KELLER AND HECKMAN LLP
Serving Business through Law and Science®

1001 G Street, N.W.
Suite 500 West
Washington, D.C. 20001 *tel.* 202.434.4100
fax 202.434.4646

STATE DATA BREACH NOTIFICATION LAWS: OVERVIEW OF REQUIREMENTS FOR RESPONDING TO A DATA BREACH UPDATED

JUNE 2021

With the ever-changing complexity of state data breach notification laws, companies facing a data breach need resources that will help them understand the issues. This summary provides an overview of the similarities and differences in data breach laws adopted in the 50 United States and District of Columbia.[1] All states require that affected residents be notified of a security breach (as that term is defined in each law), and many also require that state agencies and the three major national credit reporting agencies be notified in certain circumstances. Many state agencies require or permit companies to submit notices online, and some agencies publicly post copies of the notices they receive. As a practical matter, most companies that experience a breach that affects their customers, employees, or other individuals with whom they have a relationship will be required to comply with all or several state laws depending on where the individuals reside, and international and sector-specific data breach notification laws may also apply. In addition, many state laws impose data security requirements, which should also be consulted.

The laws continue to evolve and change, so it is important to consult experienced counsel and check relevant laws for any updates whenever you experience a data breach.

THIS SUMMARY IS INTENDED TO PROVIDE GENERAL INFORMATION ABOUT APPLICABLE LAWS AND DOES NOT CONSTITUTE LEGAL ADVICE REGARDING SPECIFIC FACTS OR CIRCUMSTANCES.

For more information on privacy and data security matters, please contact us:
Sheila Millar (+1 202.434.4143, millar@khlaw.com)
Tracy Marshall (+1 202.434.4234, marshall@khlaw.com)

[1] This summary only covers data breach notification laws for the 50 United States and District of Columbia. It does not cover laws adopted in any U.S. territories, sector-specific laws (such as the Gramm-Leach-Bliley Act, HIPAA Breach Notification Rule, and New York State Department of Financial Services Cybersecurity Regulation), or international data breach notification laws.

Definitions

CRA = Consumer Reporting Agency (Experian, Equifax, TransUnion)
AG = State Attorney General
FTC = Federal Trade Commission

1. What Type of Personal Information (PI) Triggers a Breach Notification Obligation to Individuals?

Type of Personal Information	**States**
First name/initial and last name *plus* any of: - Social Security number (SSN) - Driver's license number, state ID # - Account number, credit or debit card number, in combination w/ any PIN, security code, access code, or password that would permit access to an individual's financial account	All; some states define these types as "personal information" even absent an individual's name if the information is sufficient to commit identity theft
Name or any other personal identifier *plus* SSN, driver's license #, ID card #, credit or debit card #, or any other # or code that allows access to/use of individual's account	DC
Financial account number or credit/debit card number, even without security code, access code, PIN or password, if associated with first name/initial and last name	MA
Passwords, personal identification numbers, or other access codes for financial accounts when used with a first name/initial and last name	AK, NY, VT
Unique electronic identifier or routing code, plus security code, access code, or password that would permit access to a financial account when used with a first name/initial and last name	IA, MO, NE
Unique biometric data, such as a fingerprint, retina or iris image, or other unique representation of biometric data when used with a first name/initial and last name	AR, CA, CO, DE, DC, IL, IA, MD, NE, NM, NY, NC, OR, VT, WI, WY
An individual's DNA profile when used with a first name/initial and last name	DE, WI

An Individual or Employer Taxpayer Identification Number when used with a first name/initial and last name	DE, MD, MT, NC, WY

Type of Personal Information	**States**
User name or email address plus a password or security question and answer that would permit access to an online account	AL, CA, CO, FL, IL, NE, NJ, NV, NY, SD, VT, WA, WY DC, MD (only applies to access to an email account) OR (user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification) RI (email address plus a security code, access code, or password that would permit access to an individual's personal, medical, insurance or financial account)
ID number assigned by employer when used with a first name/initial and last name	ND SD (if in combination with required security code, access code, password, or biometric data)
Digital or electronic signature when used with a first name/initial and last name	NC, ND
Date of birth when used with a first name/initial and last name	ND, WA
Mother's maiden name when used with a first name/initial and last name	NC, ND
Genetic information plus first and last name	DC, VT

Medical information	TX AL, AR, CA, CO, DE, DC, FL, IL, MD, MO, MT, ND, OR, RI, SD, WA, WY (if used with first name/initial and last name) VA (if used with first name/initial and last name and maintained by a state government entity)
Health records or records of a wellness program or similar program of health promotion or disease prevention; a health care professional's medical diagnosis or treatment of the consumer; or a health insurance policy number	VT

Type of Personal Information	**States**
Health insurance information	AL, CA, DE, DC, FL, IL, MD, MO, ND, RI, WA, WY (if used with first name/initial and last name) TX VA (if used with the first name/initial and last name and maintained by a state government entity)
Health Information (as defined under HIPAA) plus name	SD
Medical identification number or health insurance identification number	CO, NV (if used with first name/initial and last name)
Health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify an individual	OR (if used with first name/initial and last name)
SSN (alone)	GA, IN, ME
IRS issued identity protection personal identification number	MT
Any other numbers or information that can be used to access a person's financial resources when used with a first name/initial and last name	NC, SC

Dissociated data that, if linked, would constitute PI, if the means to link the dissociated data is accessed	NJ
Individual taxpayer identification number, passport number, military identification card number, or other government issued identification number	OR, SC AL, CO, DE, MD, NM, SD, VT, WA, WY (if used with first name/ initial and last name)

2. What Form of Data Triggers a Breach Notification Obligation to Individuals?[2]

Form of Data	State(s)
Unencrypted	All states
Computerized	All states
Any Form (electronic, paper, etc.)	AK, HI, IA (if transferred to other medium from computerized form), MA, NC, SC, WA, WI

[2] Obligation to notify applies generally to businesses that own or license personal information, except GA law applies to data brokers and persons who maintain information on behalf of a data broker. Some states have imposed obligations on vendors.

3. When Must Notice to Individuals be Given?

Timing to Notify Residents	States
Within 30 days of breach	CO, ME, WA FL (plus additional 15 days for good cause shown)
No later than 45 days after discovery of breach	AL, MD, NM, OH, RI, TN, WI, VT
No later than 60 days after discovery of breach	DE, SD, LA, TX
Within 90 days after discovery of breach (unless delayed	CT

for a law enforcement investigation)	
Most expedient time possible and without unreasonable delay	AK, AZ, AR, CA, CO, DE, DC, GA, HI, ID, IL, IN, IA, KS, KY, LA, ME, MA, MI, MN, MS, MO, MT, NE, NM, NV, NH, NJ, NY, NC, ND, OR, PA, RI, SC, TX, UT, VA, WA, WY **CA guidance document recommends notifying within 10 business days**
As soon as reasonably practicable after discovery of breach	MD, OK, WV

4. What Form of Notice is Permitted?

Form of Notification	**States**
Written Notice	All states
Electronic Notice (consistent w/ 15 U.S.C. § 7001)	All states Some states permit notification by any method employed to communicate with consumers
Telephone	AZ, CO, CT, DE, GA, ID, IN, MD, MS, MT, NE, OH, OK, SC, TN, UT, VA, WV HI, MO, NC, OR, VT (if contact is made directly with affected persons) MI (if notice is not given by use of a recorded message and the recipient has expressly consented to receive notice by telephone; or if recipient has not expressly consented to receive notice by telephone, and notice by telephone does not result in a live conversation within 3 business days after initial attempt to provide telephone notice, then written or electronic notice is also provided) NH, NY (if a log of each notification is kept) PA (if consumers can be reasonably expected to receive it and notice is given in a clear and conspicuous manner, describes the incident in general terms, and verifies PI (but does not require consumers to provide PI, and consumers are provided with a telephone number or website for more information)
Fax	IN
Newspaper of general circulation	UT

Substitute notice (consisting of email; conspicuous posting on website; and notice to major statewide media) where cost > $250K, > 500,000 affected, or insufficient contact information	AR, CA, CT, FL, IL, IN, KY, LA, MA, MI, MN, MT, NV, NJ, NY, NC, ND, OH, SC, SD, TN, TX, WA

Form of Notification	**States**
Substitute notice (consisting of email; conspicuous posting on website and notice to major statewide media) with other cost/affected individual thresholds	- AK (cost > $150K, >300,000 affected) - AL (cost > $500K, >100,000 affected) - AZ, DC, GA, OK, VA, WV (cost > $50K, >100,000 affected) - CO (cost > $250K, >250,000 affected) - DE and NE (cost >$75K, >100,000 affected) - HI (cost >$100K, >200,000 affected) - ID and RI (cost >$25K, >50,000 affected) - IA and OR (cost >$250K, >350,000 affected) - KS (cost >$100K, >5,000 affected) - ME and NH (cost >$5K, >1,000 affected) - MD and PA (cost >$100K, >175,000 affected) - MS (cost > $5K, > 5,000 affected) - MO (cost >$100K, >150,000 affected) - NM (cost >$100K, >50,000 affected) - RI (cost >$50K, >50,000 affected) - VA (cost >$50K, >100,000 affected) - VT (cost > $5K, > 5,000 affected) - WY (cost > $10K for WY business or $250K for others, > 10,000 affected for WY businesses; 500,000 for others)

If breach involves a user name or email address plus a password or security Q&A that would permit access to an online account, the business may provide notice in electronic or other form that directs the consumer to promptly change password and security Q&A or take other appropriate steps to protect the account with the business and all other online accounts for which the customer uses the same user name/email address and password or security Q&A	CA, DC, IL, MD NJ, VT (except if breach involves login credentials for an email account, the business shall not provide notice via email, and shall provide notice through another permitted method or by clear and conspicuous notice delivered online when the consumer is connected to the account from an IP address from which the business knows the consumer customarily accesses the account) CO, WA (except if breach involves login credentials for an email account, the business shall not provide notice via email, and shall provide notice through another permitted method)

5. What Must Be Included in Breach Notices to Individuals Under Statute?[3]

States	Content Required
Alabama	1. Date, estimated date, or estimated date range of the breach. 2. Description of the sensitive personally identifying information acquired. 3. Description of actions taken to restore the security and confidentiality of the PI affected. 4. Description of steps an affected individual can take to protect him/herself from identity theft. 5. Information that the individual can use to contact the covered entity to inquire about the breach.

California	Notification *must* include: 1. The name and contact information of the business. 2. A list of the types of PI believed to be breached. 3. The date or estimated date of the breach, if known. 4. Whether notification was delayed as a result of a law enforcement investigation. 5. A general description of the incident. 6. 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. Notification *may* include the following: 1. Information about what the business has done to protect individuals whose information has been breached. 2. Advice on steps that the person may take to protect themselves from the breach. Notification must be at least 10-point type, must be titled *Notice of Data Breach*, and must present the information described above under the following headings: *What Happened*; *What Information Was Involved*; *What We Are Doing*; *What You Can Do*; and *For More Information*. Companies that report a breach must provide free identity theft protection for 12 months if breach involves SSNs, driver's license numbers, or California ID card numbers.

[3] Notice to state agencies prior to or simultaneously with notice individuals is required in some states. *See* Section 6.

States	Content Required
Colorado	1. Date, estimated date, or estimated date range of the breach. 2. Description of PI acquired. 3. Contact information for the covered entity. 4. Toll-free numbers, addresses, and URLs for consumer reporting agencies and the Federal Trade Commission. 5. A statement that the individual can obtain information from these sources about fraud alerts and security freezes. If an investigation determines that the information acquired has been misused or is reasonably likely to be misused, the business must also direct consumers to promptly change passwords and security Q&A or take other steps to protect online accounts that use the same username or email address and password or security Q&A.

Connecticut	The statute does not list required content, but the state Attorney General website specifies that any breach notification should include: 1. Name of person reporting, name of business and contact information. 2. A list of the types of PI that were or are reasonably believed to have been the subject of the breach. 3. A general description of the breach, including the date of the breach and the number of Connecticut residents affected. 4. Whether the notification was delayed because of a law enforcement investigation (if applicable). If the breach involves SSNs or driver's license numbers, the covered entity must provide identify protection services to residents for a period of not less than 12 months.
Delaware	Model form available at https://attorneygeneral.delaware.gov/wp-content/uploads/sites/50/2018/04/Model Security-Breach-Notification-Form-to-Consumers.pdf.
District of Columbia	1. To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired, including elements of PI. 2. Contact information for person or entity making the notification, including business address, telephone number, and toll-free telephone number if one is maintained. 3. Toll-free telephone numbers and addresses for the major CRAs, including a statement notifying the resident of the right to obtain a security freeze free of charge pursuant to 15 U.S.C. § 1681c-1 and information how a resident may request a security freeze. 4. Toll-free telephone numbers, addresses, and website addresses for FTC and DC Attorney General, including a statement that an individual can obtain information from these sources about steps to take to avoid identity theft:

States	Content Required
Hawaii	1. The incident in general terms. 2. Type of PI subject unauthorized access and acquisition. 3. General acts of the business to protect PI from further unauthorized access. 4. Telephone number to call for information and assistance if one exists. 5. Advice to remain vigilant by reviewing account statements and monitoring free credit reports.

Illinois	Notification must include, but need not be limited to: 1. The toll-free numbers and addresses for consumer reporting agencies. 2. The toll-free number, address, and website address for the Federal Trade Commission. 3. A statement that the individual can obtain information from these sources about fraud alerts and security freezes. 4. Instruction to promptly change user name or password and security Q&A and take other appropriate steps to protect all online accounts for which the resident uses the same credentials (if user name/email address plus a password or security Q&A that would permit access to an online account is accessed). Notification **must not** include information concerning the number of residents affected.
Iowa	1. Description of the breach. 2. Approximate date of the breach. 3. Type of PI obtained as a result of the breach. 4. Contact information for CRAs. 5. Advice to report suspected ID theft to local law enforcement or AG.
Maryland	1. To the extent possible, a description of the information acquired, including PI 2. Contact info for the company (address, telephone number, and toll-free telephone number if maintained). 3. Toll-free telephone numbers and addresses for CRAs. 4. Toll-free telephone numbers, addresses, and websites for FTC and MD AG and statement that individual can obtain information from them on steps to avoid identity theft.
Massachusetts	1. Individual's right to obtain a police report. 2. How to request a security freeze and information to be provided when requesting a security freeze. 3. Information on complimentary credit monitoring services. 4. Name of parent organization and subsidiary organizations affected. Notification **must not** describe the nature of the breach or number of residents affected.
Michigan	1. The breach in general terms. 2. Type of PI that is the subject of the unauthorized access or use. 3. What the business has done to protect data from further security breaches. 4. Telephone number where a notice recipient may obtain assistance or additional information. 5. Remind notice recipients of the need to remain vigilant for ID theft and fraud.

States	Content Required

Missouri	1. The incident in general terms. 2. Type of PI obtained. 3. Telephone number for the business. 4. Contact information for CRAs. 5. Advice to remain vigilant by reviewing account statements and monitoring free credit reports.
Montana	If a business discloses a breach and gives notice to the individual that suggests, indicates, or implies that the individual may obtain a copy of the file on the individual from a CRA, the business must coordinate with the CRA as to the timing, content, and distribution of the notice to the individual.
New Hampshire	1. The incident in general terms. 2. Approximate date of breach. 3. Type of PI obtained. 4. Telephone number for the business.
New Mexico	1. Name and contact information for the business. 2. Types of PI reasonably believed to have been subject to the breach. 3. Date/estimated date of the breach or range of dates. 4. General description of the incident. 5. Toll-free numbers and addresses of major CRAs. 6. Advice to review personal account statements and credit reports, as applicable. 7. Advice regarding the individual's rights under the federal Fair Credit Reporting Act.
New York	1. Contact information for the business. 2. A description of the categories of information that were, or are reasonably believed to have been, acquired, including elements of PI.
North Carolina	1. The incident in general terms. 2. Type of PI subject to the unauthorized access and acquisition. 3. General acts of the business to protect PI from further unauthorized access. 4. Telephone number for the business. 5. Advice to remain vigilant by reviewing account statements and monitoring free credit reports. 6. Toll-free numbers and addresses for CRAs. 7. Toll-free numbers, addresses, websites for FTC and NC AG with a statement that the individual can obtain information from these sources about preventing identity theft.

States	Content Required
Oregon	1. Description of the breach. 2. Approximate date of the breach. 3. Type of PI obtained as a result of the breach. 4. Contact information for the business. 5. Contact information for CRAs. 6. Advice to report suspected identity theft to law enforcement, including the FTC.
Rhode Island	1. The incident in general terms, including how the breach occurred and number of affected individuals. 2. Type of PI subject to the security breach. 3. Actual or estimated date of breach or timeframe within which the breach occurred. 4. Date breach was discovered. 5. Description of remediation services being offered, including toll-free numbers and websites for CRAs, remediation service providers, and AG. 6. How to file or obtain a police report. 7. How to request a security freeze and notice that CRAs may charge fees.
Vermont	1. The incident in general terms. 2. Type of PI subject to the security breach. 3. General acts of the business to protect PI from further security breach. 4. Toll-free number to call for further information and assistance. 5. Advice to remain vigilant by reviewing account statements and monitoring free credit reports. 6. Approximate date of the security breach. Notice of a login credential breach should include: A statement that the breach took place and advice to take steps necessary to protect the online account, including changing login credentials for the account and for any other account for which the consumer uses the same credentials.
Virginia	1. The incident in general terms. 2. Type of PI that was subject to the unauthorized access and acquisition. 3. General acts of the entity to protect the PI from further unauthorized access. 4. Telephone number to call for further information and assistance if one exists. 5. Advice to remain vigilant by reviewing account statements and monitoring free credit reports.
Washington	1. Name and contact information for the reporting entity. 2. Types of PI subject to the security breach. 3. Toll-free numbers and addresses for CRAs

States	Content Required
West Virginia	1. To the extent possible, a description of information that was reasonably believed to have been accessed or acquired, including SSNs, driver's licenses or state identification numbers and financial data. 2. Telephone number or website to contact to learn: (A) what types of info the entity maintained about individuals; and (B) whether the entity maintained information about that individual. 3. Toll-free contact numbers and addresses for CRAs and info on how to place a fraud alert or security freeze.
Wisconsin	Indicate that the entity knows of the unauthorized acquisition of PI pertaining to the individual.
Wyoming	1. Types of PI reasonably believed to have been the subject of the breach. 2. General description of the breach. 3. Approximate date of the breach, if reasonably possible to determine at the time of notice. 4. General actions taken to protect the system containing PI from further breaches. 5. Advice to remain vigilant by reviewing account statements and monitoring credit reports. 6. Whether notification was delayed as a result of law enforcement investigation. 7. Toll-free number to contact the person collecting the data or his agent and from which the individual can obtain toll-free numbers and addresses for CRAs.

6. What States Require Notification to State Agencies?

State	State Agency(ies) Requiring Notification[4]	Threshold, Timing, and Content to be Included in Notice

Alabama	Attorney General	Threshold: If notice given to >1,000 residents. Timing: Within 45 days after discovery of the breach. Content: • Events surrounding the breach. • Approximate number of residents affected. • Any services being offered to individuals without charge and instructions on how to use the services. • Name, address, telephone number, and email address of the employee or agent from whom additional information may be obtained.
Arkansas	Attorney General	Threshold: If notice given to >1,000 residents. Timing: At the same time notice is given to residents or within 45 days after determining there is a reasonable likelihood of harm, whichever occurs first. Content: None specified.
California	Attorney General	Threshold: If notice given to >500 residents. Timing: None specified. Content: • Must submit a sample notice to residents, excluding any PI. • Must provide 12 months of free credit monitoring if SSN breached.

[4] Most state agencies specify how notice should be given (e.g., via U.S. mail, e-mail, or online form) and provide contact information on their websites.

State	State Agency(ies) Requiring Notification[4]	Threshold, Timing, and Content to be Included in Notice

Colorado	Attorney General	Threshold: If notice given to >500 residents, unless investigation determines that misuse of the information has not occurred and is not likely to occur. Timing: Within 30 days after discovery of the breach. Content: • Name of organization and primary contact. • Data security breach occurred. • Date of notice to residents. • Number of residents impacted. • Copy of notice to residents.
Connecticut	Attorney General	Threshold: None specified. Timing: Within 90 days after discovery of breach. Content: • Name of person reporting, name of business and contact information. • Types of PI reasonably believed to have been the subject of the breach. • General description of the breach, including the date and number of residents affected. • Whether the notification was delayed because of law enforcement investigation (if applicable). • Must provide 24 months of free credit monitoring if SSN breached.
Delaware	Attorney General	Threshold: If notice given to >500 residents. Timing: No later than when notice is provided to residents. Content: • Notice via online form. • Must provide 12 months of free credit monitoring if SSN breached.

State	State Agency(ies) Requiring Notification[4]	Threshold, Timing, and Content to be Included in Notice

District of Columbia	Attorney General	Threshold: If notice given to >50 residents. Timing: No later than when notice is provided to residents. Content: • Name and contact information of person or entity reporting the breach. • Name and contact information of person or entity that experienced the breach. • Nature of the breach. • Types of PI compromised. • Number of DC residents affected. • Cause of the breach, including the relationship between the person or entity that experienced the breach and the person responsible for the breach, if known. • Remedial action taken to include steps taken to assist affected residents. • Date and time frame of the breach, if known. • Address and location of corporate headquarters, if outside of the District. • Any knowledge of foreign country involvement. • Sample of the notice to residents. Other: Notice shall not be delayed on the grounds that the number of affected residents has not been ascertained.

State	State Agency(ies) Requiring Notification[4]	Threshold, Timing, and Content to be Included in Notice

Florida	Attorney General	Threshold: If notice given to 500 or more residents. Timing: As expeditiously as possible, but no later than 30 days after determination of the breach or reason to believe a breach occurred. May receive an additional 15 days for good cause provided to the Dept. in writing. Content: • Events surrounding the breach. • Number of residents affected. • Any services being offered without charge. • Name, address, telephone number, e-mail address of employee or agent for more information. • Include form of notice to residents. To be provided upon request: • Police/ incident/ computer forensics report. • Copy of the policies in place regarding breaches. • Steps taken to rectify the breach. Other: If business determines, after investigation and consultation with law enforcement, that the breach has not and will not likely result in ID theft or other financial harm, notification to individuals is not required, but must provide the Dept. with written determination within 30 days.
Hawaii	Office of Consumer Protection	Threshold: If notice is given to >1,000 residents. Timing: Without unreasonable delay. Content: None specified.

State	State Agency(ies) Requiring Notification[4]	Threshold, Timing, and Content to be Included in Notice

Illinois	Attorney General	Threshold: If notice is given to 500 residents. Timing: Without unreasonable delay but no later than when individuals are notified. Content: • Description of the breach. • Number of Illinois residents affected. • Steps taken or planned relating to the incident. • If date of the breach is unknown at time of notice, must notify AG of the date as soon as possible. Other: Covered entities and business associates subject to HIPAA and HITECH Act must notify Secretary of Health and Human Services of a breach must notify the AG within 5 business days of notifying the Secretary.
Indiana	Attorney General	Threshold: None specified. Timing: Without unreasonable delay. Content: None specified.
Iowa	Attorney General	Threshold: If > 500 residents affected. Timing: Within 5 business days of notifying consumers. Content: None specified.
Louisiana	Attorney General	Threshold: None specified. Timing: Within 10 days of notice to residents. Content: Names of all individuals affected. Other: Document decision whether to report.
Maine	Department of Professional and Financial Regulation (if regulated by the Department) Attorney General (if not regulated by the Department)	Threshold: None specified. Timing: None specified. Content: • Date of the breach. • Estimated number of persons affected. • Date of notice to residents.

State	State Agency(ies) Requiring Notification[4]	Threshold, Timing, and Content to be Included in Notice
Maryland	Attorney General	Threshold: None specified. Timing: ***Before*** notifying affected residents. Content: • Brief description of the breach. • Number of residents being notified. • Type of information compromised. • Steps taken to restore the integrity of the system. • Attach a copy of notice to residents.
Massachusetts	Attorney General Director of Consumer Affairs and Business Regulation	Threshold: None specified. Timing: As soon as practicable, without unreasonable delay. Content • Detailed description of the incident. • Types of PI compromised. • Number of residents affected. • Steps taken relating to the incident. • Steps to be taken subsequent to notification. • Whether law enforcement is investigating. • Name and address of person that experienced the breach, and type of person. • Person responsible for the breach, if known. • Name and contact information for the person the Attorney General may contact. • Whether person maintains a written information security program (WISP). • Any steps taken or planned as a result of the incident, including updating the WISP. • Provide 18 months of free credit monitoring if SSN breached (CRAs must provide 42 months).

State	State Agency(ies) Requiring Notification[4]	Threshold, Timing, and Content to be Included in Notice
Missouri	Attorney General	Threshold: If notice is given to > 1,000 residents. Timing: Without unreasonable delay. Content: Timing, distribution, and content of notice to residents.
Montana	Attorney General	Threshold: None specified. Timing: Simultaneously with notice to residents. Content: • Date and method of distribution of notice to residents, excluding any PI. • Attach copy of the notice to residents and identify the number of residents who received it.
New Hampshire	Attorney General Entities subject to jurisdiction of the bank commissioner, director of securities regulation, insurance commissioner, public utilities commission, financial institutions and insurance regulators of other states, or federal banking or securities regulators who possess the authority to regulate unfair or deceptive trade practices shall notify the regulator with primary regulatory authority.	Threshold: None specified. Timing: None specified. Content: • Anticipated date of notice to residents. • Approximate number of residents who will be notified.
New Mexico	Attorney General	Threshold: If notice given to > 1,000 residents. Timing: Within 45 calendar days. Content: • Number of residents notified. • Copy of notice to residents.
New Jersey	Department of Law and Public Safety, Division of State Police	Threshold: None specified. Timing: ***Before*** notifying affected residents; quickly and without unreasonable delay. Content: None specified.

New York	Attorney General NYS Division of State Police NYS Department of State Division of Consumer Protection	Threshold: None specified. Timing: None specified. Content: Notice via online form.

State	State Agency(ies) Requiring Notification[4]	Threshold, Timing, and Content to be Included in Notice
North Carolina	Consumer Protection Division of Attorney General's Office	Threshold: None specified. Timing: Without unreasonable delay. Content: Notice via online form.
North Dakota	Attorney General	Threshold: If notice is given to >250 residents. Timing: In the most expedient time possible and without unreasonable delay. Content: None specified.
Oregon	Attorney General	Threshold: If notice is given to >250 residents. Timing: In the most expeditious time possible, without unreasonable delay, consistent with the needs of law enforcement. Content: None specified.
Rhode Island	Attorney General	Threshold: If notice is given to >500 residents. Timing: In the most expedient time possible, but no later than 45 days. Content: • Timing, content and distribution of notices. • Approximate number of affected individuals.

South Carolina	Consumer Protection Division of the Department of Consumer Affairs	Threshold: If notice is given to >1,000 residents Timing: Without unreasonable delay Content: • When the breach occurred. • When notice given to affected residents. • Number of persons affected by the breach. • A copy of the notice to affected residents.
South Dakota	Attorney General	Threshold: If notice is given to >250 residents. Timing: None specified. Content: None specified.
Texas	Attorney General	Threshold: If notice is given to >250 residents. Timing: 60 days. Content: None specified.

State	State Agency(ies) Requiring Notification[4]	Threshold, Timing, and Content to be Included in Notice
Vermont	Attorney General	Threshold: None specified. Timing: Within 14 days of discovering the breach. 14-day preliminary notice need not be submitted if, prior to the date of the breach, owner has sworn in the form provided by the AG that it maintains written policies and procedures to maintain the security of PI and to respond to a breach in a manner consistent with VT law. Content: • Date of the security breach. • Date of discovery of the breach. • Description of the breach. • Number of residents affected. • A copy of the notice sent to affected residents.

Virginia	Attorney General	Threshold: None specified. Timing: Without unreasonable delay. Content: • A cover letter on official company letterhead. • Approximate date of the incident. • How the breach was discovered. • Cause of breach. • Number of residents affected by the breach. • Steps taken to remedy the breach. • Sample notice to residents, to include any possible offers of free credit monitoring. • If notice is provided to more than 1,000 individuals, include the timing, distribution, and content of the notice.
Washington	Attorney General	Threshold: If notice given to >500 residents. Timing: Within 30 days Content: • Copy of notice to residents (eliminating any PI). • Estimated number of residents affected.

7. Other Notification Requirements

State(s)	Notice Requirements
Texas	Requires disclosure of a breach to all individuals (regardless of the state of residency) whose PI is breached. If the individual is a resident of another state that requires breach notification, then the breach notification to that individual may be provided under that state's or Texas law.

8. When is Notification to CRAs Required?

State(s)	Timing of Notification	Notice of Breach
MN	Within 48 hours of discovery.	If notification of breach provided to > 500 MN residents.
AL, AK, CO, DC, FL, HI, IN, KS, KY, MD, ME, MI, MO, NC, NV, NJ, OH, OR, PA, SC, SD, TN, VA, VT, WV, WI	Without unreasonable delay.	If notification of breach provided to > 1,000 state residents.
RI	Without unreasonable delay and no later than 45 days after confirmation of breach.	If notification of breach provided to > 500 RI residents.
NM	Within 45 days.	If notification of breach provided to > 1,000 NM residents.
ME, NH	Without unreasonable delay.	If notification of breach provided to > 1,000 persons.
NY	Without unreasonable delay.	If notification of breach provided to > 5,000 NY residents. Must notify as to timing, content and distribution of notices and approximate number of affected persons.
GA	Without unreasonable delay.	If notification of breach provided to > 10,000 GA residents.
TX	Without unreasonable delay.	If notification of breach provided to > 10,000 persons.