

Outline of State Consumer Notification Laws

	Entities Covered	Entities Covered by Federal Law	Security Breach	Definition of Personal Information	Timing of Notification	Method of Notice	Safe Harbor for Company's Notification System	Notify Consumer Reporting Agencies	Duty of Non-Owner Who Maintain the Data	Penalties and Enforcement	Other Provision
California - S.B. 1386 (§1798.82)	“Any person or business that conducts business in California, and that owns or licenses computerized data” (§1798.82(d))	no exemption	“unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information” (§1798.82(d))	Non-public (f) unencrypted “personal information” defined somewhat broadly (e)	“most expedient time possible” and without unreasonable delay” (a) UNLESS inconsistent with law enforcement needs (c)	writing; electronically; or substitute notice (e-mail, company website and state-wide media) (g)	yes, as long as consistent with law’s timing requirements (h)	not required	notify owner of information immediately after security breach (b)	Customer can bring civil action under California's Business and Professions Code §17200, including for attorneys' fees	N/A
Arkansas SB 1167- (4-110)-	similar to California-105(a)(1); includes agencies 103(9)	exemption for state or federal rules, but only if they are at least as stringent (§106)	Same as California (103)	Same as California but “personal information” includes “medical information” (103(5))	Same as California (105(a)(2))	Same as California (105(e))	Same as California (105(f))	not required	Same as California (105(b))	Attorney General can seek any remedies (§108)	<u>Exemption</u> : not required to notify if after “reasonable investigation” no reasonable likelihood of harm to customers (§105(d))
Conn. S.B. 650 (47-18-21) * not signed by governor yet	Similar to California- "Any person who..., owns, maintains or licenses computerized data” (§4(a))	no exemption	Same as California (§3(1))	Same as California (§3(2))	Not later than 15 days, unless request by law enforcement office (§4(a))	Same as California (§4(a)) <u>except</u> substitute notice allowed if over 100 affected and only must notify media and website (§4(a))	NONE	not required	<u>Same duty to notify as owners</u>	Failure to notify constitutes an unfair or deceptive trade practice (§4(b))	N/A

	Entities Covered	Entities Covered by Federal Law	Security Breach	Definition of Personal Information	Timing of Notification	Method of Notice	Safe Harbor for Company's Notification System	Notify Consumer Reporting Agencies	Duty of Non-Owner Who Maintain the Data	Penalties and Enforcement	Other Provision
Delaware H.B. 116 (12B-101)	Similar to California- "Any person or a commercial entity" (12B-102)(a))	exemption for state or federal rules (12B-103(b))	Same as California (12B-101(1))	Same as California (12B-101(3))	notify only after "conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused" (12B-102(a))	Same as California except: 1. Allows telephonic notice 2. Substitute notice thresholds lowered to \$75,000 or 100,000 residents (12B-101(4))	Same as California (12B-103(a))	not required	Same as California (12B-102(b))	Enforcement by Attorney General, who can bring an action in law or equity to require compliance or get damages (12B-104)	N/A
Florida H.B. 481 (817.5681)	Same as California- 817.5681(1)(a)	following notification procedure subject to a federal regulator sufficient to establish compliance (817.5681(9)(b))	breach must <u>materially</u> compromise security, confidentiality etc. (817.5681(4))	Same as California (817.5681(5))	<u>no later than 45 days</u> following the determination of the breach, otherwise just like California- 817.5681(1)(a)	Same as California (817.5681(5))	Same as California (817.5681(9)(a))	required if more than 1,000 residents affected (817.5681(12))	disclose to business entity and must come to agreement about who will provide notice(817.5681(2)(a))	detailed administrative sanctions for not providing timely notice (817.5681(1)(b))	<u>Exemption</u> : not required to notify if "appropriate investigation" or consultation with federal, state or local agencies determines that "not likely" to result "in harm to the individuals" 817.5681(10)(a)
Georgia - S.B. 230 (10-1-911)	<u>only information brokers covered</u> (911(2))	no exemption	Same as California (911(1))	broader definition of "personal information" than California (911(5))	Same as California (911(3))	Same as California (911(3))	Same as California (911(3))	required if more than 10,000 residents affected (912(d))	Same as California (912(b))	not mentioned	N/A

	Entities Covered	Entities Covered by Federal Law	Security Breach	Definition of Personal Information	Timing of Notification	Method of Notice	Safe Harbor for Company's Notification System	Notify Consumer Reporting Agencies	Duty of Non-Owner Who Maintain the Data	Penalties and Enforcement	Other Provision
Illinois H.B. 1633	“data collectors”- broad definition that covers everything California does (§5)	no exemption	Same as California (§5)	Same as California (§5)	Same as California (§10(a)) <u>except NO needs of law enforcement exemption!</u>	Same as California (§10(c))	Same as California (§10(d))	Not required	Same as California (§10(b))	breach of the Illinois Consumer Fraud and Deceptive Business Practices Act (§20)	N/A
Indiana S.B. 503 (IC-4-1-11)	Applies <u>ONLY</u> to <u>STATE AGENCIES</u> (4-1-11(2))	N/A	Same as California- (4-1-11(2))	Same as California (4-1-11(5))	similar to California- but only uses “without unreasonable delay” (4-1-11(5))	Same as California- (4-1-11(8))- but no e-mail requirement in substitute notice (4-1-11(9))-	NONE	required if more than 1,000 residents affected (4-1-11(10))	Same as California- (4-1-11(6))	not mentioned	N/A
Louisiana * not signed by governor yet	Same as California (§3074(A))	Financial institutions subject to the Federal Interagency Guidance exempt (§3076)	Same as California (§3073(2))	Same as California (§3073(3)(a))	Same as California (§3074(C))	Same as California (§3074(E))	Same as California (§3074(F))	Not required	Same as California (§3074(B))	creates right of civil action for damages (§3075)	N/A
Minnesota H.F. 2121 (325E.61)	Same as California (§1(1)(a))	exempt if Subject to HIPPA and financial institutions (§1(4))	Same as California (§1(1)(d))	Same as California (§1(1)(e))	Same as California (§1(1)(a))	Same as California (§1(1)(g))	Same as California (§1(1)(h))	Required to notify within 48 hours if more than 500 residents affected (1(2))	Same as California (§1(1)(b))	Attorney General can seek any remedies (§1(6))	N/A

	Entities Covered	Entities Covered by Federal Law	Security Breach	Definition of Personal Information	Timing of Notification	Method of Notice	Safe Harbor for Company's Notification System	Notify Consumer Reporting Agencies	Duty of Non-Owner Who Maintain the Data	Penalties and Enforcement	Other Provision
Montana H.B. 732 (Title 30-14)	Same as California (\$7(1))	no exemption	breach must <u>materially</u> compromise security, confidentiality etc. (\$7(4)(a))	Same as California (\$7(1))	similar to California - "without unreasonable delay" (\$7(1))	Same as California, but allows telephone notice; substitute notice allows "applicable local or statewide media"(\$7(5))	Same as California, except rather than timing requirements, only "not unreasonably delay notice" (\$7(5))	not required	Same as California- (\$7(2))	department can get temporary or permanent injunction; monetary penalties can be impose (\$8)	1. Licensee or Insurance-Support Organization have more stringent reqs.- no "materially" requirement (\$9) 2. If notice indicates customer can obtain copy of credit report, firm must help get report (\$7(7))
Nevada S.B. 347 (Title 52) * not signed by governor yet;	"data collectors"- broad definition that covers everything California does (\$20)	exempt if subject to Gramm-Leach-Bliley (\$24(5)(b))	breach must <u>materially</u> compromise security, confidentiality etc. (\$19)	Same as California- (\$21)	Same as California (\$24(1) and \$24(2))	Same as California- (\$24(4))	Same as California (\$24(5)(a))	required if more than 1,000 residents affected (\$24(6))	Same as California (\$24(2))	Attorney General can get temporary or permanent injunction (\$28)	N/A
New Jersey Assembly, No. 4001 * not signed by governor yet;	Same as California (\$12(a))	no exemption	Similar to California (\$10)	Same to California (\$10)	Same as California (\$12(a)) but must notify Division of State Police in Department of Law and Public Safety (\$12(c))	Same as California (\$12(d))	Same as California (\$12(e))	required if more than 1,000 residents affected (\$12(f))	Same as California (\$12(b))	not mentioned	<u>Exemption</u> : if company establishes that misuse is "not reasonably possible" (12(a))

	Entities Covered	Entities Covered by Federal Law	Definition of Security Breach	Definition of Personal Information	Timing of Notification	Method of Notice	Safe Harbor for Company's Notification System	Notify Consumer Reporting Agencies	Duty of Non-Owner Who Maintain the Data	Penalties and Enforcement	Other Provisions
North Dakota (51-30)	Same as California (51-30-02)	exempts federally regulated financial institutions, trusts, or credit unions (51-30-06)	Same as California (51-30-01)	broader definition of "personal information" than California (51-30-02)	Same as California (51-30-02)	Same as California- (51-30-05)	Same as California (51-30-06)	not required	Same as California (51-30-03)	Attorney General can get injunction, civil penalties (51-30-07)	N/A
Rhode Island H. 6191-SubA/2 * not signed by governor yet;	Same as California (11-49-2-3)	Companies subject to Health Insurance Portability Act or Financial Institutions or any other entity subject to a federal regulator (11-49.2-7)	Same as California (11-49.2-5(b))	Same as California (11-49.2-5(c)) but with no exception for publicly available info	Same as California (11-49.2-3)	Same as California except substitute notice thresholds are \$25,000 or 50,000 people effected (11-49.2-5(d))	Same as California (11-49.2-7)	not required	Same as California, except must notify owner only if "significant risk of identity theft" (11-49.2-3(b))	Civil fines not more than \$100 per occurrence and not more than \$25,000 per defendant (11-49.2-6)	<u>Exemption</u> : If consultation with law enforcement determines that there is no "significant risk of identity theft"
Tennessee S.B. 2220 (47-18-21) * not signed by governor yet;	"information holder"-broad any person, business or agency that owns/licenses computer data (a)(2)	exempt if subject to Gramm-Leach-Bliley (h)	breach must <u>materially</u> compromise security, confidentiality	Same as California (a)(3)	Same as California (b)	Same as California (e)	Same as California (f)	required if more than 1,000 residents affected	Same as California- (c)	personal right of action for those damaged, but cannot sue agencies (g)	N/A

	Entities Covered	Entities Covered by Federal Law	Definition of Security Breach	Definition of Personal Information	Timing of Notification	Method of Notice	Safe Harbor for Company's Notification System	Notify Consumer Reporting Agencies	Duty of Non-Owner Who Maintain the Data	Penalties and Enforcement	Other Provisions
Washington SB 6043 (42.17(§2))	Same as California (§2(1)); (§1) applies to state, county and local agencies	no exemption	Same as California (§2(§4))	Same as California (§2(1))	Same as California (§2(1))	Same as California- (§2(7))	Same as California (§2(8))	not required	Same as California (§2(2))	customer private right of action (§2(10)(a)); injunctions (§2(10)(b))	<u>exemption</u> : do not have to disclose breach if not “reasonably likely” that breach will lead to “risk of criminal activity” (§2(10)(d))
New York City Int. No. 141-A (1-§20-11)	only companies that are licensed or supervised by Department of Consumer Affairs (§20-117(c))	no exemption	Same as California- (§20-117(a)(2))	broad definition of “personal identifying information” (§20-117), with no exception for publicly available info	disclose to police immediately, then to customer “as soon as practicable ” (20-117(e))	1. written; 2. by telephone; 3. e-mail; 4. substitute notice “reasonably targeted to the individual” (20-117(f))	NONE, except as provided in the substitute notice option	not required	must inform data owner of breach and inform Department and police department (§20-117)	fine no more than \$500 and liable for a civil penalty of not more than \$100 for each violation (§20-117(h))	N/A

Outline of Proposed Federal Consumer Notification Laws

	Entities Covered	Relation to State Laws/other Federal Laws	Definition of Security Breach	Definition of Personal Information	Timing of Notification	Method of Notice	Safe Harbor for Company's Notification System	Notify Consumer Reporting Agencies	Duty of Non-Owner Who Maintain the Data	Penalties and Enforcement	Other Provisions
<p><u>Proposed Title IV, Subtitle B of the Specter-Leahy Personal Data Privacy And Security Act Of 2005</u></p>	<p>“Any business entity or agency engaged in interstate commerce that involves collective, accessing, transmitting, storing or disposing of personally identifiable information.” (<i>§421(a)</i>).</p>	<p>Pre-empts state laws on many subjects. Pre-empted provisions include definitions of security breach, method of notice, and risk assessment prevention exemptions. It also pre-empts any state provisions inconsistent with any portion of Title IV (<i>§427</i>).</p>	<p>“compromise of the security, confidentiality, or integrity of computerized data through misrepresentati on or actions that result in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to sensitive personally identifiable information.” (<i>§3(10)</i>).</p>	<p>“sensitive personally identifiable information”- very broad definition including “any name or number used in conjunction with any other information to identify a specific individual” (<i>§3(11)</i>).</p> <p>Includes lists of such information including social security number, biometric data, electronic identification number. (<i>§3(11)</i>)</p>	<p>Same as California (<i>§422(a)</i>), including delay in notification for law enforcement needs (<i>§422(a)</i>)- but cannot delay notice for law enforcement more than 30 days without a written notification from federal law officials</p> <p>If notice to federal law enforcement and state attorneys general is</p>	<p>1. Written notice to individual’s last know address, but if unknown, then via telephone 2. If more than 1,000 residents affected, can notify through “conspicuous posting” on company website 3. If more than 5,000 residents in a state or jurisdiction affected, can notify through major media outlets (<i>§422(b)</i>)</p> <p>Also, if the firm is unable to identify the specific</p>	<p>“fraud prevention” exemption: Do not need to notify (1) if information cannot be used to facilitate further transactions, (2) business has a security procedure “reasonably designed to block the use of sensitive personally identifiable information” AND(3) business has a policy to provide notice after a breach has resulted in</p>	<p>required if more than 1,000 residents affected (<i>§421(b)</i>).</p>	<p>NONE</p>	<p>Civil penalties up to \$5,000 per violation per day and up to \$55,000 per day, and up to double fines for intentional or willful violations. U.S. Attorney General also has authority to obtain injunction relief or obtain damages/ State attorneys general can get equitable relief and damages upon notifying the U.S. Attorney General. U.S.</p>	<p>1. If breach affects 10,000 residents, impacts a database associated with over 1 million, or impacts a database used by the Federal Government or involving federal employees, firm must notify the Secret Service. Secret Service then must notify the FBI if breach is terrorism-related, the U.S. Postal Inspection Service if mail fraud is involved. The firm must also notify the attorney general of each State affected by the breach. (<i>§421(a)(1)</i>) 2. Company can be exempt from notifying customers and consumer protection agencies if a “<u>reasonable risk assessment</u>” conducted in consultation with Federal law enforcement and the attorney general of each State affected by the security breach concludes that there is a de minimis risk of harm” (<i>§424(a)</i>) 3. <i>§423</i> lays out requirements for <u>content of notifications</u>- including available victim protection assistance, guidance on how to place a fraud alert, identity theft victims’ rights.</p>

					required, must notify them within 14 days. (§422(b))	residents, it must consult with the Secret Service. (421(a)(3))	fraud or unauthorized transactions. (§424(b)(1)).			AG has right to stay state actions. (§426)	4. Business that must notify customers, must also pay for monthly access credit reports and credit-monitoring for 1 year (§425).
--	--	--	--	--	--	---	---	--	--	--	--

	Entities Covered	Relation to State Laws/other Federal Laws	Definition of Security Breach	Definition of Personal Information	Timing of Notification	Method of Notice	Safe Harbor for Company's Notification System	Notify Consumer Reporting Agencies	Duty of Non-Owner Who Maintain the Data	Penalties and Enforcement	Other Provisions
<u>Proposed S.115</u>	“Any agency, or person engaged in interstate commerce, that owns or licenses electronic data containing personal information “ (§3(a)(1))	preempts any inconsistent provisions of state law (§5)	similar to California: Compromise of data security, confidentiality, or integrity “that results in, or there is a reasonable basis to conclude has resulted in” unauthorized disclosure (§2(2))	Same as California (§3(a)(1))	Same as California- “without unreasonable delay” (§3(a)(3))	By writing or e-mail, if individual has agreed to be contacted by email (§3(a)(5))- Substitute Notice- Same as California except “major media” (§2(5))	allowed but company must: use reasonable security program, provide notice, and be subject to compliance under this act or GLBA. (§3(a)(7))	not required	Same as California (§3(a)(3))	monetary penalties up to 25K per day (but not more than 5K per violation) and equitable relief available §3(b); FTC has enforcement power §3(c); (3) State AGs can enforce as well (§4)→ complicated	N/A
<u>Proposed S.751-</u> follow up to S.115	Same as s.115 (§3(a)(1))	preempts any inconsistent provisions of state law (§5)	Same as s.115- (§2(2))	goes beyond S.115 to cover <u>both encrypted and non-electronic data-</u> (§3(a)(1))	Same as §115 except adds special exception for national security needs (§3(a)(5))	Same as §115 (§3(a)(5)) <i>except:</i> <u>Substitute Notice:</u> \$500K or 500K people (§3(a)(6)); only by internet site AND notify media in areas where affected customers reside	<u>REMOVED</u>	required if more than 1,000 residents affected (§3(a)(8))	Same as s.115 (§3(a)(3))	Same as s.115 except monetary fines can reach 50K per day (§3(d))	<u>content of notification:</u> description of information; toll-free # that individual can contact for information; “toll-free contact telephone numbers and addresses for the major credit reporting agencies” (§3(a)(7))

	Entities Covered	Relation to State Laws/other Federal Laws	Definition of Security Breach	Information Covered	Timing of Notification	Method of Notice	Safe Harbor for Company's Notification System	Notify Consumer Reporting Agencies	Duty of Non-Owner Who Maintains the Data	Penalties and Enforcement	Other Provisions
<u>Proposed S.768</u>	“Covered person” (§8(a)) which means “a commercial entity” (§2(1))	State laws that give greater protection to customer data are not pre-empted	Same as S.115	“ <u>unencrypted sensitive personal information</u> ” broader than California- includes medical information, payment history; but no exception for publicly available information	Same as California but includes special exemption for finding by FTC Office of Identity Theft, created by this legislation (§8(b)(3)(B))	Same as California- §8(b)(1) except <u>NO substitute notice provision</u>	NONE	none, but if over 1,000 people affected, must notify Office of Identity Theft (§8(a)(2))	not mentioned	can have monetary penalties of no more than \$1,000 per violation (§8(c)), FTC or state AG can bring enforcement action.	after breach, consumers can ask for expunging of their sensitive personal information from database (§8(d))
<u>Proposed H.R. 1069</u>	Federal agencies and any person or business that “owns, licenses, or collects data” but is not covered by GLBA (§3(a)(1))	financial institutions covered by Gramm-Leach-Bliley have own regulations (§3(a)(1))	Same as S.115 (similar to California) (§2(2))	Same as California (§2(4))	Same as California (§3(a)(3))	Same as California- (§3(a)(5))	Same as California, although no compliance with timing requirement- but does require security program to protect from unauthorized access. (§3(a)(6))	report ALL breaches to consumer reporting agencies (§3(a)(1) (B)) and to information clearinghouse (§3(a)(8) (B))	Same as California (§3(a)(2))	daily penalties up to 25K per day and equitable relief ; authorizes FTC enforcement (§3(b)); authorizes state attorneys general enforcement (§6)	<u>amends and creates new set of guidelines for financial institutions covered by Gramm-Leach-Bliley- §526 provides rules for financial institutions- also requires specific content in notifications (§526(f))</u>

Banking Agency Security Breach Notification Rules

	Entities Covered	Relation to State Laws	Definition of Security Breach	Definition of Personal Information	Timing of Notification	Method of Notice	Safe Harbor for Company's Notification System	Notify Consumer Reporting Agencies	Duty of Non-Owner Who Maintains the Data	Penalties and Enforcement	Other Provisions
<p>Interagency Security Guidelines for Financial Institutions under Gramm-Leach-Bliley</p>	<p>Financial institutions- Same scope as §505(a) of GLBA- banks, securities firms, insurance companies etc.</p>	<p>not mentioned</p>	<p>not limited to computerized data</p>	<p>“<u>sensitive consumer information</u>”- broad definition, encompassing more than the California statute. No exemption for public available information. <u>Only applies to customer information obtained primarily for personal, family or household purposes, and who has a continuing relationship with the institution</u></p>	<p>only if “reasonable investigation” determines that “misuse of its information about a customer has occurred or is reasonably possible”- must notify affected customers “as soon as possible.” On the other hand, must <u>always</u> notify primary federal regulator</p>	<p>“any manner designed to ensure that a customer can reasonably be expected to receive it”- Notification must include “clear and conspicuous manner”- describe what information was taken and what steps to take</p>	<p>NONE</p>	<p>not required</p>	<p>financial institution bears all responsibility but there should be contract between service provider and financial institution for prompt notification to financial institution</p>	<p>not mentioned</p>	<p><u>content of notification:</u> specific provisions in customer notices- “clear and conspicuous manner”- describe what information was taken, steps to take etc.</p>