



## WHITE PAPER:

### A COMPARISON OF STATE DATA PRIVACY NOTICE REQUIREMENTS

#### EXECUTIVE SUMMARY

Unauthorized access of personal, often sensitive, information given by consumers to various entities has become a common occurrence. Often called a “data breach,” or simply a “breach,” they have the potential to cause enormous harm to both consumers, and to the entities responsible for their personal information. *Thus far, there has been no Federal legislation that applies universally to breaches.* Various Federal statutes that regulate certain industries have breach notification components (e.g., GLBA and HIPAA). In the absence of comprehensive Federal action, all 50 states have enacted some form of breach notification law so that consumers will be made aware if their personal information is at risk of misuse.

Below is a White Paper, including a chart of the various state breach notification laws, current for 2022. Also included are the statutes for Puerto Rico and the Virgin Islands. This White Paper and chart is a reference guide comparing the law between jurisdictions and a starting point for more in-depth research in all jurisdictions.

Most, if not all, the statutes share structural similarities. Many are nearly identical in both structure and content. However, there are also important, or perhaps merely arguably important, distinctions between jurisdictions.

## EXAMPLE STANDARD NOTICE PROVISION

The following is an example of a typical statutory notice provision:

“(B)(1) Any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. The disclosure described in this division may be made pursuant to any provision of a contract entered into by the person with another person prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of this section and does not waive any provision of this section. For purposes of this section, a resident of this state is an individual whose principal mailing address as reflected in the records of the person is in this state.

(2) The person shall make the disclosure described in division (B)(1) of this section in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system.”

Ohio Rev. Code Ann. § 1349.19(B)(1)-(2).

## DEFINITIONS

To better understand the statutes, below are definitions of some key terms in this White Paper and chart.

1. “PERSONAL INFORMATION: “The term “personal information” (also called “sensitive information,” “personally identifiable information,” etc.) is a term-of-art that has various definitions across jurisdictions. Typically, the definition will include a number of “data elements” such as name, address, phone number, email address, and/or social security number, that if used either alone or together could identify an individual. A good rule of thumb is that if one were to have enough data elements to commit identity theft easily against a consumer, that set of data elements is considered personal information.

2. “BREACH:” The term “breach” (also called “security breach” or “breach of the security of the system”) is a term-of-art whose definition can vary quite widely. However, it always involves unauthorized access to personal information or data controlled by an entity.
3. “ENCRYPTED” or “REDACTED:” The terms “encrypted” and “redacted” are often used to describe data or data elements that due to their encrypted or redacted nature are either 1) not personal information, 2) if accessed are not considered a breach, or 3) if accessed require no notice to be given under the relevant statutory requirement. The definitions vary, but usually “encrypted” simply means the data has been secured with a “cryptographic key,” and “redacted” means that the majority of the data cannot be seen (think a receipt only showing the last digits of a credit card number). It is important to note that these terms are sometimes used interchangeably, or one term is used perhaps to the deliberate exclusion of the other. The specific definition used, and the jurisdictional legislative history may be particularly important in construing these terms.<sup>1</sup>
4. “COVERED ENTITY:” The term “covered entity” usually means an entity with some level of business contacts with that particular state. Each statute only applies to its definition of a “covered entity.” Some statutes specify that they apply to all business who maintain the personal information of their state residents.
5. “NOTICE:” The term “notice” is in all statutes because they require notice to individuals whose personal information has been breached. Many also require notice to state Attorneys General, various state regulators, and the major Consumer Reporting Agencies (often as defined in Federal statutes and regulations, also called “CRAs”). While the chart reflects the time period required to notify individuals of a breach, it does not reflect the time period to notify these other entities. Those time frames vary widely, close attention to the individual statutes is required to determine the timing for this reporting requirement. In certain jurisdictions it is required that reports to these entities are completed prior to reports to individuals. Often these reporting requirements are triggered by how much personal information is affected, how many individual notices need to be sent, or how many “consumers” are affected. The chart will usually simply mention the threshold of “affected” individuals necessary to trigger the requirement. Review of the individual statutes is required to determine what is an

---

<sup>1</sup> Often, the statutes will specify that any safe harbor for a breach that involves encrypted data depends on whether the “cryptographic key” has been stolen or is available to the unauthorized party in possession of the personal information. It is beyond the scope of this Paper to explore the technical aspects of cryptographic keys. It’s sufficient to say that if the breached information will remain encrypted without resort to code-breaking technology it will usually meet the definition of encrypted for safe-harbor under most state statutes. In such instances breached, but properly encrypted, personal information does not trigger notice requirements.

“affected” individual. The form and contents of the notice given to individuals and other entities is often detailed in the statute itself.

## **EXCEPTIONS AND DELAYS**

Most statutes allow for notice of a breach to be delayed, or even omitted entirely, under certain circumstances. While the particulars of each circumstance are often unique to the specific statute, broadly speaking the exceptions and delays fall into the following categories:

1. **LAW ENFORCEMENT DELAY/EXCEPTION:** Every statute has some form of “law-enforcement” delay or exception. This provision involves a law enforcement request that the breached entity refrain from giving notice that would interfere in an active investigation. This is usually in the form of a stand-alone provision, but may be part of the language of the notice requirement. This provision varies by statute, but generally requires documentation, and sets time-limits on delay of notification after law-enforcement informs the breached entity that its investigation will not be prejudiced by notice. This will usually extend the time-period for notice beyond any specific number of days specified in the statute.
2. **MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE BREACH DELAY:** Most statutes have a “measures necessary to determine the scope of the breach” delay. This delay is rarely a stand-alone provision and is often part of the language of the notice requirement. This delay is usually worded such that a breached entities delay of notice for purposes of investigating and remediating a breach is presumptively “reasonable.” This usually will not extend the time-period for notice if specified in a number of days.
3. **RISK BASED EXCEPTION:** Some statutes have “risk based” exception. This exception voids the requirement to give notice of a breach if there is not a risk of harm to an individual consumer. The analysis required to determine the risk varies widely, but often required consultation with experts, law enforcement, the state Attorney General, and documentation of the determination that is maintained for a number of years.
4. **FEDERAL STATUTORY EXEMPTIONS:** Many statutes have exemptions for entities already required to give notice under a Federal law, such as the GLBA or HIPAA. Some statutes only give an exemption to one or another, and some are predicated on certain other conditions. For those that do not have these exemptions, the preemptive effect (if any) of the Federal laws is an open question.
5. **INFORMATION SECURITY COMPLIANCE EXCEPTION:** Many statutes have an exception for an entity that maintains an information security compliance program that

requires notice to individuals for breaches. This often requires documentation, must be substantially similar to the statute, and is by no means a universal exception.

## OTHER ISSUES

Some statutes contain an explicit private right of action for violation of the notice provision. The absence of this explicit provision does not mean that no private right of action exists, this is a highly jurisdictional issue. If there is an explicit private right of action, that is noted in the chart. Many statutes have an exception for publicly available information. This usually covers data elements that can be taken from public data bases, such as addresses from property tax information. However, even with the exception, it is possible that information may be both “publicly available” and “personal information” subject to notice requirements depending on the nature of the breach and the entity holding the information.

Many statutes have a requirement that 3<sup>rd</sup> parties holding personal information on behalf of an entity (think, a cloud servicer hosting a website for a business) report a breach to the entity, rather than to individuals. This notice requirement usually has a short, even immediate, timeframe. The relationship often described is similar to the relationship described under HIPAA as “Business Associate” and under the GDPR as “Data Processor.” A review of those terms may be instructive in construing these notice requirements.

There are many additional issues presented in comparing and construing these statutes, if you have any questions or comments, please contact Attorney Timothy L. Garvey, of Brownson PLLC, at:

Timothy L. Garvey  
BROWNSON PLLC  
4800 Capella Tower  
225 South Sixth Street  
Minneapolis, MN 55402  
612-332-4020  
[tgarvey@brownsonpllc.com](mailto:tgarvey@brownsonpllc.com)



## STATE DATA PRIVACY NOTICE REQUIREMENTS CHART

### ABSTRACT

A chart surveying the statutory notice requirements in the event of a data breach across the fifty states, as well as Puerto Rico and the Virgin Islands.

TIMOTHY L. GARVEY

State	Statute	Notification to Individuals	Notification to Others	Encryption, Law Enforcement, and Risk Exceptions	Explicit Private Right of Action	Selected Cases in Jurisdiction
AL	Ala. Code § 8-38-1 <i>et seq.</i>	As expeditiously as possible and without unreasonable delay, taking into account time necessary for investigation. No more than 45 days.	<p>Notice to AG<sup>1</sup> if notice is required to more than 1,000 individuals.</p> <p>Notice to CRAs<sup>2</sup> if notice required to more than 1,000 individuals at one time.</p>	<p>Encrypted data is not sensitive personally identifying information, unless the key has also been breached.</p> <p>Notice may be delayed per written request of law enforcement agency.</p> <p>If the breach is not reasonably likely to cause substantial harm.</p>	No.	<i>Blahous v. Sarrell Regional Dental Center for Public Health, Inc.</i> , No. 2:19-cv-798-RAH-SMD, 2020 WL 401624 (M.D. Ala. July 16, 2020).

---

<sup>1</sup> Refers to the State Attorney General’s Office

<sup>2</sup> Refers to the national Consumer Reporting Agencies, often as defined under federal statute (e.g., 15 U.S.C. § 1681a(p)).

<p><b>AK</b></p>	<p>Alaska Stat. §45.48.010 <i>et seq.</i></p>	<p>In the most expeditious time possible and without unreasonable delay, except as necessary to determine the scope of the breach and restore the reasonable integrity of the system.</p>	<p>Notice to AG is required.</p> <p>Notice to CRAs is required if notice is required to 1,000 or more individuals.</p>	<p>“Personal information” excludes encrypted or redacted data, so long as the key has not been “accessed or acquired.”</p> <p>Notice may be delayed at request of law enforcement agency.</p> <p>If there is not “a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from breach.”</p> <p>Notification to AG still required.</p>	<p>Yes.</p>	<p>None.</p>
------------------	---	---	--	---	-------------	--------------



AZ	Ariz. Rev. Stat. §18-551 to 552.	Within 45 days.	<p>Notice to State AG is required if notice to more than 1,000 individuals is required.</p> <p>Notice to CRAs is required if notice to more than 1,000 individuals is required.</p>	<p>“Breach” does not include encrypted or redacted information where the key is confidential.</p> <p>Notice may be delayed if law enforcement agency “advises” that the notifications will impede a criminal investigation.</p> <p>If “the person, an independent third-party forensic auditor or a law enforcement agency determines after a reasonable investigation that a security system breach has not resulted in or is not reasonably likely to result in a substantial economic loss to affected individuals.”</p>	No.	None.
----	----------------------------------	-----------------	---	---	-----	-------

<p><b>AR</b></p>	<p>Ark. Code § 4-110-101 <i>et seq.</i></p>	<p>In the most expedient time and manner possible and without unreasonable delay, taking into account legitimate needs of law enforcement or any measures necessary for investigation of breach.</p>	<p>Notice to state AG is required, if notice is required to more than 1,000 individuals.</p>	<p>“Personal Information” does not include encrypted or redacted data.</p> <p>Can delay for legitimate needs of law enforcement.</p> <p>No notification is required upon determination that there is no reasonable likelihood of harm to consumers.</p>	<p>No.</p>	<p>None.</p>
------------------	---	--	--	---	------------	--------------

CA	Cal. Civ. Code § 1798.82 et seq.	The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement...or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	<p>Notice to state AG is required if notice is required if 500 CA residents.</p> <p>Note: Different time for medical information under Health and Safety Code § 1280.15.</p>	<p>Encrypted personal information taken without the accompanying key or credential, or where the key or credential are not reasonably believed to be able to decrypt the personal information, are not subject to the disclosure requirements.</p> <p>Can delay for law enforcement needs.</p>	Yes.	<p><i>In re Ambry Genetics Data Breach Litigation</i>, SACV 20-00791-CJC, 2021 WL 4891610 (C.D.Cal. Oct. 18, 2021).</p> <p><i>In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.</i>, No. 3:19-CV-2284-H-KSC, 2020 WL 2214152 (S.D. Cal. May 7, 2020)</p> <p><i>In re Yahoo! Inc. Customer Data Sec. Breach Litig.</i>, 313 F. Supp. 3d 1113 (N.D. Cal. 2018)</p> <p><i>In re Sony Gaming Networks &amp; Customer Data Sec. Breach Litig.</i>, 996 F. Supp. 2d 942 (S.D. Cal. 2014), <i>order corrected</i>, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014)</p>
----	----------------------------------	--	--	--	------	---

CO	Colo. Rev. Stat. § 6-1-716	Notice must be made in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.	Notice to AG required if 500 Colorado residents.	Encrypted data excluded from definition of "Personal Information."  Can delay for law enforcement needs.	No.	None.
----	----------------------------	--	--	--	-----	-------

CT	Conn. Gen. Stat. § 36a-701b.	Without unreasonable delay, but not later than sixty days after the discovery of such breach, unless a shorter time is required under federal law.	Notice to AG required, no later than notice to affected individuals.	<p>Personal information secured by encryption is excluded from definition of “breach of security.”</p> <p>Can delay for law enforcement needs.</p> <p>No notification required if no risk of harm to consumers.</p>	No.	<i>Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.</i> , 147 Conn. App. 450, 83 A.3d 664 (2014), <i>aff’d</i> , 317 Conn. 46, 115 A.3d 458 (2015)
----	------------------------------	--	--	---	-----	---

<b>DE</b>	Del. Code. Tit. 6 § 12B-101 et seq.	Without unreasonable delay, but not later than 60 days unless a shorter time is required by federal law.	Notice to AG required if more than 500 DE residents.	<p>“[B]reach of security” definition excludes encrypted personal information.</p> <p>Can delay for law enforcement needs.</p> <p>Can delay if through “reasonable diligence” it cannot be determined whether DE resident’s information was breached.</p> <p>No notification required if no risk of harm to consumers.</p>	No.	None.
-----------	-------------------------------------	--	--	---	-----	-------

<b>DC</b>	D.C. Code § 28-3851 et seq.	Most expedient time possible and without unreasonable delay, consistent with legitimate needs of law enforcement and measures necessary to determine scope of breach.	<p>Notice to AG is required if 50 or more D.C. residents are affected.</p> <p>Notice to CRAs required if more than 1,000 individuals.</p>	<p>“[B]reach of the security of the system” definition excludes encrypted or redacted data.</p> <p>“[B]reach of the security of the system” definition also excludes acquisition of personal information that will likely not result in harm to the individual.</p> <p>Can delay for law enforcement needs.</p>	No.	None.
<b>FL</b>	Fla. Stat. § 501.171.	As expeditiously as practicable, taking into account time to determine scope of breach, but no later than 30 days.	<p>Notice to Department of Legal Affairs required if 500 or more FL individuals.</p> <p>Notice to CRAs required if more than 1,000 individuals.</p>	<p>“Personal Information” definition excludes encrypted information.</p> <p>Can delay for law enforcement needs.</p> <p>No notification required if breach will not result in harm to individuals.</p>	No.	None.

<b>GA</b>	Ga. Code § 10-1-910 et seq.	Most expedient time possible and without unreasonable delay, consistent with legitimate needs of law enforcement and measures necessary to determine scope of breach.	Notice to CRAs required if 10,000 or more GA residents affected.	“Personal Information” definition excludes encrypted or redacted data.  May delay for law enforcement needs.	No.	<i>In re Equifax, Inc., Customer Data Sec. Breach Litig.</i> , 362 F. Supp. 3d 1295, (N.D. Ga. 2019)  <i>Willingham v. Glob. Payments, Inc.</i> , No. 1:12-CV-01157-RWS, 2013 WL 440702, (N.D. Ga. Feb. 5, 2013)
<b>HI</b>	Haw. Rev. Stat. § 487N-1 et seq.	Without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	Notice to State Office of Consumer Protection required if more than 1,000 individuals affected.  Notice to CRAs required if more than 1,000 individuals affected.	“Personal information” definition excludes encrypted data.  “Security breach” definition also excludes encrypted data.  May delay for law enforcement needs.	Yes.	None.



<b>ID</b>	Idaho Code §28-51-104 et seq.	Most expedient time possible and without unreasonable delay, consistent with needs of law enforcement and measures necessary to determine scope of breach.	Agency notice to AG required (term “agency” may be ambiguous).	<p>“Breach of the security of the system” definition excludes encrypted data.</p> <p>“Personal information” definition excludes encrypted data elements.</p> <p>May delay for law enforcement needs.</p> <p>No notification required if personal information breached is not reasonably likely to be misused.</p>	No.	None.
-----------	-------------------------------	--	--	---	-----	-------

<p><b>IL</b></p>	<p>815 Ill. Comp. Stat. 530/1 et seq.</p>	<p>Most expedient time possible and without unreasonable delay, consistent with measures to determine scope of breach.</p>	<p>Notice to AG required if more than 500 IL residents affected.</p> <p>Notice to AG in event of state agency breach required if 250 IL residents or more affected.</p> <p>Notice to CRAs in event of state agency breach required if 1,000 or more IL residents.</p>	<p>“Personal information” definition excludes encrypted data elements. Note* the definition of “breach” in the statute refers to “computerized data” rather than personal information.</p> <p>May be delayed for law enforcement needs.</p>	<p>No.</p>	<p><i>Cnty. Bank of Trenton v. Schnuck Markets, Inc.</i>, 887 F.3d 803 (7th Cir. 2018)</p> <p><i>Cooney v. Chicago Pub. Sch.</i>, 407 Ill. App. 3d 358, 943 N.E.2d 23 (2010)</p> <p><i>Irwin v. Jimmy John's Franchise, LLC</i>, 175 F. Supp. 3d 1064 (C.D. Ill. 2016)</p> <p><i>Worix v. MedAssets, Inc.</i>, 869 F. Supp. 2d 893 (N.D. Ill. 2012)</p> <p><i>In re Michaels Stores Pin Pad Litig.</i>, 830 F. Supp. 2d 518, 521 (N.D. Ill. 2011)</p>
------------------	---	--	---	---	------------	---

<b>IN</b>	Ind. Code § 24-4.9-1-1 et seq.	Without unreasonable delay, but not more than 45 days after discovery of breach.	<p>Notice to AG required if more than 1,000 consumers affected.</p> <p>Notice to CRAs required if more than 1,000 consumers affected.</p>	<p>“Breach of security of the data” definition does not include encrypted data.</p> <p>Delay is reasonable for law enforcement needs and to determine scope of breach. Note* ambiguity as to “reasonable delay” and 45-day requirement.</p>	No.	<i>Pisciotta v. Old Nat. Bancorp</i> , 499 F.3d 629 (7th Cir. 2007)
<b>IA</b>	Iowa Code § 715C.1 & 2.	Most expeditious manner possible and without unreasonable delay, consistent with law enforcement and measures to determine scope of breach.	Notice to consumer protection office of the AG is required if more than 500 IA residents are affected.	<p>“Personal information” definition excludes encrypted data elements.</p> <p>May delay for law enforcement needs.</p> <p>Notification not required if no reasonable likelihood of financial harm.</p>	No.	None.

KS	Kan. Stat. § 50-7a01 et seq.	Most expedient time possible and without unreasonable delay, consistent with needs of law enforcement and measures to determine scope of breach.	Notice to CRAs required if more than 1,000 KS residents affected.	<p>“Security breach” definition excludes encrypted or redacted data.</p> <p>“Security breach” definition also excludes compromises that are not reasonably believed to cause identity theft to any consumer.</p> <p>May delay for law enforcement needs.</p>	No.	None.
----	------------------------------	--	---	--	-----	-------

<p><b>KY</b></p>	<p>Ky. Rev. Stat. § 365.730 et seq.</p>	<p>Most expedient time possible and without unreasonable delay, consistent with needs of law enforcement and measures to determine scope of breach.</p>	<p>Notice to CRAs required if more than 1,000 KY residents affected.</p>	<p>No notification required if personal information was encrypted.</p> <p>“Breach of the security of the system” definition excludes encrypted or redacted data.</p> <p>“Breach of the security of the system” definition also excludes compromises that are not reasonably believed to cause identity theft or fraud.</p> <p>May delay for law enforcement needs.</p>	<p>Yes (for improper destruction of PI, not lack of notification).</p>	<p><i>Savidge v. Pharm-Save, Inc.</i>, No. 3:17-CV-00186-TBR, 2017 WL 5986972 (W.D. Ky. Dec. 1, 2017)</p>
------------------	---	---	--	--	--	---

<b>LA</b>	La. Rev. Stat. § 51:3071 et seq.	Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach, but not later than 60 days.	Notice to AG is required if reasonable delay is required.	<p>“Personal information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>Notification not required if no reasonable likelihood of harm to residents of LA.</p>	Yes.	<p><i>Melancon v. Louisiana Off. of Student Fin. Assistance</i>, 567 F. Supp. 2d 873 (E.D. La. 2008)</p> <p><i>Ponder v. Pfizer, Inc.</i>, 522 F. Supp. 2d 793 (M.D. La. 2007)</p>
<b>ME</b>	10 Me. Rev. Stat. § 1346 et seq.	As expediently as possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach, but not later than 30 days.	<p>Notice to appropriate state regulators within Department of Professional and Financial Regulation, or AG, is required.</p> <p>Notice to CRAs required if more than 1,000 persons affected.</p>	<p>“Personal information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>Non-“information brokers” do not need to give notice if it is not reasonably possible that the breached personal information will be misused.</p>	No.	<p><i>In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.</i>, 613 F. Supp. 2d 108 (D. Me. 2009), <i>aff'd in part, rev'd in part sub nom. Anderson v. Hannaford Bros. Co.</i>, 659 F.3d 151 (1st Cir. 2011)</p>

<b>MD</b>	Md. Code Com. Law § 14-3504 et seq.	As soon as reasonably practicable, but no later than 45 days.	<p>Notice to AG is required prior to notification of any individual.</p> <p>Notice to CRAs required if more than 1,000 individuals affected.</p>	<p>“Personal information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>No notice required if no likelihood of misuse of personal information.</p>	No.	<p><i>In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.</i>, 440 F. Supp. 3d 447 (D. Md. 2020)</p> <p><i>Chambliss v. Carefirst, Inc.</i>, 189 F. Supp. 3d 564, 570 (D. Md. 2016)</p>
<b>MA</b>	Mass. Gen. Laws 93H § 1 et seq.	As soon as practicable and without unreasonable delay.	<p>Notice to AG and director of consumer affairs and business regulation is required.</p> <p>Notice to CRAs required at direction of director of consumer affairs and business regulation.</p>	<p>“Breach of security” definition excludes encrypted data.</p> <p>May delay for law enforcement needs.</p>	Likely yes. Note* contained in section on SSN breaches, and vaguely worded.	<p><i>Katz v. Pershing, LLC</i>, 672 F.3d 64 (1st Cir. 2012)</p> <p><i>Adams v. Cong. Auto Ins. Agency, Inc.</i>, 90 Mass. App. Ct. 761, 65 N.E.3d 1229 (2016)</p>

<b>MI</b>	Mich. Comp. Laws § 445.63 & 445.72	Without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	Notice to CRAs required if 1,000 or more MI residents affected.	Notice is not required if personal information was redacted.  May delay for law enforcement needs.	No.	None.
<b>MN</b>	Minn. Stat. § 325E.61.	Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	Notice to CRAs required if more than 500 persons affected.	No notice required if personal information was encrypted.  May delay for law enforcement needs.	No.	<i>In re Target Corp. Data Sec. Breach Litig.</i> , 66 F. Supp. 3d 1154 (D. Minn. 2014)



<b>MS</b>	Miss. Code § 75-24-29.	Without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	None.	<p>“Breach of security” definition excludes encrypted data.</p> <p>May delay for law enforcement needs.</p> <p>Notice not required if no likely harm to affected individuals.</p>	No.	None.
<b>MO</b>	Mo. Rev. Stat. § 407.1500.	Without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	<p>Notice to AG required if more than 1,000 consumers affected.</p> <p>Notice to CRAs required if more than 1,000 consumers affected.</p>	<p>“Personal information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>Notification not required if risk of identity theft or fraud to any consumer not reasonably likely to occur.</p>	No.	<i>Amburgy v. Express Scripts, Inc.</i> , 671 F. Supp. 2d 1046 (E.D. Mo. 2009)

<b>MT</b>	Mont. Code § 30-14-1701 et seq.	Without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	<p>Notice to AG consumer protection office required.</p> <p>Notice to CRAs may be required. Note* section is ambiguous and may require notice only where specific CRA information is included in notice to individual.</p>	<p>Notice is not required where personal information was encrypted.</p> <p>May delay for law enforcement needs.</p>	No.	None.
-----------	---------------------------------	--	--	---	-----	-------

NE	Neb. Rev. Stat. § 87-801 et seq.	As soon as possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach	Notice to AG is required.	<p>“Breach of the security of the system” definition excludes encrypted data.</p> <p>“Personal information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>No notice required if personal information not reasonably likely to be used for an unauthorized purpose.</p>	No.	None.
----	----------------------------------	---	---------------------------	--	-----	-------

<b>NV</b>	Nev. Rev. Stat. 603A.010 et seq.	Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	Notice to CRAs is required if more than 1,000 persons are affected.	<p>No notification required if personal information is encrypted.</p> <p>“Personal information” definition excludes encrypted data elements.</p> <p>May delay for law enforcement needs.</p>	Yes. Note* this is a private cause of action for the data collector for being breached, rather than against it for failure to give notice.	None.
<b>NH</b>	N.H. Rev. Stat. § 359-C:19 et seq.	As soon as possible.	<p>Notice to state regulator with primary regulatory authority, or AG, is required.</p> <p>Notice to CRAs required if more than 1,000 consumers affected.</p>	<p>“Personal information” definition excludes encrypted data elements.</p> <p>May delay for law enforcement needs.</p> <p>No notification required where personal information is not reasonably likely to be misused.</p>	Yes.	None.

NJ	N.J. Stat. § 56:8-161 to 56:8-166.1	Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	<p>Notice to the Division of State Police in the Department of Law and Public Safety required.</p> <p>Notice to CRAs required if more than 1,000 persons affected.</p>	<p>“Breach of security” definition excludes encrypted data.</p> <p>May delay for law enforcement needs.</p> <p>Notice not required if misuse of personal information not reasonably possible.</p>	No.	<i>In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.</i> , No. CV 19-MD-2904, 2021 WL 5937742 (D.N.J. Dec. 16, 2021)
----	-------------------------------------	---	--	---	-----	--

<p><b>NM</b></p>	<p>N.M. Stat. § 57-12C-6 et seq.</p>	<p>Most expedient time possible, but not later than 45 days.</p>	<p>Notice to AG required if more than 1,000 NM residents affected.</p> <p>Notice to CRAs required if more than 1,000 NM residents affected.</p>	<p>“[P]ersonal identifying information” definition excludes encrypted or redacted data elements.</p> <p>“[S]ecurity breach” definition excludes encrypted data.</p> <p>May delay for law enforcement needs.</p> <p>May delay to determine scope of breach.</p> <p>Notice not required if there is not significant risk of identity theft or fraud.</p>	<p>No.</p>	<p>None.</p>
------------------	--------------------------------------	--	---	--	------------	--------------

NY	N.Y. Gen. Bus. Law § 899-aa.	Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	<p>Notice to AG required.</p> <p>Notice to department of state required.</p> <p>Notice to division of state police required.</p> <p>Notice to CRAs required if more than 5,000 NY residents affected.</p>	<p>“Private information” definition excludes encrypted data element.</p> <p>May delay for law enforcement needs.</p>	No.	<i>Abdale v. N. Shore Long Island Jewish Health Sys., Inc.</i> , 49 Misc. 3d 1027, 19 N.Y.S.3d 850 (N.Y. Sup. Ct. 2015)
----	------------------------------	---	---	--	-----	---

NC	N.C. Gen Stat. § 75-60 et seq.	Without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	<p>Notice to Consumer Protection Division of AGs Office required.</p> <p>Notice to CRAs required if more than 1,000 persons affected.</p>	<p>“Security breach” definition excludes encrypted or redacted data.</p> <p>May delay for law enforcement needs.</p>	Yes.	<p><i>Rogers v. Keffer, Inc.</i>, 243 F. Supp. 3d 650 (E.D.N.C. 2017)</p> <p><i>Best v. Cequel</i>, No. 4:14-CV-61-FL, 2014 WL 6453960 (E.D.N.C. Nov. 17, 2014), <i>aff'd</i>, 598 F. App'x 178 (4th Cir. 2015)</p> <p><i>Owens v. Dixie Motor Co.</i>, No. 5:12-CV-389-FL, 2014 WL 12703392 (E.D.N.C. Mar. 31, 2014)</p> <p><i>Fisher v. Commc'n Workers of Am.</i>, No. 08 CVS 3154, 2008 WL 4754850 (N.C. Super. Oct. 30, 2008)</p>
----	--------------------------------	--	---	--	------	--



<p><b>ND</b></p>	<p>N.D. Cent. Code § 51-30-01 et seq.</p>	<p>Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.</p>	<p>Notice to AG required if more than 250 individuals affected.</p>	<p>“Breach of the security of the system” definition excludes personal information secured by encryption.</p> <p>“Personal information” definition excludes encrypted data elements.</p> <p>Notice not required where breached personal information was encrypted.</p> <p>May delay for law enforcement needs.</p>	<p>No.</p>	<p>None.</p>
------------------	---	--	---	--	------------	--------------

<b>OH</b>	Ohio Rev. Code § 1349.19	Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach, but not more than 45 days.	Notice to CRAs required if more than 1,000 OH residents affected.	<p>“Personal information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>No notice required if no material risk of identity theft or other fraud to the resident.</p>	No.	<i>Mulkey v. RoundPoint Mortg. Servicing Corp.</i> , No. 1:21 CV 01058, 2021 WL 5804575 (N.D. Ohio Dec. 7, 2021)
<b>OK</b>	Ok. Stat. Tit. 24 § 161 et seq.	Without unreasonable delay consistent with needs of law enforcement and measures to determine scope of the breach.	None.	<p>“Breach of the security of the system” definition excludes encrypted or redacted data.</p> <p>“Personal information” excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>No notice required if no reasonable belief breach will cause identity theft or fraud to any OK resident.</p>	No.	None.

<b>OR</b>	Or. Rev. Stat. § 646A.600 et seq.	Most expeditious manner possible, without unreasonable delay, but not later than 45 days.	<p>Notice to AG required if more than 250 consumers affected.</p> <p>Notice to CRAs required if more than 1,000 consumers affected.</p>	<p>“Personal information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>No notice required if consumers are unlikely to suffer harm.</p>	No.	None.
-----------	-----------------------------------	---	---	--	-----	-------

PA	73 Pa. Stat. and Cons. Stat. Ann. § 2301 et seq.	Without unreasonable delay consistent with law enforcement needs and measures to determine scope of the breach.	Notice to CRAs required if more than 1,000 individuals affected.	<p>“Personal information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>No notice required breach involves encrypted or redacted personal information.</p>	No.	<i>Dittman v. UPMC</i> , 649 Pa. 496, 196 A.3d 1036 (2018)
----	--	---	--	--	-----	--

<p><b>PR</b></p>	<p>P.R. Laws Tit. 10 § 4051 et seq.</p>	<p>Clients must be notified as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security. Within a non-extendable term of 10 days after the violation of the system's security has been detected, the parties responsible shall inform the Department, which shall make a public announcement of the fact within 24 hours after having received the information. Note* relatively unique statutory language.</p>	<p>Notice to the Department of Consumer Affairs required.</p>	<p>“Personal information file” definition excludes information for which a cryptographic code is needed.</p> <p>No notice is required if personal information files are protected by an encrypted code, however, only a password is not sufficient. Note* potential gap for plaintext files protected by only a password.</p>	<p>Likely yes. Note* statute is vague as to creation of remedy.</p>	<p>None.</p>
------------------	---	--	---	---	---	--------------

<p><b>RI</b></p>	<p>R.I. Gen. Laws § 11-49.3-1 &amp; 11-49-3.6.</p>	<p>Most expedient time possible, consistent with needs of law enforcement and the ability to ascertain the information required to fulfill the notice requirements, but not later than 45 days.</p>	<p>Notice to AG required if more than 500 RI residents affected.</p> <p>Notice to CRAs required if more than 500 RI residents affected.</p>	<p>“Breach of the security of the system” definition excludes encrypted data.</p> <p>“Personal information” definition excludes encrypted data elements.</p> <p>May delay for law enforcement needs.</p> <p>No notice required where breach does not pose significant risk of identity theft to any RI resident.</p>	<p>No.</p>	<p>None.</p>
------------------	--	---	---	--	------------	--------------

SC	S.C. Code Ann. § 39-1-90.	Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	<p>Notice to Consumer Protection Division of the Department of Consumer Affairs required if more than 1,000 persons affected.</p> <p>Notice to CRAs required if more than 1,000 persons affected.</p>	<p>“Breach of the security of the system” definition excludes encrypted or redacted data.</p> <p>“Personal identifying information” definitions excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>Notice is not required if use of breached information does not create material risk of harm to SC resident and is not reasonably likely to be used illegally.</p>	Yes.	<i>In re Blackbaud, Inc., Customer Data Breach Litig.</i> , No. 3:20-MN-02972-JMC, 2021 WL 3568394 (D.S.C. Aug. 12, 2021)
----	---------------------------	---	---	--	------	---

<b>SD</b>	S.D. Cod. Laws § 22-40-19 to 22-40-26.	No later than 60 days.	<p>Notice to AG is required if more than 250 SD residents are affected.</p> <p>Notice to CRAs required.</p>	<p>“Breach of system security” definition excludes encrypted data.</p> <p>May delay for law enforcement needs.</p> <p>No notice required if breach will likely not result in harm to affected person.</p>	No.	None.
<b>TN</b>	Tenn. Code Ann. §47-18-2102 et seq.	No later than 45 days.	Notice to CRAs required if more than 1,000 persons affected.	<p>“Breach of system security” definition excludes encrypted data.</p> <p>May delay for law enforcement needs.</p>	Yes.	<p><i>Walton v. Nova Info. Sys.</i>, No. 3:06-CV-292, 2008 WL 1751525 (E.D. Tenn. Apr. 11, 2008)</p> <p><i>Wolfe v. MBNA Am. Bank</i>, 485 F. Supp. 2d 874, 890 (W.D. Tenn. 2007)</p>



TX	Tex. Bus. Com. Code § 521.053	Without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach, but not later than 60 days.	<p>Notice to AG required if 250 residents of TX affected.</p> <p>Notice to CRAs required if more than 10,000 persons affected.</p>	<p>“Sensitive personal information” definition excludes encrypted data.</p> <p>“[B]reach of system security” excludes properly encrypted data. Note* properly here is used not because this differs in any material way from other similar statutes, but because the language of the statute is unique as to encryption.</p> <p>May delay for law enforcement needs.</p>	No.	<i>Bliss &amp; Glennon Inc. v. Ashley</i> , 420 S.W.3d 379, 395 (Tex. App. 2014)
----	-------------------------------	--	--	--	-----	--

UT	Utah Code § 13-44-101 et seq.	Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	None.	<p>“Personal information” definition excludes encrypted data elements.</p> <p>May delay for law enforcement needs.</p> <p>No notice required if no reasonable likelihood of misuse of personal information for identity theft or fraud purposes.</p>	No.	None.
----	-------------------------------	---	-------	--	-----	-------

VT	9 VT. Stat. Ann. § 2435.	Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach, but not later than 45 days.	<p>Notice to Department of financial Regulation or AG required.</p> <p>Notice to CRAs required if 1,000 or more consumers affected.</p>	<p>“Data broker security breach” definition excludes encrypted data elements. Note* statute also has “security breach” definition that does not exclude encrypted data elements.</p> <p>“Personally identifiable information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>Notice not required if misuse of breached information not reasonably possible.</p>	No.	None.
----	--------------------------	---	---	--	-----	-------

<p><b>VA</b></p>	<p>Va. Code Ann. § 18.2-186.6</p>	<p>Without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.</p>	<p>Notice to AG required.</p> <p>Notice to CRAs required if more than 1,000 persons affected.</p>	<p>“Breach of the security of the system” definition excludes encrypted or redacted data.</p> <p>“Personal information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>No notice required if there is no reasonable belief that breach will cause identity theft or another fraud to individuals.</p>	<p>Yes. Note* Statute is not “explicit” in creating private right of action, but subsequent case law has found that there is such a right.</p>	<p><i>Schmidt v. Experian Info. Sols., Inc.</i>, No. 120CV358AJTJFA, 2020 WL 7680548 (E.D. Va. Nov. 13, 2020)</p> <p><i>In re Cap. One Consumer Data Sec. Breach Litig.</i>, 488 F. Supp. 3d 374 (E.D. Va. 2020)</p>
------------------	-----------------------------------	---	---	--	--	--

VI	V.I. Code Tit. 14 § 2208 et seq.	Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	None.	<p>“[P]ersonal information” definition excludes encrypted data elements.</p> <p>May delay for law enforcement needs.</p>	Yes.	None.
----	----------------------------------	---	-------	--	------	-------

<p><b>WA</b></p>	<p>Wash. Rev. Code. § 19.255.005 et seq.</p>	<p>Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach, but not later than 30 days.</p>	<p>Notice to AG is required if more than 500 WA residents affected.</p>	<p>“Personal information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>“Personal information” definition excludes data elements or combination thereof that would not enable a person to commit identity theft against a consumer. Note* this is a unique creation of a risk/harm analysis safe harbor.</p>	<p>Yes. Note* cases on this point have found there is no right of action for lack of notice, but there is for failure to properly secure data, but this may be altered by the 2020 amendment.</p>	<p><i>Buckley v. Santander Consumer USA, Inc.</i>, No. C17-5813 BHS, 2018 WL 1532671 (W.D. Wash. Mar. 29, 2018)</p> <p><i>Grigsby v. Valve Corp.</i>, No. C12-0553JLR, 2013 WL 12310666 (W.D. Wash. Mar. 18, 2013)</p>
------------------	--	--	---	--	---	--

<b>WV</b>	W.Va. Code § 46A-2A-101 et seq.	Without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	Notice to CRAs required if more than 1,000 persons affected.	<p>“Breach of the security of the system” definition excludes encrypted or redacted data.</p> <p>“Personal information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p> <p>Notice not required if breached data was encrypted or redacted.</p> <p>Notice not required if breached data is not reasonably believed to cause identity theft or other fraud.</p>	No.	None.
<b>WI</b>	Wis. Stat. § 134.98.	Within a reasonable time, not to exceed 45 days.	Notice to CRAs required if 1,000 or more individuals affected.	<p>“Personal information” definition excludes encrypted or redacted data elements.</p> <p>May delay for law enforcement needs.</p>	No.	<i>Fox v. Iowa Health Sys.</i> , 399 F. Supp. 3d 780, 800 (W.D. Wis. 2019)

WY	Wyo. Stat. § 40-12-501 et seq.	Most expedient time possible and without unreasonable delay consistent with needs of law enforcement and measures to determine scope of breach.	None.	<p>“Personal identifying information” definition excludes redacted data elements. Note* the statute does not mention encryption.</p> <p>May delay for law enforcement.</p> <p>No notice required if no reasonable likelihood of misuse of personal information.</p>	No.	None.
----	--------------------------------	---	-------	---	-----	-------