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 OCTOBER 2018

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 the District of Columbia. Alabama and South Dakota became the last states to adopt breach notification laws, which took effect on May 1, 2018 and July 1, 2018, respectively. Since our last update, the Colorado law was amended by requiring notice to affected residents and the state's Attorney's General within 30 days of determination of a breach, imposing content requirements for notices to residents, and expanding the definition of "personal information." As a practical matter, most companies that experience a breach will be required to comply with all or several state laws depending on where the data subjects reside, and international data breach notification laws may also apply.

Because privacy is a politically popular topic for legislators, laws continue to evolve and change. It is important to confirm that no changes have been made to relevant laws whenever you experience a data breach. While this summary focuses on data breach notification obligations, many state laws also impose specific data security requirements for companies that handle personal information, which should also be consulted.

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)

Definitions

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

1. What Type of Personal Information 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 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, or address *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[1]	D.C.

[1] This definition of "personal information" and some of the other types of personal information described in this chart that trigger the breach notification requirement 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 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.

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	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 e-mail address plus a password or security question and answer that would permit access to an online account	CA, CO, FL, IL, MD, NE, NV, SD, WY 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) 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)
ID # 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
Mother's maiden name when used with a first name/initial and last name	NC, ND
Medical Information	AL, AR, CA, CO, DE, FL, IL, MD, MO, MT, ND, SD, WY (if used in combination with first name/initial and last name) 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) TX (specifically the physical or mental health or condition of the individual) VA (If used in combination with the first name/initial and last name *and* maintained by a state government entity)

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 *and* 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 personal information, 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?[2]

Form of Data	State(s)
Unencrypted	All states with data breach laws (AL, AK, AZ, AR, CA, CO, CT, D.C., DE, FL, GA, HI, ID, IL, IN, IA, KS, KY, LA, ME, MD, MA, MI, MN, MS, MO, MT, NE, NM, NV, NH, NJ, NY, NC, ND, OH, OK, OR, PA, RI, SC, SD, TN, TX, UT, VT, VA, WA, WV, WI, WY)
Computerized	All states with data breach laws (AL, AK, AZ, AR, CA, CO, CT, D.C., DE, FL, GA, HI, ID, IL, IN, IA, KS, KY, LA, ME, MD, MA, MI, MN, MS, MO, MT, NE, NM, NV, NH, NJ, NY, NC, ND, OH, OK, OR, PA, RI, SC, SD, TN, TX, UT, VT, VA, WA, WV, WI, WY)

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

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

3. When Must Notice to Individuals be Given?

Timing to Notify Residents	States
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 NOTE: CA guidance document recommends notifying within 10 business days.
Within 90 days after discovery of breach (unless delayed for a law enforcement investigation)	CT
No later than 45 days after discovery of breach	AL, FL, MD, NM, OH, RI, TN, WA, WI, VT
As soon as reasonably practicable after discovery of breach	MD, OK, WV
Within 30 days of breach	CO FL (plus additional 15 days for good cause shown)
No later than 60 days after discovery of breach	DE, SD

4. What Form of Notice is Permitted?

Form of Notification	States
Written Notice	All states with data breach laws. (AL, AK, AZ, AR, CA, CO, CT, DE, D.C., FL, GA, HI, ID, IL, IN, IA, KS, KY, LA, ME, MD, MA, MI, MN, MS, MO, MT, NE, NM, NV, NH, NJ, NY, NC, ND, OH, OK, OR, PA, RI, SC, SD, TN, TX, UT, VT, VA, WA, WV, WI, WY)

Form of Notification	States
Electronic Notice (consistent w/ 15 U.S.C. § 7001)	AL, AK, AZ, AR, CA, CO, CT, DE, D.C., FL, GA, HI, ID, IL, IN, IA, KS, KY, LA, ME, MD, MA, MI, MN, MS, MO, MT, NE, NM, NV, NH, NJ, NY, NC, ND, OH, OK, OR, PA, RI, SC, SD, TN, TX, UT, VT, VA, WA, WV, WY Same states that permit written notice, except that WI permits notification "by a method the entity has previously employed to communicate with the subject of the personal information."
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 the 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 such notification is kept by the person or business who notifies affected persons) PA (if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet Website to visit for further information or assistance)
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

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) - 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) - 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)
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?[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 personal information involved in the breach. 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.

[3] AG or other approval prior to or simultaneously with notifying affected individuals is required in some states. *See* Section 6.

States	Content Required
California	Notification *must* include: 1. The name and contact information of the business. 2. A list of the types of personal information 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 the breach involves SSNs, driver's license numbers, or California identification card numbers. For a breach that involves PI for an online account and no other PI, companies can comply with the notification requirement by providing notice in electronic or other form that directs affected person to change his/her password and security question or answer, or take other steps appropriate to protect the account and all other online accounts for which the person uses the same user name or email address and password or security question or answer.

States	Content Required
Colorado	Notification *must* include: 1. Date, estimated date, or estimated date range of the breach. 2. Description of the sensitive personal information 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 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.
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 personal information 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.
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.

States	Content Required
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 shall not include information concerning the number of Illinois residents affected by the breach.
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. In the event of a breach that compromises an email account and no other personal information, the business may provide notice in electronic form that directs the individual to change his/her password and security question and answer, as applicable, and take other appropriate steps to protect the email account and any other accounts for which the individual uses the same username/email and password/security Q&A.
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. Required fees for CRAs. 4. 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
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, then 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.
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 personal information subject to the security breach. 3. Toll-free numbers and addresses for CRAs
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.

States	Content Required
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 & Agency Information	Threshold, Timing, and Specific Content to be Included In Notice
Alabama	Attorney General	Threshold: If notice is given to >1,000 residents. Timing: Within 45 days after discovery of the breach. Specific Content: • A synopsis of the events surrounding the breach at the time that notice is provided. • The approximate number of individuals in the state who were affected by the breach. • Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions on how to use the services. • The name, address, telephone number, and email address of the employee or agent of the covered entity from whom additional information may be obtained about the breach
California	Attorney General Submit electronic form: https://oag.ca.gov/ecrime/databreach/report-a-breach	Threshold: If notice is given to >500 residents at one time. Timing: None specified. Specific Content: Must electronically submit a sample copy of the notification to residents, excluding any PI.
Colorado	Attorney General	Threshold: If notice is given to ≥500 residents, unless the 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. Specific Content: None specified.

State	State Agency(ies) Requiring Notification & Agency Information	Threshold, Timing, and Specific Content to be Included In Notice
Connecticut	Attorney General Notify by E-mail: Office of the Attorney General 55 Elm Street Hartford, CT 06106 ag.breach@ct.gov	Threshold: None specified. Timing: Within 90 days after discovery of breach. Specific Content: • Name of person reporting, name of business and contact information. • List of types of personal information that were or are 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).
Delaware	Attorney General	Threshold: If notice is given to >500 residents. Timing: No later than when notice is provided to the resident. Specific Content: None specified.

State	State Agency(ies) Requiring Notification & Agency Information	Threshold, Timing, and Specific Content to be Included In Notice
Florida	Attorney General Notify by U.S. Mail: Office of Attorney General Department of Legal Affairs The Capitol PL-01 Tallahassee, FL 32399-1050	Threshold: If notice is 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. Specific Content: • Synopsis of the events surrounding the breach. • Number of residents who were or potentially have been affected by the breach. • Any services being offered or scheduled to be offered, without charge, and instructions as to how to use such services. • Name, address, telephone number, e-mail address of employee or agent from whom additional information may be obtained. To be provided upon request: • Police/ incident/ computer forensics report. • Copy of the policies in place regarding breaches. • Steps that have been taken to rectify the breach. In addition, if a business, after an investigation and consultation with relevant law enforcement agencies, determines that the breach has not and will not likely result in ID theft or other financial harm to individuals, notification to individuals is not required, but the business must provide the Dept. with its written determination within 30 days after such determination.

State	State Agency(ies) Requiring Notification & Agency Information	Threshold, Timing, and Specific Content to be Included In Notice
Hawaii	Office of Consumer Protection Notify by U.S. Mail: Office of Consumer Protection Department of Commerce and Consumer Affairs 235 South Beretania Street, Suite 801 Honolulu, Hawaii 96813-2419	Threshold: If notice is given to >1,000 residents at one time Timing: Without unreasonable delay. Specific Content: None specified.
Illinois	Attorney General	Threshold: 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. Timing: Within 5 business days of notifying the Secretary. Specific Content: None specified.
Indiana	Attorney General Notify by U.S. Mail or Fax: Consumer Protection Division Office of the Indiana Attorney General ATTN: Security Breach Notification 302 W. Washington St., 5th Floor Indianapolis, IN 46204 317-232-6201	Threshold: None specified. Timing: Without unreasonable delay. Specific Content: Form provided at http://www.in.gov/attorneygeneral/files/841375_1(1).PDF.
Iowa	Attorney General Notify by U.S. Mail: Office of the Attorney General Consumer Protection Division 1305 E. Walnut Street Des Moines, IA 50319	Threshold: If > 500 residents affected. Timing: Within 5 business days of notifying consumers. Specific Content: None specified.

State	State Agency(ies) Requiring Notification & Agency Information	Threshold, Timing, and Specific Content to be Included In Notice
Louisiana	Attorney General Notify by U.S. Mail: Consumer Protection Section Office of the Attorney General 1885 North Third St. Baton Rouge, LA 70802	Threshold: None specified. Timing: Within 10 days of notice to LA residents. Specific Content: Notice must be written and include names of all individuals affected by the breach.
Maine	Department of Professional and Financial Regulation (if regulated by the Department) Notify by U.S. Mail: Department of Professional & Financial Regulation 35 State House Station Augusta, Maine 04333 Attorney General (if not regulated by the Department) Notify by U.S. Mail: Maine Attorney General Attn: Consumer Protection Division 6 State House Station Augusta, Maine 04333	Threshold: None specified. Timing: None specified. Specific Content: • Date of the breach. • Estimated number of persons affected by the breach. • Actual or anticipated date that the residents will be notified. • Can use form: http://www.maine.gov/tools/whatsnew/attach.php?id=618758&an=1.
Maryland	Attorney General Notify by U.S. Mail: Office of the Attorney General Attn: Security Breach Notification 200 St. Paul Place Baltimore, MD 21202 Notify by Fax: (410) 576-6566 Attn: Security Breach Notification Notify by E-mail: Idtheft@oag.state.md.us	Threshold: None specified. Timing: ***Before*** notifying affected individuals. Specific Content: • Brief description of the breach. • Number of MD residents being notified. • Type of information compromised. • Steps taken to restore the integrity of the system. • Attach a copy of the notice to consumers.

State	State Agency(ies) Requiring Notification & Agency Information	Threshold, Timing, and Specific Content to be Included In Notice
Massachusetts	Attorney General and Director of Consumer Affairs and Business Regulation Notify by U.S. Mail: Massachusetts Office of the Attorney General Public Information and Assistance Center One Ashburton Pl. Boston, MA 02108-1518 E-mail: ago@state.ma.us Office of Consumer Affairs and Business Regulation (OCABR) 10 Park Plaza, Suite 5170 Boston, MA 02116	Threshold: None specified. Timing: As soon as practicable and without unreasonable delay. Specific Content • Detailed description of the incident. • Number of MA residents affected. • Steps taken relating to the incident. • Steps to be taken subsequent to notification. • Whether law enforcement is investigating. • Name and contact information for the person whom the Office of the Attorney General may contact. • OCABR requires this form: http://www.mass.gov/ocabr/data-privacy-and-security/data/security-breach-notificationssubmission.html. Sample letter available on website
Missouri	Attorney General Notify by U.S. Mail: Attorney General's Office Consumer Protection Unit 207 W. High St. P.O. Box 899 Jefferson City, MO 65102 attorney.general@ago.mo.gov	Threshold: If notice is given to > 1,000 residents at once Timing: Without unreasonable delay. Specific Content: Timing, distribution, and content of the notice to individuals.

State	State Agency(ies) Requiring Notification & Agency Information	Threshold, Timing, and Specific Content to be Included In Notice
Montana	Attorney General Notify by U.S. Mail: Office of Consumer Protection P.O. Box 200151 Helena, MT 59620-0151	Threshold: None specified. Timing: Simultaneously with notice to individuals. Specific Content: • Date and method of distribution of the notice to individuals, excluding any information that personally identifies an individual. • Attach a copy of the notice to individuals and identify the number of residents who received it.
New Hampshire	Attorney General Notify by U.S. Mail: New Hampshire Department of Justice Office of the Attorney General 33 Capitol Street Concord, NH 03301 Other State Regulatory Agencies: Entities subject to the jurisdiction of the bank commissioner, the director of securities regulation, the insurance commissioner, the public utilities commission, the 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. Specific Content: • Anticipated date of the notice to the individuals • Approximate number of residents who will be notified.
New Mexico	Attorney General	Threshold: If notice is given to > 1,000 residents at once. Timing: Within 45 calendar days. Specific Content: • Number of residents who were notified • Copy of notification to residents

State	State Agency(ies) Requiring Notification & Agency Information	Threshold, Timing, and Specific Content to be Included In Notice
New Jersey	Department of Law and Public Safety, Division of State Police A breach of security can be reported to the New Jersey State Police 24 hours a day at: 609-963-6900	Threshold: None specified. Timing: ***Before*** notifying affected individuals; quickly and without unreasonable delay. Specific Content: None specified.
New York	Must notify the following three (3) agencies by fax or email: Attorney General's Office: Security Breach Notification Consumer Frauds & Protection Bureau 120 Broadway - 3rd Floor New York, NY 10271 Fax: 212-416-6003 E-mail: breach.security@ag.ny.gov New York State Division of State Police: Security Breach Notification New York State Intelligence Center 630 Columbia Street Ext Latham, NY 12110 fax: 518-786-9398 E-mail: risk@nysic.ny.gov New York State Department of State Division of Consumer Protection: Attn: Director of the Division of Consumer Protection Security Breach Notification 99 Washington Avenue, Suite 650 Albany, NY 12231 Fax: 518-473-9055 E-mail: security_breach_notification@dos.ny.gov	Threshold: None specified. Timing: None specified. Specific Content: Notice made using state form: https://its.ny.gov/sites/default/files/documents/Business-Data-Breach-Form.pdf

State	State Agency(ies) Requiring Notification & Agency Information	Threshold, Timing, and Specific Content to be Included In Notice
North Carolina	Consumer Protection Division of the Attorney General's Office Notify by U.S. Mail: Consumer Protection Division NC Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001	Threshold: None specified. Timing: Without unreasonable delay. Specific Content: Notice should be made using North Carolina Security Breach Reporting Form: http://www.ncdoj.gov/getdoc/81eda50e-8feb-4764-adca-b5c47f211612/Report-a-Security-Breach.aspx
North Dakota	Attorney General Notify by U.S. Mail: Office of the Attorney General Consumer Protection and Antitrust Division Gateway Professional Center 1050 E. Interstate Ave., Suite 200 Bismarck, ND 58503-5574	Threshold: If notice is given to >250 residents at once. Timing: In the most expedient time possible and without unreasonable delay. Specific Content: None specified.
Oregon	Attorney General Notify by U.S. Mail or Electronically: Office of the Attorney General Financial Fraud/Consumer Protection Section Civil Enforcement Division Oregon Department of Justice 1162 Court Street NE Salem, OR 97301-4096 help@oregonconsumer.gov	Threshold: If notice is given to >250 residents at once. Timing: In the most expeditious time possible, without unreasonable delay, consistent with the needs of law enforcement. Specific Content: None specified.

State	State Agency(ies) Requiring Notification & Agency Information	Threshold, Timing, and Specific Content to be Included In Notice
Rhode Island	Attorney General Notify by U.S. Mail or Electronically: Office of the Attorney General Consumer Protection Unit 150 South Main Street Providence, Rhode Island 02903 consumers@riag.ri.gov	Threshold: If notice is given to >500 residents at once. Timing: In the most expedient time possible, but no later than 45 days. Specific Content: • Timing, content and distribution of notices. • Approximate number of affected individuals.
South Carolina	Consumer Protection Division of the Department of Consumer Affairs Notify by U.S. Mail: Legal Division RE: Security Breach Notification South Carolina Department of Consumer Affairs P.O. Box 5757 Columbia, SC 29250	Threshold: If notice is given to >1,000 residents at once Timing: Without unreasonable delay. Specific Content: • When the breach occurred. • When notice was given to affected persons. • Number of persons affected by the breach. • A copy of the notice sent to affected persons.
South Dakota	Attorney General Notify by mail or electronic mail	Threshold: If notice is given to >250 residents. Timing: None specified. Specific Content: None specified.

State	State Agency(ies) Requiring Notification & Agency Information	Threshold, Timing, and Specific Content to be Included In Notice
Vermont	Attorney General Notify by telephone, fax, or email: Phone: 802-828-5479 Fax: 802-828-5479 Email: data.security@atg.state.vt.us	Threshold: None specified. Timing: Within 14 days of discovering the breach. However, 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. Specific Content: • Date of the security breach. • Date of discovery of the breach. • Description of the breach. • Number of persons affected by the breach. • A copy of the notice sent to affected persons.
Virginia	Attorney General Notify by U.S. Mail: Computer Crime Section Virginia Attorney General's Office 900 East Main Street Richmond, VA 23219	Threshold: None specified. Timing: Without unreasonable delay. Specific Content: • A cover letter on official company letterhead. • Approximate date of the incident. • How the breach was discovered. • Cause of breach. • Number of VA residents affected by the breach. • Steps taken to remedy the breach. • Sample of notification to residents, to include any possible offers of free credit monitoring. If notice is provided to more than 1,000 individuals at one time, the notice to the attorney general must include the timing, distribution, and content of the notice to individuals.

State	State Agency(ies) Requiring Notification & Agency Information	Threshold, Timing, and Specific Content to be Included In Notice
Washington	Attorney General Notify by E-Mail: SecurityBreach@atg.wa.gov	Threshold: If notice is given to >500 residents at once Timing: By the time notice is provided to consumers. Specific Content: • A copy of the notice sent to affected persons (eliminating any PI). • Estimated number of WA residents affected by the breach.

7. Other Notification Requirements

State(s)	Notice Requirements
Texas	Requires disclosure of a breach to all individuals (regardless of the state of residency) whose personal information 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 law or under 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

4827-0484-8758, v. 1