice	legitimate needs of	electronic records	otherwise consistent	may seek all the
	computerized data	the name and	technology that	requirement: No.	law enforcement, as	and signatures set	with the timing	remedies in chapter
	that includes	the data elements	renders the		provided in section	forth in section	requirements" under	51-15 [including
	personal	are not encrypted:	electronic files,	Government notice	51-30-04, or any	7001 of title 15 of	North Dakota's law,	injunctions and civil
	information that	(1) The	media, or data	requirement: Yes.	measures necessary	the United	then that person "is	penalties of 'not
	the person does	individual's social	bases unreadable	"[A] any person that	to determine the	States Code; or	deemed to be in	more than five
	not own shall notify the owner	security number;	or unusable."	experiences a breach of the security system	scope of the breach and to restore the	3. Substitute notice, if the person	compliance with the notification	thousand dollars for each violation']. A
	or licensee of the	(2) The operator's license number	(§51-30-01(1))	as provided in this	integrity of the data	demonstrates that	requirements of [the	violation of this
	information of the	assigned to an	Exception: "Good-	section shall disclose	system."	the cost of	law] if the person	chapter is deemed
	breach of the	individual by the	faith acquisition of	to the attorney	(§51-30-02)	providing notice	notifies the subject	a violation of
	security of the data	department	personal	general by mail or	(30 - 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	would	individuals in	chapter 51-15. The
	immediately	of transportation	information by an	email any breach of	<b>Delay</b> : Delay is	exceed two hundred	accordance with its	remedies, duties,
	following the	under section 39-	employee or agent	the security system	permitted "if a law	fifty thousand	policies in the event	prohibitions, and
	discovery, if the	06-14;	of the person is not	which exceeds two	enforcement agency	dollars, or that the	of a breach of the	penalties of this
	personal	(3) A nondriver	a breach of the	hundred fifty	determines that the	affected class of	security of the	chapter are not
	information was,	color photo	security of the	individuals."	notification will	subject persons	system."	exclusive and are in
	or is reasonably	identification card	system, if the	(§51-30-02)	impede a criminal	to be notified	(§51-30-06)	addition to all other
	believed to have	number assigned	personal		investigation."	exceeds five	Eastellassiss	causes of action,
	been, acquired by an unauthorized	to the individual by the department	information is not used or subject to		Notification "must be made after the	hundred thousand, or the person does	For following interagency	remedies, and penalties under
	person."	of transportation	further unauthorized		law enforcement	not have sufficient	guidelines: Yes.	chapter 51-15, or
	(§51-30-03)	under section 39-	disclosure."		agency determines	contact	If a "financial	otherwise provided
	(851 50 05)	06-03.1;	(§51-30-01(1))		that it will not	information."	institution, trust	by law."
		(4) The	(0 (-))		compromise the	(§51-30-05)	company, or credit	(§51-30-07)
		individual's			investigation."	,	union" is "subject	,



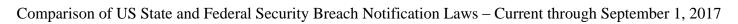


	North Dakota											
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute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

	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?			
		individual's digitized or other electronic signature." (§51-30-01(4)(a)) * 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))  ** 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))  Exception: "Personal information' does not include									

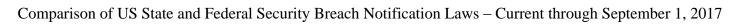


				North Dakota	a			
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice 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))						



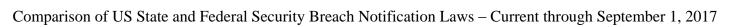


	Ohio											
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?				
Ohio Rev. Code Ann. §1349.19	Covered entities: "Any person* that owns or licenses computerized data that includes personal information." (§1349.19(B)(1))  * "[P]erson" includes a business entity only if the business entity conducts business in [Ohio]." (§1349.19(A)(6))  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	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	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))  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	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))  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	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))  Delay: "The person may delay the disclosure or notification if a law enforcement agency determines that the disclosure or notification will	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 notification is required would exceed \$250,000, or the affected class of subject residents to	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))  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,	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))  Private right of action: No.				





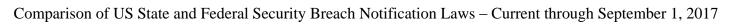
	Ohio										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice 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))				





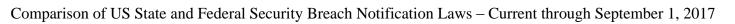
Ohio											
are cov the require ser	entities What data are covered? Is covered? ere a ement for vice iders?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is 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))				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						

				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?
						least once a week for three consecutive weeks; (b) Conspicuous posting of the disclosure or notice on the business entity's web site, if the entity maintains one; (c) Notification to major media outlets in the geographic area in which the business entity is located." (§1349.19(E))		





Oklahoma										
	covered? brea a r	s there been a each? Is there 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 et seq.  "An individual or entity that owns or licenses or fir computerized data that includes personal information." one of (\$163(A)) follow elements:  "Entity: relate: "[E]ntity' [Oklatincludes corporations, business trusts, estates, encry partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governmental subdivisions, agencies, or any other legal entity, whether for profit." (\$162(2))	irst initial and name in unau and a linked to any or more of the owing data ments that te to a[n] the security and all all all all all all all all all al	reach of the arity of a sem' means the athorized access acquisition of accepted* and adacted** aputerized data compromises security or acceptional armation aritinated by an aritination a	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))  Credit reporting agency notice requirement: No.  Government notice requirement: No.	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))  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	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))	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 sact 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))  For following interagency guidelines: Yes: "A financial institution that complies with the notification requirements	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			

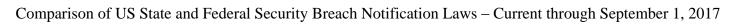




	Oklahoma											
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice 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.				

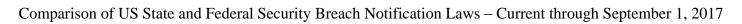
	hat entities e covered? Is	What data are		Oklahoma											
requ	there a quirement for service providers?	covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?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

				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?
			unauthorized disclosure." (§162(1))  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))					



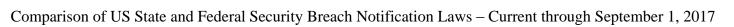


	Oregon										
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?			
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is			
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private			
	requirement for		analysis?		·	available?		right of action?			
	service		·								
	providers?										
Oregon Revised	Covered entities:	Personal	Breach definition:	Consumers:	Timing:	Method:	For establishing	State enforcement:			
Statutes	"A person that	information:	A "[b]reach of	"The consumer to	Notification shall be	Notification can be	own notification	"If the [Director of			
§646A.600 et seq	owns or licenses	"Personal	security means an	whom the personal	made "in the most	made:	method: No.	the Department of			
	personal	information'	unauthorized	information pertains	expeditious manner	"(a) In writing;		Consumer and			
	information that	means:	acquisition of	after the person	possible, without	(b) Electronically, if	For following	Business Services]			
	the person uses in	(a) A consumer's	computerized data	discovers the breach	unreasonable delay,	the person	interagency	has reason to			
	the course of the	first name or first	that materially	of security or after	consistent with the	customarily	guidelines: Yes.	believe that any			
	person's business,	initial and last	compromises the	the person receives	legitimate needs of	communicates with	"This section does	person has engaged			
	vocation,	name in	security,	notice of a breach of	law enforcement	the consumer	not apply to:	or is engaging in			
	occupation or	combination with	confidentiality or	security."	described in	electronically or if	(a) A person that	any violation of [the			
	volunteer	any one or more of	integrity of personal	(§604(1)(a))	[§604(3)] and	the notice is	complies with	breach notification			
	activities."	the following data	information that a	"'C	consistent with any	consistent with the	notification	law], the director			
	(§604(1))	elements, if	person maintains."	"Consumer' means	measures that are	provisions regarding	requirements or	may issue an order,			
	Person:	encryption, redaction or other	(§602(1)(a))	an individual resident	necessary to determine sufficient	electronic records and signatures set	procedures for a breach of security	subject to ORS chapter 183,			
	Person means "an	methods have not	Exception:	of [Oregon]." (§602(2))	contact information	forth in the	that the person's	directed to the			
	individual, private	rendered the data	"Breach of	(8002(2))	for the affected	Electronic	primary or	person to cease and			
	or public	elements unusable	security' does not	Credit reporting	consumer, determine	Signatures in Global	functional federal	desist from the			
	corporation,	or if the data	include an	agency notice	the scope of the	and National	regulator adopts,	violation, or require			
	partnership,	elements are	inadvertent	requirement: Yes.	breach of security	Commerce Act (15	promulgates or	the person to pay			
	cooperative,	encrypted and the	acquisition of	"If a person discovers	and restore the	U.S.C. 7001) as that	issues in rules,	compensation to			
	association, estate,	encryption key has	personal	a breach of security	reasonable integrity,	Act existed on the	regulations,	consumers injured			
	limited liability	been acquired:	information by a	that affects more than	security and	effective date of this	procedures,	by the violation."			
	company,	(A) A	person or the	1,000 consumers, the	confidentiality of the	2015 Act;	guidelines or	(§624(3))			
	organization or	consumer's	person's employee	person shall notify,	personal	(c) By telephone, if	guidance, if the	(0 ( ))			
	other entity,	Social Security	or agent if the	without unreasonable	information."	the person contacts	rules, regulations,	Penalties:			
	whether or not	number;	personal	delay, all consumer	(§604(1)(a))	the affected	procedures,	"(a) In addition to			
	organized to	(B) A	information is not	reporting agencies		consumer directly;	guidelines or	all other penalties			
	operate at a profit,	consumer's	used in violation of	that compile and	Delay:	or	guidance provide	and enforcement			
	or a public body as	driver license	applicable law or in	maintain reports on	"A person that owns	(d) With substitute	greater protection to	provisions provided			
	defined [under	number or state	a manner that harms	consumers on a	or licenses personal	notice, if the person	personal	by law, any person			
	Oregon law]."	identification	or poses an actual	nationwide basis	information may	demonstrates that	information and	who violates or who			
	(§602(10))	card number	threat to the	of the timing,	delay notifying a	the cost of	disclosure	procures, aids or			
		issued by the	security,	distribution and	consumer of a breach	notification	requirements at	abets in the			
	Service provider	Department	confidentiality or	content of the notice	of security only	otherwise would	least as thorough as	violation of [the			
	requirement:	of 	integrity of the	the person gave to	if a law enforcement	exceed \$250,000 or	the protections and	breach notification			
	Yes. "A person	Transportation;	personal	affected consumers	agency determines	that the affected	disclosure	law] shall be subject			
	that maintains or	(C) A	information."	and shall include in	that a notification	class of consumers	requirements	to a penalty of not			





	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			

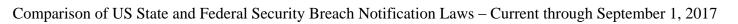




				Oregon				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	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))

				Oregon				
State Statute	What entities are covered? Is	What data are covered?	Has there been a breach? Is there	Who receives notice?	When must notice be given? May	How must notice be given? Is	Is there an exemption or	Enforcement? Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?			available?		right of action?
	service							
	providers?	1 ( ) 6					notice described in	
		paragraph (a) of this subsection						
		without the					subparagraph (A) of this paragraph to the	
		consumer's first					Attorney General	
		name or first					within a reasonable	
		initial and last					time after the	
		name if:					Attorney General	
		(i) Encryption,					requests the copy."	
		redaction or					(§604(8))	
		other methods						
		have not						
		rendered the data						
		element or combination of						
		data elements						
		unusable; and						
		(ii) The data						
		element or						
		combination of						
		data elements						
		would enable a						
		person to commit						
		identity theft						
		against a						
		consumer." (§§602(11)(a), (b))						
		(\$\$002(11)(a), (b))						
		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						

				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))						





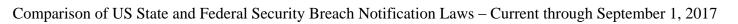
				Pennsylvania				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?		·	available?		right of action?
	service		J					8
	providers?							
73 Pa. Stat.	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:
§2301 et seq.	"An entity* that	information:	A "[b]reach of the	"[A]ny resident of	"Except as provided	"[Notice] [m]ay be	own notification	"A violation of this
	maintains, stores,	"An individual's	security of the	[Pennsylvania] whose	in [(§2304)	provided by any of	method: Yes.	act shall be deemed
	or manages	first name or first	system" is "[t]he	unencrypted and	authorization delay	the following	"An entity that	to be an unfair or
	computerized data	initial and last	unauthorized access	unredacted personal	pursuant to the needs	methods of	maintains its own	deceptive act or
	that includes	name in	and acquisition of	information was, or	of law enforcement]	notification:	notification	practice in violation
	personal	combination with	computerized data	reasonably is	or in order to take	(1) Written notice to	procedures as part	of the act of
	information."	and linked to any	that materially	believed to have	any measures	the last known	of an information	December 17, 1968
	(§2303(a))	one or more of the	compromises the	been, accessed and	necessary to	home address for	privacy or security	(P.L.1224, No.387),
	4.00	following data	security or	acquired by an	determine the scope	the individual.	policy for the	known as the Unfair
	* "Entity" means a	elements, when	confidentiality of	unauthorized person."	of the breach and to	(2) Telephonic	treatment of	Trade Practices and
	"[s]tate agency, a	the name and data	personal	(§2303(a))	restore the reasonable	notice, if the	personal	Consumer
	political	elements are not	information	C 124	integrity of the data	customer can be	information and is	Protection Law."
	subdivision of	encrypted or	maintained by the	Credit reporting	system, the notice	reasonably expected	consistent with the	(§2308)
	[Pennsylvania] or an individual or a	redacted: (i) Social security	entity as part of a database of personal	agency notice requirement: Yes.	shall be made without unreasonable delay."	to receive it and the notice is given in a	notice requirements of this act shall be	Private right of
	business doing	number;	information	"When an entity	(§2303(a))	clear and	deemed to be in	action: No.
	business in	(ii) Driver's	regarding multiple	provides notification	(82303(a))	conspicuous	compliance with the	"The Office of
	[Pennsylvania]."	license number or	individuals and that	under this act to more	Delay:	manner, describes	notification	Attorney General
	(§2302)	state identification	causes or the entity	than 1,000 persons at	"The notification	the incident in	requirements of this	shall have exclusive
	(82302)	card number;	reasonably believes	one time, the entity	required by this act	general terms and	act if it notifies	authority to bring an
	Service provider	(iii) Financial	has caused or will	shall also notify,	may be delayed if a	verifies personal	subject persons in	action under the
	requirement:	account number,	cause loss or injury	without unreasonable	law enforcement	information but	accordance with its	Unfair Trade
	Yes. "A vendor	credit or debit card	to any resident of	delay, all consumer	agency determines	does not require the	policies in the event	Practices and
	that maintains,	number, in	[Pennsylvania]."	reporting agencies	and advises the entity	customer to provide	of a breach of	Consumer
	stores, or manages	combination with	(§2302)	that compile and	in writing specifically	personal	security of the	Protection Law for a
	computerized data	any required		maintain files on	referencing this	information and the	system."	violation of this
	on behalf of	security code,	Exception: "Good	consumers on a	section that the	customer is	(§2307(a))	act."
	another entity	access code, or	faith acquisition of	nationwide basis."	notification will	provided with a		(§2308)
	shall provide	password that	personal	(§2305)	impede a criminal or	telephone number to	For following	
	notice of any	would permit	information by an		civil investigation.	call or Internet	interagency	
	breach of the	access to an	employee or agent	Government notice	The notification	website to visit for	guidelines: Yes.	
	security system	individual's	of the entity for the	requirement: No.	required by this act	further information	"(1) A financial	
	following	financial account."	purposes of the		shall be made after	or assistance.	institution that	
	discovery by the	(§2302)	entity is not a		the law enforcement	(3) E-mail notice, if	complies with the	
	vendor to the		breach of the		agency determines	a prior business	notification	
	entity on whose		security of the		that it will not	relationship exists	requirements	
	behalf the vendor		system if the		compromise the	and the person or	prescribed by the	



				Pennsylvania	1			
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 email 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))	

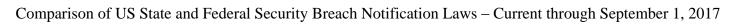


	Pennsylvania										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute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





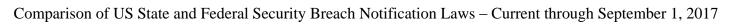
				Puerto Rico				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?		ľ	available?		right of action?
	service		J					8
	providers?							
10 L.P.R.A. St	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:
§4051 et seq.	"Any entity* that	information:	"[Violation of the	Affected "citizen	Clients [presumably	"To notify the	own notification	The Secretary of
	is the owner or	"Personal	Security System]	Residents of Puerto	meaning affected	citizens the entity	method: Possibly.	State "may impose
	custodian of a	information file'	means any situation	Rico." A covered	citizens] "must be	shall have the	The Act states that	fines of five
	database that	refers to a file	in which it is	entity "must notify	notified as	following options:	"[n]o provision of	hundred (500)
	includes personal	containing at least	detected that access	said citizens of any	expeditiously as	(1) Written direct	this Act shall be	dollars up to a
	information of	the name or first	has been permitted	breach of the security	possible, taking into	notice to those	interpreted as being	maximum of five
	citizen residents of	initial and the	to unauthorized	of the system when	consideration the	affected by mail or	prejudicial to those	thousand (5,000)
	Puerto Rico."	surname of a	persons or entities	the database whose	need of law	by authenticated	institutional	dollars for each
	(§4052)	person, together	to the data files so	security has been	enforcement agencies	electronic means	information and	violation."
		with any of the	that the security,	breached contains, in	to secure possible	according to the	security policies	(§4055)
	* Entity means	following data so	confidentiality or	whole or in part,	crime scenes and	Digital Signatures	that an enterprise or	
	"every agency,	that an association	integrity of the	personal information	evidence as well as	Act.	entity may have in	Private right of
	board, body,	may be established	information in the	files and the same are	the application of	(2) When the cost of	force prior to its	action: Yes.
	examining board,	between certain	data bank has been	not protected by an	measures needed to	notifying all those	effectiveness and	"The fines [imposed
	corporation, public	information with	compromised; or	encrypted code but	restore the system's	potentially affected	whose purpose is to	by the Secretary of
	corporation,	another and in	when normally	only by a password."	security."	according to	provide protection	State] do not affect
	committee,	which the information is	authorized persons or entities have had	(§4052)	(§4052)	subsection (1) of	equal or better to the information on	the rights of the consumers to
	independent office, division,		access and it is	Credit reporting	Delay:	this section or of identifying them is	security herein	initiate actions or
	administration,	legible enough so that in order to	known or there is	agency notice	Before providing	excessively onerous	established."	claims for damages
	bureau,	access it there is	reasonable	requirement: No.	notice, covered	due to the number	(§4054)	before a competent
	department,	no need to use a	suspicion that they	requirement. 140.	entities may "tak[e]	of persons affected,	(84024)	court."
	authority, official,	special	have violated the	Government notice	into consideration the	to the difficulty in	For following	(§4055)
	instrumentality or	cryptographic	professional	requirement: Yes.	need of law	locating all persons	interagency	(84033)
	administrative	code:	confidentiality or	The Department of	enforcement agencies	or to the economic	guidelines: No.	
	organism of the	(1) Social security	obtained	Consumer Affairs	to secure possible	situation of the	Suravinio	
	three branches of	number;	authorization under	must be notified	crime scenes and	enterprise or entity;		
	the Government;	(2) Driver's	false representation	within 10 days after	evidence as well as	or whenever the		
	every corporation,	License Number,	with the intention of	the violation of the	the application of	cost exceeds one		
	partnership,	Voter's	making illegal use	system's security has	measures needed to	hundred thousand		
	association,	Identification or	of the information.	been detected.	restore the system's	dollars (\$100,000)		
	private company	other Official	This includes both	(§4052)	security." However,	or the number of		
	or organization	Identification;	access to the data		"[w]ithin a non-	persons exceeds one		
	authorized to do	(3) Bank or	banks through the	Additionally, "[i]n	extendable term of	hundred thousand		
	business or	financial account	system and physical	those cases in which	ten (10) days after the	[(\$100,000)], the		
	operate in the	numbers of any	access to the	the breach or	violation of the	entity shall issue the		
	Commonwealth of	type with or	recording media	irregularity in the	system's security has	notice through the		





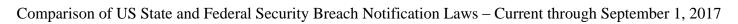
	Puerto Rico											
a	What entities are covered? Is there a equirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?				
w pp ex in re le le or (§ Sr re Y Y th op or to be sa pp in re le	ruerto Rico; as well as every public or private ducational astitution, regardless of the evel of education affered by it." §4051)(d))  Service provider requirement:  Yes. "Any entity hat as part of their perations resells are provides access to digital data and that at the ame time contain resonal afformation files of citizens must resonal afformation of any iolation of the ystem's security hat has allowed coess to those ites to mauthorized resons." §4052)	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))  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))	that contain the same and any removal or undue retrieval of said recordings." (§4051)(c))  Risk of harm analysis: No, except insofar as definition of a "breach" incorporates elements of such a test.	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)	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)	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						

				Puerto Rico				
State Statute	What entities are covered? Is there a requirement for service	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?
	providers?							
						that sector." (§4053)		
						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)		





	Rhode Island										
State Statute	What entities are covered? Is there a requirement for service	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?			
	providers?										
R.I. Gen. Laws §11-49.3-1 et seq.	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))  *A "[p]erson" includes "any individual, sole proprietorship, partnership, association, corporation, joint venture, business or legal entity, trust, estate, cooperative, or other entereds."	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;	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))  Exception: "Goodfaith acquisition of personal information by an appelation of the security of personal information by an appelation of the security of personal information by an appelation of the security of	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))  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	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	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	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	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 about the last of the second will be a civil violation of this about the last of the second will be a civil violation of this about the last of the second will be a civil violation of this about the last of the civil violation of this about the last of the civil violation of the civil viola			
	other commercial entity." (§11-49.3-3(a)(7)) Service provider requirement:	(iii) Account number, credit, or debit card number, in combination with any required security code,	employee or agent of the agency for the purposes of the agency is not a breach of the security of the	the notices and the approximate number of affected individuals.  Notification to the	provided in [§11-49.3-4(c)]." (§11-49.3-4(a))  Delay: "The notification	(\$25,000), or that the affected class of subject persons to be notified exceeds fifty thousand (50,000), or the	requirements of § 11-49.3-4, and notifies subject persons in accordance with such municipal	this chapter has occurred and that proceedings would be in the public interest, the attorney general may bring			
	Yes. "(a)(1) Any municipal agency, state agency, or person that stores, owns, collects, processes, maintains,	access code, password, or personal identification number, that would permit access to an	system; provided, that the personal information is not used or subject to further unauthorized disclosure." (§11-49.3-3(a)(1))	major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents." (§11-49.3-4(a)(2))	required by this section may be delayed if a federal, state, or local law enforcement agency determines that the notification will	municipal agency, state agency, or person does not have sufficient contact information. (§11-49.3-3(c))	agency's, state agency's, or person's notification policies in the event of a breach of security." (§11-49.3-6(a)(1))	an action in the name of the state against the business or person in violation." (§11-49.3-5)			





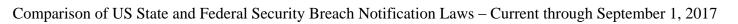
	Rhode Island											
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute 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.				



	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?				
		policy number, subscriber identification number, or any unique identifier used by a health insurer to identify the individual." (§11-49.3-3(a)(3))  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))			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))		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))  "A provider of health care, 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					

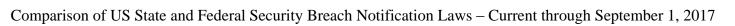


	Rhode Island									
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute 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))			



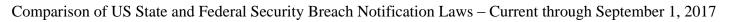


	South Carolina										
State Statute	What entities are covered? Is there a requirement for	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?			
	service providers?		-								
S.C. Code §39-1-	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:			
90	"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))  * A "person" includes "a natural	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	"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	"[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	"[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	"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	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	"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			
	person, an individual, or an organization." (§37-20-110)	the data elements are neither encrypted nor redacted: (a) social security	identifying information maintained by the person, when illegal use of the	occurred or is reasonably likely to occur or use of the information creates	necessary to determine the scope of the breach and restore the reasonable integrity of the data	records and signatures in Section 7001 of Title 15 USC and Chapter 6, Title 11	considered to be in compliance with the notification requirements of this section if the person	Department of Consumer Affairs." (§39-1-90(H)) Private right of			
	Service provider requirement: Yes. "A person conducting business in [South Carolina] and	number; (b) driver's license number or state identification card number issued instead of a	information has occurred or is reasonably likely to occur or use of the information creates a material risk of	a material risk of harm to the resident." (§39-1-90(A)) Credit reporting	system." (§39-1-90(A))  Delay: Notification "may be delayed if a law	of the 1976 Code; (3) telephonic notice; or (4) substitute notice, if the person demonstrates that	notifies subject persons in accordance with its policies in the event of a breach of security of the	action: Yes.  "A resident of [South Carolina] who is injured by a violation of this section, in addition			
	maintaining computerized data or other data that includes personal identifying information that	driver's license; (c) financial account number, or credit card or debit card number in combination	harm to a resident." (§39-1-90(D)(1))  Exception: "Good faith acquisition of	agency and government notice requirement: Yes. "If a business provides notice to more than one	enforcement agency determines that the notification impedes a criminal investigation. The notification required	the cost of providing notice exceeds two hundred fifty thousand dollars or that the affected	system." (§39-1-90(F))  For following interagency guidelines: Yes.	to and cumulative of all other rights and remedies available at law, may: (1) institute a civil action to recover			
	the person does not own shall notify the owner or licensee of the information of	with any required security code, access code, or password that would permit	personal identifying information by an employee or agent of the person for the purposes of its	thousand persons at one time pursuant to this section, the business shall notify, without unreasonable	by this section must be made after the law enforcement agency determines that it no longer compromises	class of subject persons to be notified exceeds five hundred thousand or the	The law "does not apply to a bank or financial institution that is subject to and in compliance with	damages in case of a wilful [sic] and knowing violation; (2) institute a civil action that must be			



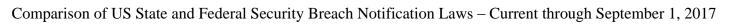


	South Carolina										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute 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 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))			





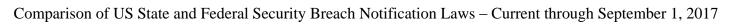
				Tennessee				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?		·	available?		right of action?
	service							9
	providers?							
Tenn. Code Ann.	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:
§47-18-2107	Any "information	information:	A "[b]reach of	"[A]ny resident of	"[F]ollowing	"[N]otice may be	own notification	Not specified.
	holder," which is	"[A]n individual's	system security" is	[Tennessee] whose	discovery or	provided by one (1)	method: Yes.	
	defined as "any	first name or first	the	personal information	notification of a	of the following	"[I]f an information	Private right of
	person or business	initial and last	"acquisition of"	was, or is reasonably	breach of system	methods:	holder maintains its	action: Yes.
	that conducts	name, in	"[u]nencrypted	believed to have	security [t]he	(1) Written notice;	own notification	"Any customer of
	business in	combination with	computerized data;	been, acquired by an	disclosure must be	(2) Electronic	procedures as part	an information
	[Tennessee], or	any one (1) or	or [e]ncrypted	unauthorized person."	made no later than	notice, if the notice	of an information	holder who is a
	any agency of	more of the	computerized data	(§2107(b))	forty-five (45) days	provided is	security policy for	person or business
	[Tennessee] or any	following data	and the encryption		from the discovery or	consistent with the	the treatment of	entity, but who is
	of its political	elements:	key" "by an	Credit reporting	notification of the	provisions regarding	personal	not an agency of
	subdivisions, that	(i) Social security	unauthorized person	agency notice	breach of system	electronic records	information and if	this state or any
	owns or licenses	number;	that materially	requirement: Yes.	security, unless a	and signatures set	the policy is	political subdivision
	computerized	(ii) Driver license	compromises the	"If an information	longer period of time	forth in 15 U.S.C. §	otherwise consistent	of this state, and
	personal information of	number; or	security, confidentiality, or	holder discovers	is required due to the legitimate needs of	7001 or if the	with the timing	who is injured by a violation of this
	residents of	(iii) Account number, credit	integrity of personal	circumstances	law enforcement, as	information holder's primary method of	requirements of this section, the	section, may
	[Tennessee]."	card, or debit card	information	requiring notification pursuant to this	provided in	communication with	information holder	institute a civil
	(§§2107(b), (a)(3))	number, in	maintained by the	section of more than	[§2107(d)]."	the resident of this	is in compliance	action to recover
	(882107(0), (a)(3))	combination with	information holder."	one thousand (1,000)	(§2107(b))	state has been by	with the notification	damages and to
	Exception: "This	any required	(§2107(a)(1)(A))	persons at one (1)	(\$2107(0))	electronic means; or	requirements of this	enjoin the
	section does not	security code,	(32107(4)(1)(11))	time, the information	Delay:	(3) Substitute	section, as long as	information holder
	apply to any	access code, or	Exception:	holder must also	Delay permitted "if a	notice, if the	the information	from further action
	information holder	password that	"Does not include	notify, without	law enforcement	information holder	holder notifies	in violation of this
	that is subject to:	would permit	the good faith	unreasonable delay,	agency determines	demonstrates that	subject persons in	section. The rights
	(1) Title V of the	access to an	acquisition of	all consumer	that the notification	the cost of	accordance with its	and remedies
	Gramm-Leach-	individual's	personal	reporting agencies, as	will impede a	providing notice	policies in the event	available under this
	Bliley Act of 1999	financial account."	information by an	defined by 15 U.S.C.	criminal	would exceed two	of a breach of	section are
	(Pub. L. No. 106-	(§2107(a)(4)(A))	employee or agent	§ 1681a, and credit	investigation. If the	hundred fifty	system security."	cumulative to each
	102); or		of the information	bureaus that compile	notification is	thousand dollars	(§2107(f))	other and to any
	(2) The Health	Exception:	holder for the	and maintain files on	delayed, it must be	(\$250,000), that the		other rights and
	Insurance	Personal	purposes of the	consumers on a	made no later than	affected class of	For following	remedies available
	Portability and	information	information holder	nationwide basis, of	forty-five (45) days	subject persons to	interagency	under law."
	Accountability Act	"[d]oes	if the personal	the timing,	after the law	be notified exceeds	guidelines: No.	(§2107(h))
	of 1996 (42 U.S.C.	not include	information is not	distribution, and	enforcement agency	five hundred		
	§ 1320d et seq.),	information that is	used or subject to	content of the	determines that	thousand (500,000),		
	as expanded by the	lawfully made	further unauthorized	notices."	notification will not	persons, or the		
1	Health	available to the	disclosure."	(§2107(g))	compromise the	information holder		





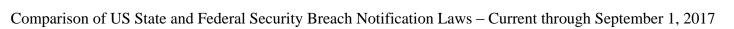
	Tennessee											
a	What entities are covered? Is there a equirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?				
To CU Exc AA	rechnology for clinical and conomic Health act (42 U.S.C. § 000jj et seq., and 2 U.S.C. § 17921 t seq.)." § 2107(i))  ervice provider equirement: 'es. "Any nformation holder nat maintains computerized data nat includes ersonal nformation that ne information older does not wn shall notify ne owner or censee of the nformation of any reach of system ecurity if the ersonal nformation was, r is reasonably elieved to have een, acquired by n unauthorized erson. The isclosure must be nade no later than orty-five (45) ays from the	general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable." (§2107(a)(4)(B))	(§2107(a)(1)(B))  Risk of harm analysis: No, except as definition of "breach" may incorporate elements of such a test.	Government notice requirement: No.	investigation." (§2107(d))	does not have sufficient contact information." (§2107(e))  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))						

	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))										





	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	Covered entities: "A person who conducts business in [Texas] and owns or licenses computerized data that includes sensitive personal information." (§521.053(b))  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))	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;	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))  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	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))  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))	Timing: "The disclosure shall be made as quickly as possible" (§521.053(b))  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))	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))  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	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))  For following interagency guidelines: No.	State enforcement: "The attorney general may bring an action to recover the civil penalty imposed under this subsection." (§521.151(g))  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		



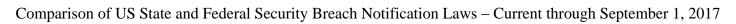


				Texas				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
		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))  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))	manner." (§521.053(a))  Risk of harm analysis: No, except as provided in the definition of a breach.	Government notice requirement: No.		(3) notice published in or broadcast on major statewide media." (§521.053(f))  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))		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

				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?
								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)) "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))



				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.

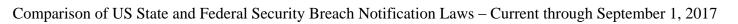




				Utah				
State Statute	What entities are covered? Is	What data are covered?	Has there been a breach? Is there	Who receives notice?	When must notice be given? May	How must notice be given? Is	Is there an exemption or	Enforcement? Penalties? Is
	there a	covereu.	a risk of harm	notice.	notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?		notice be delayed.	available?	Sale har but :	right of action?
	service		anarysis:			avaliable:		right of action:
	providers?							
Utah Code 13-	Covered entities:	Personal	Breach definition:	Residents: Affected	Timing:	Method:	For establishing	State enforcement:
44-	"A person who	information:	"Breach of system	Utah residents.	Notice must be given	"A notification	own notification	The Utah attorney
101 et seq.	owns or licenses	"Personal	security' means an	(§13-44-202(1)(b))	"in the most	required by this	method: Yes.	general may seek an
101 ct seq.	computerized data	information'	unauthorized	(\$15 44 202(1)(0))	expedient time	section may be	"If a person	injunction against a
	that includes	means a person's	acquisition of	Credit reporting	possible without	provided:	maintains the	violator, attorney
	personal	first name or first	computerized data	agency notice	unreasonable delay:	(i) in writing by	person's own	fees and costs, and
	information	initial and last	maintained by a	requirement: No.	(a) considering	first-class mail to	notification	may also seek civil
	concerning a Utah	name, combined	person that	1	legitimate	the most recent	procedures as part	penalties:
	resident."	with any one or	compromises the	Government notice	investigative needs	address the person	of an information	"(a) no greater than
	(§13-44-202(1)(a))	more of the	security,	requirement: No.	of law enforcement,	has for the resident;	security policy for	\$2,500 for a
		following data	confidentiality, or	•	as provided in	(ii) electronically, if	the treatment of	violation or series of
	Service provider	elements relating	integrity of personal		[the law enforcement	the person's	personal	violations
	requirement:	to that person	information."		delay exception,	primary method of	information the	concerning a
	Yes. "A person	when either the	(§13-44-102(1)(a))		described below];	communication with	person is considered	specific consumer;
	who maintains	name or date			(b) after determining	the resident is by	to be in compliance	and
	computerized data	element is	Exception:		the scope of the	electronic means, or	with this chapter's	(b) no greater than
	that includes	unencrypted or not	A breach "does not		breach of system	if provided in	notification	\$100,000 in the
	personal	protected by	include the		security; and	accordance with the	requirements if the	aggregate for
	information that	another method	acquisition of		(c) after restoring the	consumer disclosure	procedures are	related violations
	the person does	that renders the	personal		reasonable integrity	provisions of	otherwise consistent	concerning more
	not own or license	data unreadable or	information by an		of the system."	15 U.S.C. Section	with this chapter's	than one consumer."
	shall notify and	unusable:	employee or agent		(§13-44-202(2))	7001;	timing requirements	(§13-44-301(3))
	cooperate with the owner or licensee	(i) Social Security number;	of the person possessing		Delay:	(iii) by telephone, including through	and the person notifies each	Private right of
	of the information	(ii) [F]inancial	unencrypted		(a) "[A] person may	the use of automatic	affected Utah	action: No.
	of any breach of	account number.	computerized data		delay providing	dialing technology	resident in	"Nothing in this
	system security	or credit or debit	unless the personal		notification under	not prohibited by	accordance with the	chapter creates a
	immediately	card number [and]	information is used		[§13-44-202(1)] at	other law; or	person's	private right of
	following the	any required	for an unlawful		the request of a law	(iv) by publishing	information security	action [or] affects
	person's discovery	security code,	purpose or disclosed		enforcement agency	notice of the breach	policy in the event	any private right of
	of the breach if	access code, or	in an unauthorized		that determines that	of system security:	of a breach."	action existing
	misuse of the	password that	manner."		notification may	(A) in a newspaper	(§13-44-202(5)(b))	under other law,
	personal	would permit	(§13-44-102(1)(b))		impede a criminal	of general		including contract
	information occurs	access to the			investigation.	circulation; and	For following	or tort."
	or is reasonably	person's account;	Risk of harm		(b) A person who	(B) as required in	interagency	(§13-44-301(2))
	likely to occur."	or	analysis: Yes.		delays providing	Section 45-1-101	guidelines: Yes.	
	(§13-44-202(3)(a))	(iii) [D]river	"A person who		notification shall	[regulating	"A person who is	
		license number or	owns or licenses		provide notification	publication and	regulated by state	

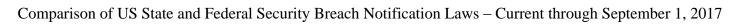


				Utah				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	provided	state identification card number." (§13-44-102(3)(a))  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))	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))		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))	broadcasting]." (§13-44-202(5)(a))	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))	



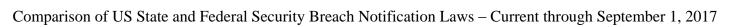


				Vermont				
State Statute	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
	are covered? Is	covered?	breach? Is there	notice?	be given? May	be given? Is	exemption or	Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?			available?		right of action?
	service		J					8
	providers?							
Vt. Stat. Ann. tit.	Covered entities:	Personally	Breach definition:	Consumers:	Timing:	Method:	For establishing	State enforcement:
9, §2430 et seq.	"[A]ny data	identifiable	A "security	"Consumers,"	"Notice of the breach	"For purposes of	own notification	"[T]he Attorney
1	collector* that	information:	breach" means	defined as Vermont	shall be made in the	this subsection,	method: No.	General and state's
	owns or licenses	"[A]n individual's	"unauthorized	residents.	most expedient time	notice to consumers		attorney shall have
	computerized	first name or first	acquisition of	(§§2430(2),	possible and without	may be provided by	For following	sole and full
	personal	initial and last	electronic data or a	2435(b)(1))	unreasonable delay,	one of the following	interagency	authority to
	information that	name in	reasonable belief of		but not later than 45	methods:	guidelines: Yes.	investigate potential
	includes personal	combination with	an unauthorized	Credit reporting	days after the	(A) Direct notice to	"[A] financial	violations and to
	information	any one or more of	acquisition of	agency notice	discovery or	consumers, which	institution that is	enforce, prosecute,
	concerning a	the following data	electronic data that	requirement: Yes.	notification,	may be by one of	subject to the	obtain, and impose
	consumer."	elements, when	compromises the	If notice must be	consistent with the	the following	following	remedies for [any]
	(§2435(b)(1))	either the name or	security,	given to "more than	legitimate needs of	methods:	guidances, and any	violation."
		the data elements	confidentiality, or	1,000 consumers at	the law enforcement	(i) Written notice	revisions, additions,	If the data
	* Data collector	are not encrypted	integrity of a	one time pursuant to	agency, as provided	mailed to the	or substitutions	collector is licensed
	"may include the	or redacted or	consumer's	[the law], the data	in [§§2435(b)(3) and	consumer's	relating to an	or registered with
	State, State	protected by	personally	collector shall notify,	(4)], or with any	residence;	interagency	the Department of
	agencies, political subdivisions of the	another method	identifiable	without unreasonable	measures necessary	(ii) Electronic	guidance shall be	Financial
		that renders them	information	delay, all consumer	to determine the	notice, for those consumers for	exempt from this section:	Regulation under Title 8, the
	State, public and private	unreadable or unusable by	maintained by the data collector."	reporting agencies that compile and	scope of the security breach and restore the	whom the data	(1) The Federal	Department shall
	universities,	unauthorized	(§2430(8)(A))	maintain files on	reasonable integrity,	collector has a	Interagency	have full authority.
	privately and	persons:	"In determining	consumers on a	security, and	valid e-mail	Guidance Response	(§§2435(g)(1), (2))
	publicly held	(i) Social Security	whether personally	nationwide basis, as	confidentiality of the	address if:	Programs for	(\$\frac{9}{2433}(\frac{9}{2})(1), (2))
	corporations,	number;	identifiable	defined in 15 U.S.C.	data system."	(I) the data	Unauthorized	Private right of
	limited liability	(ii) Motor vehicle	information has	§ 1681a(p), of the	(§2435(b)(1))	collector does not	Access to Consumer	action: No.
	companies,	operator's license	been acquired or is	timing, distribution,	(\$2433(0)(1))	have contact	Information and	action. 140.
	financial	number or	reasonably believed	and content of the	Delay:	information set	Customer Notice,	
	institutions, retail	nondriver	to have been	notice. This	Delay is permitted	forth in	issued on March 7,	
	operators, and any	identification card	acquired by a	subsection shall not	"upon request of a	subdivisions (i)	2005, by the Board	
	other entity that,	number;	person without valid	apply to a person who	law enforcement	and (iii) of	of Governors of the	
	for any purpose,	(iii) Financial	authorization, a data	is licensed or	agency. A law	[§2435(b)(6)], the	Federal Reserve	
	whether by	account number or	collector may	registered under Title	enforcement agency	data collector's	System, the Federal	
	automated	credit or debit card	consider the	8 by the department	may request the delay	primary method	Deposit Insurance	
	collection or	number, if	following factors,	of banking,	if it believes that	of	Corporation, the	
	otherwise,	circumstances	among others:	insurance, securities,	notification may	communication	Office of the	
	handles, collects,	exist in which the	(i) indications that	and health care	impede a law	with the	Comptroller of the	
	disseminates, or	number could be	the information is	administration."	enforcement	consumer is by	Currency, and the	
	otherwise deals	used without	in the physical	(§2435(c))	investigation, or a	electronic means,	Office of Thrift	



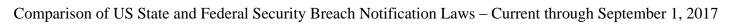


	Vermont									
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?		
	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))  Service provider requirement: Yes. "Any data collector that	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))  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))	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))  Exception: A security breach "does not include good faith but unauthorized acquisition or access of personal information by an employee or agent	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	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))	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	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))			



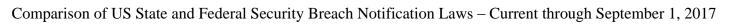


	Vermont										
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?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





				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?
	providers		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	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		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		
			secret' if the notice and detailed	state's attorney, or another law		further security breach;		

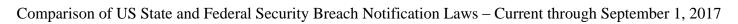




				Vermont				
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
			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))	enforcement officer engaged in legitimate law enforcement activities without the consent of the data collector." (§2435(b)(3))  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		(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))		

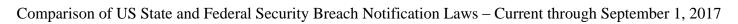


				Vermont				
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is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



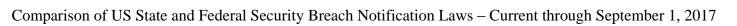


	Virginia										
State Statute	What entities are covered? Is there a	What data are covered?	Has there been a breach? Is there a risk of harm	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?			
	requirement for service providers?		analysis?			avanable:		right of action:			
Va. Code §18.2- 186.6	Covered entities:  "[A]n individual or entity* that owns or licenses computerized data that includes personal information."  (§18.2-186.6(B))  * "Entity' includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit."	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	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)) "An individual or entity shall disclose the breach of the security of the	Residents: "[T]he Office of the Attorney General and any affected resident of the Commonwealth." (§18.2-186.6(B))  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."	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))  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 determines	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))	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))  For following interagency guidelines: Yes "An entity that is subject to Title V of	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)) "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)) "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			
	(§18.2-186.6(A))	would permit access to a resident's financial	system if encrypted information is accessed and	(§18.2-186.6(E))  Breaches of payroll	and advises the individual or entity that the notice will	Substitute notice: "Substitute notice consists of all of the	the Gramm-Leach- Bliley Act (15 U.S.C. § 6801 et	State Corporation Commission." (§18.2-186.6(K))			





Virginia										
State Statute	What entities are covered? Is there a	What data are covered?	Has there been a breach? Is there a risk of harm	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private		
	requirement for		a risk of harm analysis?		nouce be delayed:	available?	sale narbor:	right of action?		
	service		anarysis.			avanabic.		right of action.		
	providers?									
	1	accounts."	acquired in an	data:	impede a criminal or	following:	seq.) and maintains	Private right of		
	Service provider	(§18.2-186.6(A))	unencrypted form,	"Notwithstanding any	civil investigation, or	a. E-mail notice if	procedures for	action: Yes.		
	requirement:		or if the security	other provision of	homeland or national	the individual or the	notification of a	"Nothing in this		
	Yes. "An	Exception:	breach involves a	this section, any	security. Notice shall	entity has e-mail	breach of the	section shall limit		
	individual	Personal	person with access	employer or payroll	be made without	addresses for the	security of the	an individual from		
	or entity that maintains	information "does not include	to the encryption key and the	service provider that owns or licenses	unreasonable delay after the law	members of the affected class of	system in accordance with the	recovering direct economic damages		
	computerized data	information that is	individual or entity	computerized data	enforcement agency	residents;	provision of that	from a violation of		
	that includes	lawfully obtained	reasonably believes	relating to income tax	determines that the	b. Conspicuous	Act and any rules,	this section."		
	personal	from publicly	that such a breach	withheld pursuant to	notification will no	posting of the notice	regulations, or	(§18.2-186.6(I))		
	information	available	has caused or will	Article 16 (§ 58.1–	longer impede the	on the website of	guidelines	(310.2 100.0(1))		
	that the individual	information, or	cause identity theft	460 et seq.) of	investigation or	the individual or the	promulgated thereto			
	or entity does not	from federal, state,	or other fraud to any	Chapter 3 of Title	jeopardize national	entity if the	shall be deemed to			
	own or license	or local	resident of the	58.1 shall notify the	or homeland	individual or the	be in compliance			
	shall notify the	government	Commonwealth."	Office of the	security."	entity maintains a	with this section."			
	owner or licensee	records lawfully	(§18.2-186.6(C))	Attorney General	(§18.2-186.6(B))	website; and	(§18.2-186.6(G))			
	of the information	made available to	<b>.</b>	without unreasonable		c. Notice to major	"An entity that			
	of any breach of	the general	Exception:	delay after the		statewide media."	complies with the			
	the security of the system without	public."	"Good faith acquisition of	discovery or notification of		(§18.2-186.6(A))	notification			
	unreasonable	(§18.2-186.6(A))	personal	unauthorized access		Notice contents	requirements or procedures			
	delay following		information by an	and acquisition of		requirement:	pursuant to the			
	discovery of the		employee or agent	unencrypted and		"The notice shall	rules, regulations,			
	breach of the		of an individual or	unredacted		include a	procedures, or			
	security of the		entity for the	computerized data		description of the	guidelines			
	system, if the		purposes of the	containing a taxpayer		following:	established by the			
	personal		individual or entity	identification number		(1) The incident in	entity's primary or			
	information		is not a breach of	in combination with		general terms;	functional state or			
	was accessed and		the security of the	the income tax		(2) The type of	federal regulator			
	acquired by an		system, provided	withheld for that		personal	shall be in			
	unauthorized		that the personal	taxpayer that		information	compliance with			
	person or the individual or		information is not	compromises the confidentiality of		that was subject to the unauthorized	this section."			
	entity		used for a purpose other than a lawful	such data and that		access or	(§18.2-186.6(H))			
	reasonably		purpose of the	creates a reasonable		access of acquisition;				
	believes the		individual or entity	belief that an		(3) The general acts				
	personal		or subject to further	unencrypted and		of the business to				
	information was		unauthorized	unredacted version of		protect the personal				

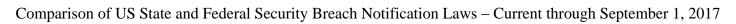




	Virginia										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?			
	accessed and acquired by an unauthorized person." (§18.2-186.6(D))  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		disclosure." (§18.2-186.6(A))  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))	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 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		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))					



				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))				

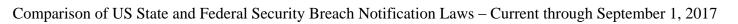




	Virgin Islands (US)										
State Statute	What entities are covered? Is	What data are covered?	Has there been a breach? Is there	Who receives notice?	When must notice be given?	How must notice be given? Is	Is there an exemption or	Enforcement? Penalties? Is			
	there a		a risk of harm		May notice be	substitute notice	safe harbor?	there a private			
	requirement for		analysis?		delayed?	available?		right of action?			
	service										
	providers?										
14 V.I.C. §2208	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	Local			
	"Any agency that	information:	A "breach of the	To any "resident of	Notice must be	"[N]otice' may be	own notification	enforcement: "Any			
	owns or licenses	"[A]n individual's	security of the	the Virgin Islands	given "in the most	provided by one of	method: Yes.	business that			
	computerized data	first name or first	system' means	whose unencrypted	expedient time	the following	If an agency	violates, proposes			
	that includes personal	initial and last name in combination with	unauthorized acquisition of	personal information was, or	possible and without	methods: (1) Written notice.	"maintains its own notification	to violate, or has violated this title			
	information."	any one or more of	computerized data	is reasonably	unreasonable delay,	(2) Electronic	procedures as part	may be enjoined."			
	(§2208(a))	the following data	that compromises	believed to have	consistent with the	notice, if the notice	of an information	(§2211(b))			
	(32200(4))	elements, when	the security,	been, acquired by	legitimate needs of	provided is	security policy for	(3-211(0))			
	Service provider	either the name or	confidentiality, or	an unauthorized	law enforcement, as	consistent with the	the treatment of	Private right of			
	requirement: Yes.	the data elements	integrity of personal	person."	provided in	provisions	personal	action: Yes.			
	"Any agency that	are not encrypted:	information	(§2208(a))	[§2208(c)], or any	regarding electronic	information and is	"Any customer			
	maintains	(1) Social Security	maintained by the	(0 (7)	measures necessary	records and	otherwise	injured by a			
	computerized data	number.	agency."	Credit reporting	to determine the	signatures set forth	consistent with the	violation of this			
	that includes	(2) Driver's license	(§2208(d))	agency notice	scope of the breach	in section 7001 of	timing requirements	title may commence			
	personal	number.		requirement: No.	and restore the	Title 15 of the	of this part shall be	a civil action to			
	information that the	(3) Account	Exception: "Good		reasonable integrity	United States Code.	deemed to be in	recover damages."			
	agency does not own shall notify the	number, credit or debit card number,	faith acquisition of personal	Government	of the data system." (§2208(a))	(3) Substitute notice, if the agency	compliance with the notification	(§2211(a))			
	owner or licensee	in combination with	information by an	notice	(§2208(a))	demonstrates that	requirements of this				
	of the information	any required	employee or agent	requirement: No.	Delay:	the cost of	section if it notifies				
	of any breach of the	security code,	of the agency for		Notification may be	providing notice	subject persons in				
	security of the data	access code, or	the purposes of the		delayed "if a law	would exceed	accordance with its				
	immediately	password that	agency is not a		enforcement agency	\$100,000, or that	policies in the event				
	following	would permit	breach of the		determines that the	the affected class of	of a breach of				
	discovery, if the	access to an	security of the		notification will	subject persons to	security of the				
	personal	individual's	system, provided		impede a criminal	be notified exceeds	system."				
	information was, or	financial account."	that the personal		investigation. The	50,000, or the	(§2208(h))				
	is reasonably	(§2208(e))	information is not		notification	agency does not					
	believed to have	E	used or subject to		required by this	have sufficient	For following				
	been, acquired by an unauthorized	Exception: Personal	further unauthorized		section must be	contact information."	interagency guidelines: No.				
	person."	information does	disclosure."		made after the law enforcement agency	(§2208(g))	guidennes: No.				
	(§2208(b))	not include	(§2208(d))		determines that it	(\$2200(8))					
	(32200(0))	"publicly available	(32200(d))		will not	Substitute notice:					
		information that is	Risk of harm		compromise the	"Substitute notice					
		lawfully made	analysis: No.		investigation."	shall consist of all					
		available to the			(§2208(a))	of the following:					

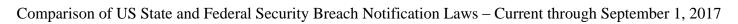


			V	irgin Islands (U	S)			
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute 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))		



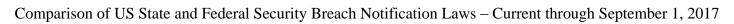


	Washington										
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?			
	providers?										
Was. Rev. Code. §19.255.010 et seq.	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))  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	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 (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))  Exception:  "[D]oes not	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))  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))	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))  * 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))  Credit reporting agency notice requirement: No.  Government notice	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))  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	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."	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 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))  For following interagency guidelines: Yes "A covered entity	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))  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)) "The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law."			
	been, acquired by an unauthorized person." (§19.255.010(2))	include publicly available information that is lawfully made	Risk of harm analysis: Yes. "Notice is not required if the	"Any person or business that is required to issue a	notification will impede a criminal investigation. The notification required	(§19.255.010(8))  Substitute notice: "Substitute notice	under the federal health insurance portability and accountability act of	(§19.255.010(13) (c))			



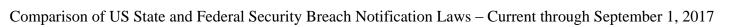


Washington										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute 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		





				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?
						contact information of the reporting person or business subject to this section; (ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; and (iii) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information." (§19.255.010(14))	notwithstanding the notification requirement in subsection (16) of this section." (§19.255.010(10)) "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 23 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part 24 364, Appendix	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." (§19.255.020)(3) (a))  Special liability for vendors to financial institutions: "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

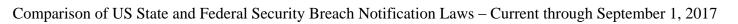




	Washington										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute 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))			

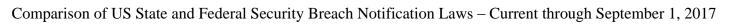


	Washington										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute 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))				



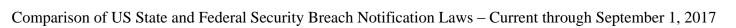


	West Virginia									
State Statute	What entities are covered? Is there a requirement for	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?		
	service providers?		unary sis-			uvunusie.		right of action.		
W. Va. Code §46A- 2A-101 et seq.	Covered entities: "An individual or entity* that owns or licenses computerized data that includes personal information." (§46A-2A-102(a))  * "Entity' includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governmental subdivisions, agencies or instrumentalities, or any other legal entity, whether for profit." (§46A-2A-101(2))  Service provider	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))	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))  "An individual or entity must give notice of the breach of the security of	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))  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	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 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))  Delay: 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."	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	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))  For following interagency guidelines: Yes "An entity that complies with the notification requirements or requirements or	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))  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))		
	requirement: Yes.		the system if	Title V of the Gramm	Notification "must be	that the individual	procedures pursuant	(3 1011 211 104(0))		





	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?			
	"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))	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))	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))  * "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."	Leach Bliley Act." (§46A-2A-102(f))  Government notice requirement: No.	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))	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))  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 if the individual or the entity maintains a website; or (iii) Notice to major statewide media." (§46A-2A-101(7))  Notice contents requirement: "The notice shall include: (1) To the extent possible, a	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))	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))			

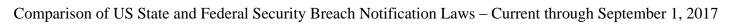




				West Virginia	a			
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	providers:		(§46A-2A-101(3))			description of the		
			** "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			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;		
			the personal information." (§46A-2A-101(8))  Exception: "Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the			(2) A telephone number or website address that the individual may use to contact the entity or the agent of the entity and from whom the individual may learn: (A)What types of information the		
			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			entity maintained about that individual or about individuals in general; (B)Whether or not the entity maintained information about that individual; (3) The toll-free		

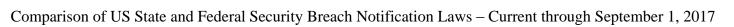


	West Virginia										
State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?			
			or subject to further unauthorized disclosure." (§46A-2A-101(1))  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))			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))					





	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	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	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, or any security code,	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 of personal information pertaining to the resident of [Wisconsin] who is the subject of the personal information." (§§134.98(2)(a), (b))  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))	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))  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	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))  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."	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))  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))  "Upon written request by a person who has received a	For establishing own notification method: No.  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))	Enforcement: Not specified.  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))  Private right of action: No.			



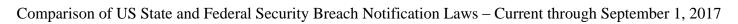


	Wisconsin										
State Statute	What entities are covered? Is there a	What data are covered?	Has there been a breach? Is there a risk of harm	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice	Is there an exemption or safe harbor?	Enforcement?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

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

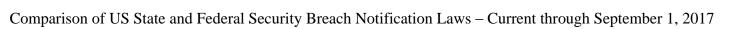


	Wisconsin										
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?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



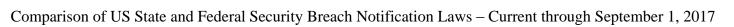


				Wyoming				
State Statute	What entities are covered? Is	What data are covered?	Has there been a breach? Is there	Who receives notice?	When must notice be given? May	How must notice be given? Is	Is there an exemption or	Enforcement? Penalties? Is
	there a		a risk of harm		notice be delayed?	substitute notice	safe harbor?	there a private
	requirement for		analysis?			available?		right of action?
	service							
	providers?							
Wyoming	Covered entities:	Personal	Breach definition:	Residents:	Timing:	Method:	For establishing	State enforcement:
Statutes 40-12-	"An individual or	identifying	"Breach of the	The affected	"[W]hen [an entity]	"[N]otice to	own notification	"The attorney
501 et seq.	commercial entity	information:	security of the data	Wyoming resident.	becomes aware of a	consumers may be	method: No.	general may bring
	that conducts	"Personal	system' means	(§40-12-502(a)).	breach of the security	provided by one (1)	E. C. H	an action in law or
	business in Wyoming and that	identifying information'	unauthorized acquisition of	Credit reporting	of the system, [it shall] conduct in	of the following methods:	For following interagency	equity to address any violation of this
	owns or licenses	means the first	computerized data	agency notice	good faith a	(i) Written notice;	guidelines: Yes.	section and for other
	computerized data	name or first	that materially	requirement: No.	reasonable and	(ii) Electronic mail	"Any financial	relief that may be
	that includes	initial and last	compromises the	requirement. 10.	prompt investigation	notice;	institution as	appropriate to
	personal	name of a person	security,	Government notice	to determine the	(iii) Substitute	defined in 15 U.S.C.	ensure proper
	identifying	in combination	confidentiality or	requirement: No.	likelihood that	notice, if the person	6809 or federal	compliance of this
	information about	with one (1) or	integrity of personal	_	personal identifying	demonstrates:	credit union as	section to recover
	a resident of	more of the data	identifying		information has been	(A) that the cost of	defined by 12	damages, or both.
	Wyoming"	elements specified	information		or will be misused. If	providing notice	U.S.C. 1752 that	The provisions of
	(§40-12-502(a))	in W.S. 6-3-	maintained by a		the investigation	would exceed	maintains	this section are not
		901(b)(iii) through	person or business		determines that the	\$10,000 for	notification	exclusive and do not
	Service provider	(xiv) [as listed	and causes or is		misuse of personal	Wyoming-based	procedures subject	relieve an individual
	requirement:	below], when the	reasonably believed		identifying	persons or	to the requirements	or a commercial
	Yes. "Any person	data elements are	to cause loss or		information about a	businesses, and	of 15 U.S.C.	entity subject to this
	who maintains computerized data	not redacted."* (§40-12-501(a)	injury to a resident of [Wyoming]."		Wyoming resident has occurred or is	\$250,000 for all other businesses	6801(b)(3) and 12 C.F.R. Part 364	section from compliance with all
	that includes	(§40-12-301(a) (vii))	(§40-12-501(a)(i))		reasonably likely to	operating but not	Appendix B or Part	other applicable
	personal	(VII))	(§40-12-301(a)(1))		occur, the individual	based in	748 Appendix B, is	provisions of law."
	identifying	The listed data	Exception: "Good		or the commercial	Wyoming;	deemed to be in	(§40-12-502(f))
	information on	elements include:	faith acquisition of		entity shall give	(B) that the	compliance with	(3 10 12 302(1))
	behalf of another	"(iii) Social	personal identifying		notice as soon as	affected class of	this section if the	Private right of
	business entity	security number;	information by an		possible to the	subject persons to	financial institution	action: No.
	shall disclose to	(iv) Driver's	employee or agent		affected Wyoming	be notified exceeds	notifies affected	
	the business entity	license number;	of a person or		resident. Notice shall	10,000 for	Wyoming	
	for which the	(v) Account	business for the		be made in the most	Wyoming-based	customers in	
	information is	number, credit	purposes of the		expedient time	persons or	compliance with the	
	maintained any	card number or	person or business		possible and without	businesses and	requirements of 15	
	breach of the	debit card number	is not a breach of		unreasonable delay,	500,000 for all	U.S.C. 6801	
	security of the	in combination	the security of the		consistent with the	other businesses	through 6809 and	
	system as soon as	with any security	data system,		legitimate needs of law enforcement and	operating but not based in	12 C.F.R. Part 364 Appendix B or Part	
	practicable	code, access code or password that	provided that the personal identifying		consistent with any		748 Appendix B."	
	following the determination that	would allow	information is not		measures necessary	Wyoming; or (C) the person	(§40-12-502(c))	
	determination that	would allow	imormation is not		measures necessary	(C) the person	(840-12-302(C))	





	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))					





				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?
		(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; (xiii) Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes; (xiv) An individual taxpayer identification number." (§6-3-901(b)) *"Redact' means				Notice contents requirement: "[Notice] shall be clear and conspicuous and shall include, at a minimum: (i) A toll-free number: (A) that the individual may use to contact the person collecting the date, or his agent; and (B) from which the individual may learn the toll free contact telephone numbers and addresses for the major credit reporting agencies. (ii) The types of personal identifying information that were or are reasonably believed to have been the subject of the breach; (iii) A general description of the breach incident; (iv) The		
		alteration or				approximate date of		



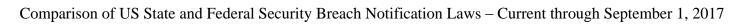
				Wyoming				
State Statute	What entities are covered? Is there a requirement for service	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?
	providers?							
	provided	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))  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))				the breach of security, if that information is reasonably possible to determine at the time notice is provided; (v) In general terms, the actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches; (vi) Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports; (vii) Whether notification was delayed as a result of a law enforcement investigation, if that information is reasonably possible to determine at the time the notice is provided. (§40-12-502(e))		



				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?
						* 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: (A) email notice when the business has an email address for the affected person; (B) conspicuous posting on the business's website; and (C) publication in local or statewide media.		

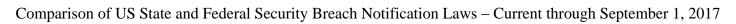


	Gramm-Leach-Bliley Act (GLBA)										
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial 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, et seq.	Covered entities: "[F]inancial institution[s]." (§ 6801(a))  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	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))  Exception: "Nonpublic personal information does not include publicly available information." (§6809(4)(B))	"[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))  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	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))	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))	"[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	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))	State and Federal enforcement:  "(a) In General. Subject to subtitle B of the Consumer Financial Protection Act of 2010 [12 U.S.C. 5511 et seq.], 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			



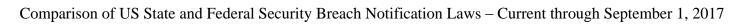


	Gramm-Leach-Bliley Act (GLBA)										
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial 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 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		[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	poncies?		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		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			
	any subsidiaries of such entities (except brokers, dealers, persons		functions on behalf of the financial institution, including marketing			the information may be provided pursuant to [the general exceptions		foreign banks), commercial lending companies			



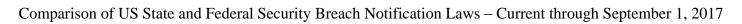


			Gramm-	Leach-Bliley Act	(GLBA)			
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial 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			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)		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
			sharing of account number			of this title." (§6803(c))		foreign banks, and any



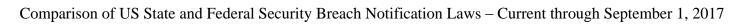


	Gramm-Leach-Bliley Act (GLBA)										
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial institutions provide the disclosure? What must it contain?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?			
			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))  General exceptions:  "[Disclosure of nonpublic personal information is permitted]:  (1) as necessary to effect, administer, or enforce a transaction					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			



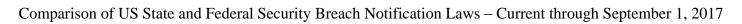


			Gramm-	Leach-Bliley Act	(GLBA)			
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial 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 respect to investment Advisers Act of 1940 [15 U.S.C.A. § 80b-1 et seq.], by the Securities and Exchange Commission with



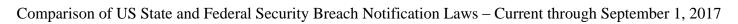


	Gramm-Leach-Bliley Act (GLBA)										
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial 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			





	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?			
			fiduciary or representative capacity on behalf of the consumer;  (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;  (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 et seq.], to law enforcement agencies (including					subsection.  (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.  (b) Enforcement of section 6801.  (1) In general. Except as provided in paragraph (2), the agencies and authorities described in subsection (a),			





	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 et seq.], or (B) from a consumer 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			

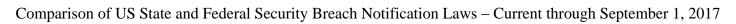


	Gramm-Leach-Bliley Act (GLBA)										
Statute	What entities are covered?	What data are covered?	Prohibition against disclosing nonpublic personal information	To whom must financial institutions disclose their nonpublic personal information policies?	When must this disclosure be given?	How must financial 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.			

	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))									

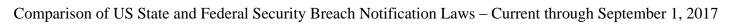


		Health	<b>Insurance Porta</b>	bility and Accoun	tability Act of 199	6 (HIPAA)		
Federal	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
Statute	are covered?	covered?	breach? Is there	notice?	be given? May	be given? What	exemption or	Penalties? Is
			a risk of harm		notice be delayed?	must it contain?	safe harbor?	there a private
			analysis?		v			right of action?
45 CFR §§	Covered entities:	Protected health	Breach definition:	Notice must be	Timing:	Method:	Safe harbor for	Federal
160.103,	"Covered entity	information:	"Breach means the	given to:	"[A] covered entity	"(1) Written notice.	encryption/	enforcement:
164.400-414, 42	means:	"Protected health	acquisition, access,	- "[E]ach individual	shall provide the	(i) Written	destruction of	Penalties imposed
USC §1320d, et	(1) A health plan.	information'*	use, or disclosure of	whose unsecured	required notification	notification by	data: Yes.	by HHS Secretary.
seq.	(2) A health care	means individually	protected health	protected health	without unreasonable	first-class mail to	"Unsecured	"(A) if it is
	clearinghouse.	identifiable health	information in a	information has been,	delay and in no case	the individual at	protected health	established that the
	(3) A health care	information:**	manner not	or is reasonably	later than 60 calendar	the last known	information means	person did not know
	provider who	(1) Except as	permitted under	believed by the	days after discovery	address of the	protected health	(and by exercising
	transmits any	provided in	subpart E of this	covered entity to	of a breach."	individual or, if	information that is	reasonable diligence
	health information	paragraph (2) of	part [§164.500]	have been, accessed,	(§164.404(b))	the individual	not rendered	would not have
	in electronic form	this definition, that	which compromises	acquired, used, or		agrees to	unusable,	known) that such
	in connection with	is:	the security or	disclosed as a result	Discovery:	electronic notice	unreadable, or	person committed a
	a transaction	(i) Transmitted	privacy of the	of [a] breach."	"[A] breach shall be	and such	indecipherable* to	violation, they will
	covered by the	by electronic	protected health	(§164.404(a)(1))	treated as discovered	agreement has not	unauthorized	be fined at least
	HIPAA."	media;	information."		by a covered entity as	been withdrawn,	persons through the	\$100 per violation,
	(§160.103)	(ii) Maintained in	(§164.402)	Government notice	of the first day on	by electronic mail.	use of a technology	but not more than
		electronic media;		requirement: Yes.	which such breach is	The notification	or methodology	\$1.5 million total.
	Business	or	Exception:	"(a) Standard: A	known to the covered	may be provided	specified by the	(B) in the case of a
	associate notice	(iii) Transmitted	"Breach excludes:	covered entity shall,	entity, or, by	in one or more	Secretary in the	violation of such
	requirement:	or maintained in	(i) Any	following the	exercising reasonable	mailings as	guidance issued	provision in which
	"(1) A business	any other form or	unintentional	discovery of a breach	diligence would have	information is	under section	it is established that
	associate* shall,	medium.	acquisition, access,	of unsecured	been known to the	available.	13402(h)(2) of	the violation was
	following the	(2) Protected health information	or use of protected	protected health information as	covered entity. A	(ii) If the covered	Public Law 111-5 on the HHS	due to reasonable
	discovery of a breach of	excludes	health information by a workforce	provided in	covered entity shall be deemed to have	entity knows the individual is	website."	cause and not to willful neglect, they
	unsecured	individually	member or person	§ 164.404(a)(2),	knowledge of a	deceased and has	(§164.402)	will be fined at least
	protected health	identifiable health	acting under the	notify the Secretary	breach if such breach	the address of the	"Protected health	\$1,000 per
	information, notify	information in:	authority of a	of Health and	is known, or by	next of kin or	information (PHI) is	violation, but not
	the covered entity	(i) Education	covered entity or a	Human Services].	exercising reasonable	personal	rendered unusable,	more than \$1.5
	of such breach.	records covered	business associate,	(b) Implementation	diligence would have	representative of	unreadable, or	million total.
	(2) For purposes	by the Family	if such acquisition,	specifications:	been known, to any	the individual (as	indecipherable	(C) in the case of a
	of paragraph (1) of	Educational	access, or use was	Breaches involving	person, other than the	specified under	only if one or more	violation of such
	this section, a	Rights and	made in good faith	500 or more	person committing	§164.502(g)(4) of	of the following	provision in which
	breach shall be	Privacy Act, as	and within the scope	individuals: For	the breach, who is a	subpart E), written	applies:	it is established that
	treated as	amended, 20	of authority and	breaches of	workforce member or	notification by	(a) Electronic PHI	the violation was
	discovered by a	U.S.C. 1232g;	does not result in	unsecured protected	agent of the covered	first-class mail to	has been encrypted	due to willful
	business associate	(ii) Records	further use or	health information	entity (determined in	either the next of	as specified in the	neglect—
	as of the first day	described at 20	disclosure in a	involving 500 or	accordance with the	kin or personal	HIPAA Security	(i) if the violation
	on which such	U.S.C.	manner not	more individuals, a	federal common law	representative of	Rule by the use	is corrected as



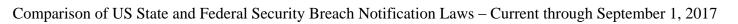


		Health	Insurance Porta	bility and Accoun	tability Act of 199	6 (HIPAA)		
Federal	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
Statute	are covered?	covered?	breach? Is there	notice?	be given? May	be given? What	exemption or	Penalties? Is
			a risk of harm		notice be delayed?	must it contain?	safe harbor?	there a private
			analysis?					right of action?
	breach is known to	1232g	permitted under	covered entity shall	of agency)."	the individual. The	of an algorithmic	described in
	the business	(a)(4)(B)(iv); and	subpart E	provide the	(§164.404(a)(2))	notification may	process to	subsection
	associate or, by	(iii) Employment	[§164.500] of this	notification required		be provided in one	transform data into	(b)(3)(A), a
	exercising	records held by a	part;	by paragraph (a) of	Delay for law	or more mailings	a form in which	penalty in an
	reasonable	covered entity in	(ii) Any inadvertent	this section	enforcement:	as information is	there is a low	amount that is at
	diligence, would	its role as	disclosure by a	contemporaneously	"If a law enforcement	available.	probability of	least the amount
	have been known	employer".	person who is	with the notice	official states to a	(2) Substitute	assigning meaning	described in
	to the business	(§160.103)	authorized to access	required by	covered entity or	notice. In the case in	without use of a	paragraph (3)(C)
	associate. A		protected health	§ 164.404(a) and in	business associate	which there is	confidential	but not to exceed
	business associate	* Health	information at a	the manner specified	that a notification,	insufficient or out-	process or key and	the amount
	shall be deemed to	information:	covered entity or	on the HHS Web site.	notice, or posting	of-date contact	such confidential	described in
	have knowledge of	"Health	business associate	(c) Implementation	required under this	information that	process or key that	paragraph (3)(D);
	a breach if the	information means	to another person	specifications: For	subpart would	precludes written	might enable	and
	breach is known,	any information,	authorized to access	breaches of	impede a criminal	notification to the	decryption has not	(ii) if the violation
	or by exercising	including genetic	protected health	unsecured protected	investigation or cause	individual under	been breached.	is not corrected as
	reasonable	information,	information at the	health information	damage to national	paragraph (d)(1)(i)	Encryption	described in such
	diligence would	whether oral or	same covered entity	involving less than	security, a covered	of this section, a	processes	subsection, a
	have been known,	recorded in any	or business	500 individuals, a	entity or business	substitute form of	identified below	penalty in an
	to any person,	form or medium,	associate, or	covered entity shall	associate shall:	notice reasonably	have been tested	amount that is at
	other than the	that:	organized health	maintain a log or	(a) If the statement is	calculated to reach	by the National	least the amount
	person committing	(1) is created or	care arrangement in	other documentation	in writing and	the individual shall	Institute of	described in
	the breach, who is	received by a	which the covered	of such breaches and,	specifies the time for	be provided.	Standards and	paragraph (3)(D)."
	an employee,	health care	entity participates,	not later than 60 days	which a delay is	Substitute notice	Technology	(42 U.S.C. §1320d–
	officer, or other	provider, health	and the information	after the end of each	required, delay such	need not be	(NIST) and judged	5(a)(1))
	agent of the	plan, public health	received as a result	calendar year,	notification, notice,	provided in the case	to meet this	
	business associate	authority,	of such disclosure is	provide the	or posting for the	in which there is	standard.	Private right of
	(determined in	employer, life	not further used or	notification required	time period specified	insufficient or out-	(i) Valid	action: No.
	accordance with	insurer, school or	disclosed in a	by paragraph (a) of	by the official; or	of-date contact	encryption	However, at least
	the Federal	university, or	manner not	this section for	(b) If the statement is	information that	processes for	one state supreme
	common law of	health care	permitted under	breaches occurring	made orally,	precludes written	data at rest are	court has held that
	agency)."	clearinghouse; and	subpart E	during the preceding	document the	notification to the	consistent with	the HIPAA can
	(§164.410(a))	(2) relates to the	[§164.500] of this	calendar year, in the	statement, including	next of kin or	NIST Special	provide the standard
	* Business	past, present, or	part;	manner specified on	the identity of the	personal	Publication 800–	of care for common
	* Business associate:	future physical or mental health or	(iii) A disclosure of protected health	the HHS Web site." (§164.408)	official making the statement, and delay	representative of the individual under	111, Guide to Storage	law negligence claims against
	"(1) Except as	condition of an	information where a	(8104.408)	the notification,			health care
	provided in	individual; the	covered entity or		notice, or posting	paragraph (d)(1)(ii). (i) In the case in	Encryption Technologies for	providers and does
	paragraph (2) of	provision of health	business associate		temporarily and no	which there is	End User Devices.	not preempt these
	this definition,	care to an	has a good faith		longer than 30 days	insufficient or out-	(ii) Valid	claims. See Byrne
	business associate	individual; or the	belief that an		from the date of the	of-date contact	( )	v. Avery Ctr. for
	business associate	marvioual, of the	oenei mat an		from the date of the	or-date contact	encryption	v. Avery Cir. jor





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





		Health	<b>Insurance Portal</b>	bility and Accou	ntability Act of 199	06 (HIPAA)		
Federal	What entities	What data are	Has there been a	Who receives	When must notice	How must notice	Is there an	Enforcement?
Statute	are covered?	covered?	breach? Is there	notice?	be given? May	be given? What	exemption or	Penalties? Is
			a risk of harm		notice be delayed?	must it contain?	safe harbor?	there a private
			analysis?		ľ			right of action?
	utilization	the provision of	involved, including			number that	media have been	Ü
	review, quality	health care to an	the types of			remains active	shredded or	
	assurance,	individual; and	identifiers and the			for at least 90	destroyed	
	billing, benefit	(i) identifies the	likelihood of re-			days where an	such that the PHI	
	management,	individual; or	identification;			individual can	cannot be read or	
	practice	(ii) with respect	(ii) The			learn whether the	otherwise cannot	
	management,	to which there is	unauthorized person			individual's	be reconstructed.	
	and repricing;	a reasonable	who used the			unsecured	(ii) Electronic	
	or	basis to believe	protected health			protected health	media have been	
	(B) Any other	the information	information or to			information may	cleared, purged,	
	function or	can be used to	whom the			be included in the	or destroyed	
	activity	identify the	disclosure was			breach.	consistent	
	regulated by	individual."	made;			(3) Additional	with NIST	
	this subchapter;	(§160.103)	(iii) Whether the			notice in urgent	Special	
	or		protected health			situations. In any	Publication 800–	
	(ii) Provides,		information was			case deemed by the	88, Guidelines	
	other than in the		actually acquired or			covered entity to	for Media	
	capacity of a		viewed; and			require urgency	Sanitization, such	
	member of the		(iv) The extent to			because of possible	that the PHI	
	workforce of		which the risk to the			imminent misuse of	cannot be	
	such covered		protected health			unsecured protected	retrieved."	
	entity, legal,		information has			health information,	74 Fed. Reg. 19009	
	actuarial,		been mitigated."			the covered entity	(April 27, 2009) (as	
	accounting,		(§164.402)(2))			may provide	amended by 78 Fed.	
	consulting, data					information to	Red. 5695 (Jan. 25,	
	aggregation (as defined in §					individuals by	2013)); see also	
	164.501 of this					telephone or other	http://www.csrc.nist	
	subchapter),					means, as appropriate, in	.gov	
	management,					addition to notice		
	administrative,					provided under		
	accreditation, or					paragraph (d)(1) of		
	financial services					this section."		
	to or for such					(§164.404)(d))		
	covered entity, or					(3104.404)(a))		
	to or for an					Notice contents		
	organized health					requirement:		
	care arrangement					"(A) A brief		
	in which the					description of what		
	covered entity					happened, including		

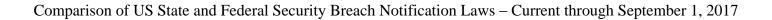


Statute are covered? covered? breach? Is there a risk of harm notice? be given? May notice be delayed? be given? What exemption or safe harbor?	
participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.  (2) A covered entity participating (2) the discovery of the breach and the date of the discovery of the breach, if known; individually if the breach, if known; individually individua	Enforcement? Penalties? Is there a private
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.  (2) A covered entity participating entity or other types of entity participating entity or other types of entity participating entity or earlier of the types of entity participating entity entities entity	right of action?
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.  (2) A covered entity participating entity of individually of the types 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	6
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.  (2) A covered entity participating  the breach, if known; (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	
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.  (2) A covered entity or arrangement or for arrangement or arrangement, to the person.  (2) A covered entity or arrangement or from another business associate of such covered entity or arrangement, to the person.	
individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. (2) A covered entity participating  (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	
identifiable health health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to from another  business associate of such covered entity or arrangement, to from another  business associate of such covered entity or arrangement, to from another  covered entity or arrangement, to the person.  (2) A covered entity participating  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	
health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.  (2) A covered entity participating  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 entity participating	
information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.  (2) A covered entity participating entity participating entity or such covered entity participating entity or entity or entity or entity participating entity entity or entity	
such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.  (2) A covered entity participating  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	
entity or arrangement, or from another business business covered entity or arrangement, to the person.  (2) A covered entity participating	
arrangement, or from another business security number, date of birth, home address, account number, diagnosis, the person.  (2) A covered entity participating as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were	
from another business associate of such covered entity or arrangement, to the person.  (2) A covered entity participating  from another security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were	
business associate of such covered entity or arrangement, to the person. (2) A covered entity participating	
associate of such covered entity or arrangement, to the person.  (2) A covered entity participating date of birth, home address, account number, diagnosis, disability code, or other types of information were	
covered entity or arrangement, to the person.  (2) A covered entity participating address, account number, diagnosis, disability code, or other types of information were	
arrangement, to the person. (2) A covered entity participating  number, diagnosis, disability code, or other types of information were	
the person. (2) A covered other types of entity participating information were	
(2) A covered other types of information were	
entity participating information were	
In an organized   Involved):	
health care (C) Any steps	
arrangement that individuals should	
performs a take to protect	
function or themselves from	
activity as potential harm	
described by resulting from the	
paragraph (1)(i) of this definition for breach; (D) A brief	
or on behalf of description of what	
such organized the covered entity	
health care involved is doing to	
arrangement, or involved is doing to investigate the	
that provides a breach, to mitigate	
service as harm to individuals,	
described in and to protect	
paragraph (1)(ii)	
of this definition breaches; and	
to or for such (E) Contact	
organized health procedures for	



		Health	<b>Insurance Portal</b>	bility and Accou	ntability Act of 199	06 (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)					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))  Plain language requirement: The notification shall be written in "plain language." (§164.404(c)(2))  Notification to the Media: "(a) Standard. 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) Implementation specification: Timeliness of notification. Except		

	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) Implementation specifications: Content of notification. 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.