

**STATE DATA BREACH NOTIFICATION LAWS –
OVERVIEW OF REQUIREMENTS FOR RESPONDING TO A DATA BREACH**

UPDATED APRIL 2019

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.

Since our last update, several states amended their laws to impose additional requirements, such as free credit monitoring for individuals whose Social Security number is acquired. Notably, the Massachusetts law was recently amended (effective April 11, 2019) to require that, in addition to offering complimentary credit monitoring, companies that experience a breach that triggers notices to the Office of Consumer Affairs and Business Regulation and the Attorney General's Office must indicate in such notices whether they maintain a written information security program (WISP), as required by the law. The requirement to maintain a WISP is not new, but businesses that experience a breach affecting Massachusetts residents will now be subject to more scrutiny.

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.

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.

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)

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 <i>plus</i> any of: <ul style="list-style-type: none"> - 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 states except D.C. (AK, AL, AZ, AR, CA, CO, CT, DE, FL, GA, HI, ID, IL, IN, IA, KS, KY, LA, ME, MD, MA, MI, MN, MS, MO, MT, NE, NV, NH, NJ, NM, NY, NC, ND, OH, OK, OR, PA, RI, SC, SD, TN, TX, UT, VT, VA, WA, WV, WI, WY) MA: financial account number, or credit or debit card number, even without any required security code, access code, PIN or password, is reportable if associated with first name/initial and last name. SD: account number or credit/debit card number plus required security code, access code, or password that permits access to a financial account is reportable, even in the absence of a name
Name, phone number, <u>or</u> address <i>plus</i> SSN, driver’s license #, ID card #, credit or debit card #, or any other # or code that allows access to/use of individual’s account ²	D.C.

² This definition of “personal information” is similar to the definition of “sensitive customer information” under the Gramm-Leach-Bliley (GLB) Act. That term is defined in the GLB Act as a customer’s name, address, or telephone number, plus a SSN, driver’s license number, account number, credit or debit card

Type of Personal Information	States
Passwords, personal identification numbers, or other access codes for financial accounts when used with a first name/initial and last name	AK, VT
Account #, credit card #, or debit card # (alone) – if information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised	GA, ME
Account passwords, PIN or other access codes (alone) – if information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised	GA, ME, NC
Driver’s license number, or state ID # (alone) – if information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised	ME
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 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	IL, IA, NE, NC, WI, WY
Data from automatic measurements of physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer’s identity in the course of a financial or other transaction	OR
Biometric data (defined as a record generated by automatic measurements of an identified individual’s fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry that is used to uniquely authenticate an individual’s identity when the individual accesses a physical location, device, system or account), when used with a first name/initial and last name	CO, DE, MD, NM
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

number, or a personal identification number or password that would permit access to the customer’s account. It also includes any combination of components of customer information that would allow someone to log onto or access the customer’s account, such as user name and password or password and account number.

KELLER AND HECKMAN LLP

Type of Personal Information	States
User name or e-mail address plus a password or security question and answer that would permit access to an online account	<p>CA, CO, FL, IL, MD, NE, NV, SD, WY</p> <p>AL (user name or e-mail address plus password or security Q&A that would permit access to an online account associated with covered entity)</p> <p>RI (e-mail address plus a security code, access code, or password that would permit access to an individual's personal, medical, insurance or financial account)</p>
ID # assigned by employer when used with a first name/initial and last name	<p>ND</p> <p>SD (if in combination with required security code, access code, password, or biometric data)</p>
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
Mother's maiden name when used with a first name/initial and last name	NC, ND
Medical Information	<p>AL, AR, CA, CO, DE, FL, IL, MD, MO, MT, ND, SD, WY (if used in combination with first name/initial and last name)</p> <p>OR, RI (if used in combination with first name/initial and last name; specifically, information about an individual's medical history, mental or physical condition or medical diagnosis or treatment)</p> <p>TX (specifically the physical or mental health or condition of the individual)</p> <p>VA (If used in combination with the first name/initial and last name <i>and</i> maintained by a state government entity)</p>

Type of Personal Information	States
Health Insurance Information	AL, CA, DE, FL, IL, MD, MO, ND, WY, RI (if used in combination with first name/initial and last name) TX VA (If used in combination with the first name/initial and last name <i>and</i> maintained by a state government entity)
Health Information (as defined under HIPAA) plus name	SD
Medical identification number or a health insurance identification number	CO, NV (if used in combination 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 in combination with first name/initial and last name)
SSN (alone)	GA (if information compromised would alone be sufficient to perform or attempt to perform identity theft against the person whose information was compromised) IN (if SSN not encrypted or redacted) ME (if information compromised would alone be sufficient to permit a person to fraudulently assume or attempt to assume identity of the person whose information was compromised)
Internal Revenue Service–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
Any elements that when not combined with a name would be sufficient to permit a person to commit identity theft	OR
Dissociated data that, if linked, would constitute PI, if the means to link the dissociated data is accessed with access to the dissociated data.	NJ
U.S. Passport number or other United States issued identification number	OR AL, CO, DE, MD, NM (if used in combination with first name/initial and last name)

Type of Personal Information	States
Numbers or information issued by a governmental or regulatory entity that uniquely identify an individual	SC AL, SD (if used in combination with first name/initial and last name)
Tribal identification card	WY
Federal or state government issued identification card	WY
Military identification number	AL, CO (if used in combination with first name/initial and last name)
Student identification number	CO (if used in combination with first name/initial and last name)

2. What Form of Data Triggers a Breach Notification Obligation to Individuals?³

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

³ Obligation to notify applies generally to businesses that own or license personal information of resident of the state, except under the GA law, which applies to information brokers or a person or business who maintains such data on behalf of an information broker.

3. When Must Notice to Individuals be Given?

Timing to Notify Residents	States
Within 30 days of breach	CO FL (plus additional 15 days for good cause shown)
No later than 45 days after discovery of breach	AL, MD, NM, OH, RI, TN, WA, WI, VT
No later than 60 days after discovery of breach	DE, SD, LA
Within 90 days after discovery of breach (unless delayed for a law enforcement investigation)	CT
Most expedient time possible and without unreasonable delay	AK, AZ, AR, CA, CO, DE, D.C., 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 <u>NOTE: CA guidance document recommends notifying within 10 business days.</u>
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 a method the entity has employed to communicate with consumers.

Form of Notification	States		
Telephone	<p>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))</p>		
Fax	IN		
Newspaper of general circulation	UT (but notice must be in accordance with Utah Code Section 45-1-101)		
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		
Substitute notice (consisting of email; conspicuous posting on website; AND notice to major statewide media) with other cost/affected individual thresholds	<table border="0"> <tr> <td data-bbox="741 935 1360 1243"> <ul style="list-style-type: none"> - AK (cost > \$150K, >300,000 affected) - AZ, D.C., 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) </td> <td data-bbox="1360 935 1971 1307"> <ul style="list-style-type: none"> - 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) </td> </tr> </table>	<ul style="list-style-type: none"> - AK (cost > \$150K, >300,000 affected) - AZ, D.C., 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) 	<ul style="list-style-type: none"> - 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)
<ul style="list-style-type: none"> - AK (cost > \$150K, >300,000 affected) - AZ, D.C., 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) 	<ul style="list-style-type: none"> - 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) 		

Form of Notification	States
Substitute notice (conspicuous posting on website AND notice to major statewide media; OR alternative form with AG approval) with other cost/affected individual thresholds	AL (cost > \$500K, >100,000 affected)

5. What Must Be Included in Breach Notices to Individuals Under Statute?⁴

States	Content Required
Alabama	<ol style="list-style-type: none"> 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.

⁴ Notice to state agencies prior to or simultaneously with notice individuals is required in some states. *See* Section 6.

States	Content Required
<p>California</p>	<p>Notification <i>must</i> include:</p> <ol style="list-style-type: none"> 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. <p>Notification <i>may</i> include the following:</p> <ol style="list-style-type: none"> 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. <p>Notification must be at least 10-point type, must be titled <i>Notice of Data Breach</i>, and must present the information described above under the following headings: <i>What Happened</i>; <i>What Information Was Involved</i>; <i>What We Are Doing</i>; <i>What You Can Do</i>; and <i>For More Information</i>.</p> <p>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.</p> <p>If breach only involves PI for an online account, businesses can comply by providing notice in electronic or other form that directs individuals to change password and security Q&A, or take other steps to protect the account and other accounts for which the person uses the same user name/ email address and password or security Q&A.</p>
<p>Colorado</p>	<p>Notification <i>must</i> include:</p> <ol style="list-style-type: none"> 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. <p>If an investigation determines that the information acquired during the breach has been misused or is reasonably likely to be misused, then the entity must also direct consumers to promptly change passwords and security Q&As, as applicable, or take other steps appropriate to protect online accounts that use the same username or email address and password or security Q&As.</p>

States	Content Required
Connecticut	<p>The statute does not list required content, but the state Attorney General website specifies that any breach notification should include:</p> <ol style="list-style-type: none"> 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). <p>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.</p>
Delaware	<p>Model form available at https://attorneygeneral.delaware.gov/wp-content/uploads/sites/50/2018/04/Model-Security-Breach-Notification-Form-to-Consumers.pdf.</p>
Hawaii	<ol style="list-style-type: none"> 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	<p>Notification must include, but need not be limited to:</p> <ol style="list-style-type: none"> 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). <p>Notification must not include information concerning the number of residents affected.</p>
Iowa	<ol style="list-style-type: none"> 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.

States	Content Required
Maryland	<ol style="list-style-type: none"> 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. <p>If breach only involves PI for an online account, businesses can comply with notification requirement by providing notice in electronic or other form that directs individuals to change password and security Q&A, or take other steps to protect the account and other accounts for which the person uses the same user name/ email address and password or security Q&A.</p>
Massachusetts	<ol style="list-style-type: none"> 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. <p>Notification must not describe the nature of the breach or number of residents affected. Sample letter available at http://www.mass.gov/ago/docs/consumer/93h-sampleletter-residents.pdf</p>
Michigan	<ol style="list-style-type: none"> 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.
Missouri	<ol style="list-style-type: none"> 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	<p>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, then the business must coordinate with the CRA as to the timing, content, and distribution of the notice to the individual.</p>
New Hampshire	<ol style="list-style-type: none"> 1. The incident in general terms. 2. Approximate date of breach. 3. Type of PI obtained. 4. Telephone number for the business.

States	Content Required
New Mexico	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.
Oregon	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.

States	Content Required
Vermont	<ol style="list-style-type: none"> 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.
Virginia	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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
West Virginia	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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 ⁵	Threshold, Timing, and Specific Content to be Included In Notice
Alabama	Attorney General	<p><u>Threshold:</u> If notice given to >1,000 residents. <u>Timing:</u> Within 45 days after discovery of the breach. <u>Content:</u></p> <ul style="list-style-type: none"> • Synopsis of events surrounding the breach at time notice is provided. • 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.
California	Attorney General	<p><u>Threshold:</u> If notice given to >500 residents. <u>Timing:</u> None specified. <u>Content:</u></p> <ul style="list-style-type: none"> • Must submit a sample notice to residents, excluding any PI. • Must provide 12 months of free credit monitoring if SSN breached.

⁵ 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 ⁶	Threshold, Timing, and Specific Content to be Included In Notice
Colorado	Attorney General	<p><u>Threshold:</u> If notice given to ≥ 500 residents, unless investigation determines that misuse of the information has not occurred and is not likely to occur.</p> <p><u>Timing:</u> Within 30 days after discovery of the breach.</p> <p><u>Content:</u></p> <ul style="list-style-type: none"> • Name of organization and primary contact. • Data security breach occurred. • Date of notice to residents. • Number of residents impacted. <p>Copy of notice to residents.</p>
Connecticut	Attorney General	<p><u>Threshold:</u> None specified.</p> <p><u>Timing:</u> Within 90 days after discovery of breach.</p> <p><u>Content:</u></p> <ul style="list-style-type: none"> • 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	<p><u>Threshold:</u> If notice given to > 500 residents.</p> <p><u>Timing:</u> No later than when notice is provided to residents.</p> <p><u>Content:</u></p> <ul style="list-style-type: none"> • Notice via online form. • Must provide 12 months of free credit monitoring if SSN breached.

⁶ 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 ⁶	Threshold, Timing, and Specific Content to be Included In Notice
Florida	Attorney General	<p><u>Threshold:</u> If notice given to 500 or more residents. <u>Timing:</u> 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. <u>Content:</u></p> <ul style="list-style-type: none"> • Synopsis of the events surrounding the breach. • Number of residents affected. • Any services being offered without charge and instructions. • Name, address, telephone number, e-mail address of employee or agent from whom additional information may be obtained. • Include form of notice to residents. <p>To be provided upon request:</p> <ul style="list-style-type: none"> • Police/ incident/ computer forensics report. • Copy of the policies in place regarding breaches. • Steps taken to rectify the breach. <p><u>Other:</u> 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.</p>
Hawaii	Office of Consumer Protection	<p><u>Threshold:</u> If notice is given to >1,000 residents. <u>Timing:</u> Without unreasonable delay. <u>Content:</u> None specified.</p>
Illinois	Attorney General	<p><u>Threshold:</u> Covered entities and business associates that are subject to HIPAA and HITECH Act and are required to notify Secretary of Health and Human Services of a breach. <u>Timing:</u> Within 5 business days of notifying the Secretary. <u>Content:</u> None specified.</p>

State	State Agency(ies) Requiring Notification ⁶	Threshold, Timing, and Specific Content to be Included In Notice
Indiana	Attorney General	<p><u>Threshold:</u> None specified. <u>Timing:</u> Without unreasonable delay. <u>Content:</u> None specified.</p>
Iowa	Attorney General	<p><u>Threshold:</u> If > 500 residents affected. <u>Timing:</u> Within 5 business days of notifying consumers. <u>Content:</u> None specified.</p>
Louisiana	Attorney General	<p><u>Threshold:</u> None specified. <u>Timing:</u> Within 10 days of notice to residents. <u>Content:</u> Names of all individuals affected. <u>Other:</u> Must document decision whether to report and keep for 5 years.</p>
Maine	Department of Professional and Financial Regulation (if regulated by the Department) Attorney General (if not regulated by the Department)	<p><u>Threshold:</u> None specified. <u>Timing:</u> None specified. <u>Content:</u></p> <ul style="list-style-type: none"> • Date of the breach. • Estimated number of persons affected. • Actual or anticipated date of notice to residents.
Maryland	Attorney General	<p><u>Threshold:</u> None specified. <u>Timing:</u> Before notifying affected residents. <u>Content:</u></p> <ul style="list-style-type: none"> • 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.

State	State Agency(ies) Requiring Notification ⁶	Threshold, Timing, and Specific Content to be Included In Notice
Massachusetts	Attorney General Director of Consumer Affairs and Business Regulation	<p><u>Threshold:</u> None specified.</p> <p><u>Timing:</u> As soon as practicable and without unreasonable delay.</p> <p><u>Content</u></p> <ul style="list-style-type: none"> • 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. • If SSN compromised, must offer free credit monitoring services for 18 months through a third party vendor. • Must provide 18 months of free credit monitoring if SSN breached (CRAs that experience a breach must provide 42 months).
Missouri	Attorney General	<p><u>Threshold:</u> If notice is given to > 1,000 residents.</p> <p><u>Timing:</u> Without unreasonable delay.</p> <p><u>Content:</u> Timing, distribution, and content of notice to residents.</p>

State	State Agency(ies) Requiring Notification ⁶	Threshold, Timing, and Specific Content to be Included In Notice
Montana	Attorney General	<p><u>Threshold</u>: None specified.</p> <p><u>Timing</u>: Simultaneously with notice to residents.</p> <p><u>Content</u>:</p> <ul style="list-style-type: none"> • 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	<p>Attorney General</p> <p>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.</p>	<p><u>Threshold</u>: None specified.</p> <p><u>Timing</u>: None specified.</p> <p><u>Content</u>:</p> <ul style="list-style-type: none"> • Anticipated date of notice to residents. • Approximate number of residents who will be notified.
New Mexico	Attorney General	<p><u>Threshold</u>: If notice given to > 1,000 residents.</p> <p><u>Timing</u>: Within 45 calendar days.</p> <p><u>Content</u>:</p> <ul style="list-style-type: none"> • Number of residents notified. • Copy of notice to residents.
New Jersey	Department of Law and Public Safety, Division of State Police	<p><u>Threshold</u>: None specified.</p> <p><u>Timing</u>: <i>Before</i> notifying affected residents; quickly and without unreasonable delay.</p> <p><u>Content</u>: None specified.</p>
New York	<p>Attorney General</p> <p>NYS Division of State Police</p> <p>NYS Department of State Division of Consumer Protection</p>	<p><u>Threshold</u>: None specified.</p> <p><u>Timing</u>: None specified.</p> <p><u>Content</u>: Notice via online form.</p>
North Carolina	Consumer Protection Division of Attorney General’s Office	<p><u>Threshold</u>: None specified.</p> <p><u>Timing</u>: Without unreasonable delay.</p> <p><u>Content</u>: Notice via online form.</p>

State	State Agency(ies) Requiring Notification ⁶	Threshold, Timing, and Specific Content to be Included In Notice
North Dakota	Attorney General	<p><u>Threshold:</u> If notice is given to >250 residents. <u>Timing:</u> In the most expedient time possible and without unreasonable delay. <u>Content:</u> None specified.</p>
Oregon	Attorney General	<p><u>Threshold:</u> If notice is given to >250 residents. <u>Timing:</u> In the most expeditious time possible, without unreasonable delay, consistent with the needs of law enforcement. <u>Content:</u> None specified.</p>
Rhode Island	Attorney General	<p><u>Threshold:</u> If notice is given to >500 residents. <u>Timing:</u> In the most expedient time possible, but no later than 45 days. <u>Content:</u></p> <ul style="list-style-type: none"> • Timing, content and distribution of notices. • Approximate number of affected individuals.
South Carolina	Consumer Protection Division of the Department of Consumer Affairs	<p><u>Threshold:</u> If notice is given to >1,000 residents <u>Timing:</u> Without unreasonable delay <u>Content:</u></p> <ul style="list-style-type: none"> • 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	<p><u>Threshold:</u> If notice is given to >250 residents. <u>Timing:</u> None specified. <u>Content:</u> None specified.</p>

State	State Agency(ies) Requiring Notification ⁶	Threshold, Timing, and Specific Content to be Included In Notice
Vermont	Attorney General	<p><u>Threshold:</u> None specified.</p> <p><u>Timing:</u> 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.</p> <p><u>Content:</u></p> <ul style="list-style-type: none"> • 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	<p><u>Threshold:</u> None specified.</p> <p><u>Timing:</u> Without unreasonable delay.</p> <p><u>Content:</u></p> <ul style="list-style-type: none"> • 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	<p><u>Threshold:</u> If notice given to >500 residents.</p> <p><u>Timing:</u> By the time notice is provided to residents.</p> <p><u>Content:</u></p> <ul style="list-style-type: none"> • 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, D.C., 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.

EQUIFAX:

E-mail: psol@equifax.com
 Contact Number: 866-510-4211
<http://www.equifax.com/help/data-breach-solutions/>

EXPERIAN:

E-mail: databreachinfo@experian.com
 Contact Number: 866-751-1323
<http://www.experian.com/data-breach/data-breach-security.html>

TRANSUNION:

E-mail: databreach@transunion.com
 Contact Number: 800-971-4307
<https://www.transunion.com/solution/data-breach-services>