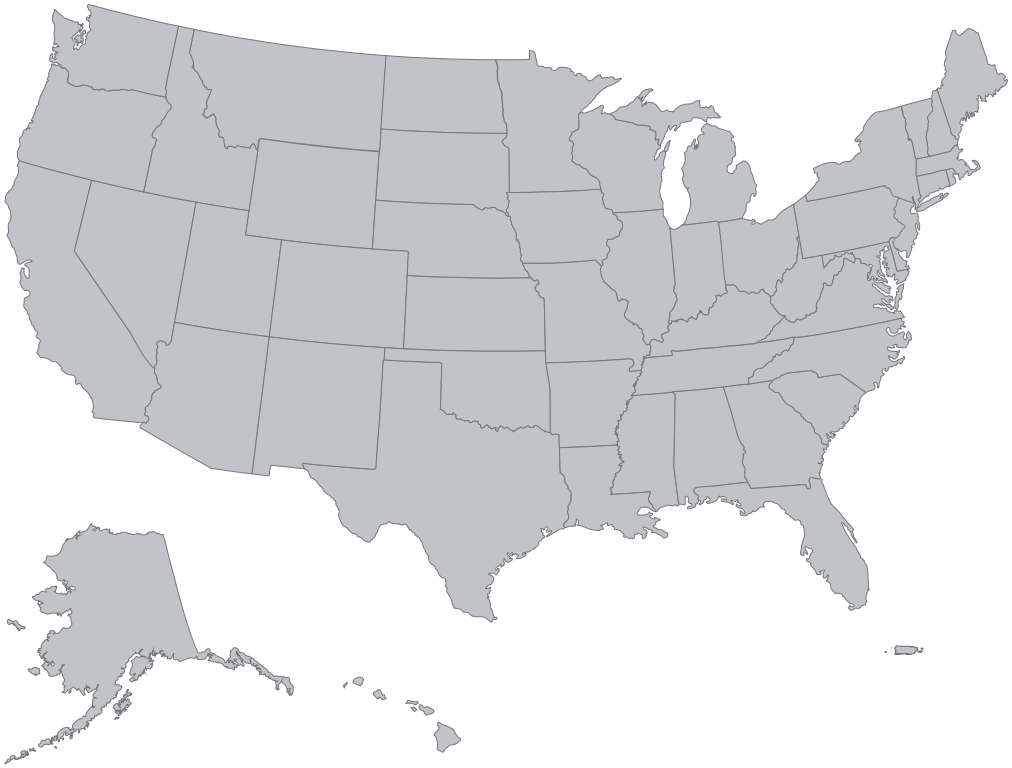
Weil

Security Breach Notification Laws

Data Privacy Survey 2014



Security Breach Notification Laws

Data Privacy Survey 2014

> “The likelihood of a **data breach** is no longer a question; it is almost a **certainty**.”

— Experian, *2014 Data Breach Industry Forecast*

Table of Contents

Note: All data contained herein is accurate as of April 24, 2014.

Please note that the following summary of state data breach notification statutes is for informational purposes only and does not constitute legal advice. Data breach laws change quickly. This summary is not intended to be and should not be used as a substitute for reviewing the latest statutes and consulting with counsel.

Introduction

By Christopher J. Cox and David R. Singh

Businesses today collect ever-increasing amounts of personal information about their customers, from account passwords and email addresses to highly sensitive medical and financial information. Well-funded, sophisticated hackers are always looking for ways to obtain such information or access and exploit a company's most sensitive, confidential data. As a result, companies face greater risks than ever from lapses in data security. As of April 7, 2014, The Privacy Rights Clearinghouse reported 619 data security breaches in the United States in 2013 alone, comprising over 250 million individual records.[1] These breaches have many causes, including criminal hacking, intentional leaks by insiders, unintended public disclosures, lost laptops or flash drives, and general negligence. As a result, data breaches are difficult to predict and even more difficult to prevent.

In 2013, The Privacy Rights Clearinghouse reported more than 600 data security breaches —comprising in excess of 250 million individual records—in the United States.

A data breach can result in massive exposure for businesses. According to a recent study, the average cost of a data breach to a U.S. company was $188 per record compromised.[2] If thousands or even millions of customer records are affected, the damages may be substantial – this is repeatedly evidenced as more and more well-known companies experience data breaches. In 2007, for example, the TJX Companies projected costs of over $250 million due to a data breach involving the theft of some 45 million customer credit and debit card numbers.[3] Target Corporation is still incurring costs from the criminal hacking of its point-of-sale systems in late 2013 and the accessing of sensitive information belonging to millions of customers, including debit and credit card data.

The costs from a breach of data security are varied. In addition to the immediate expenses for investigating and repairing the breach, companies should expect to incur costs to notify affected parties, manage public relations, and respond to government inquiries and investigations. A company may also face legal action on multiple fronts, from consumer or shareholder class actions to lawsuits from affected business partners to FTC or state attorney general enforcement actions. And, perhaps most significantly, there may be serious long-term reputational impact on the business's brand or customer relationships.

The likelihood of a data breach and the risks involved are so high that the possibility can no longer be ignored – companies must take the initiative to reduce the likelihood of a breach and to reduce the impact of a breach when the inevitable occurs. In addition, it is essential for affected businesses to retain counsel with expertise in rapidly evolving data privacy laws and the ability to effectively handle the litigation onslaught in the aftermath of a data breach, including class actions and regulatory enforcement actions. Although there is no piece of comprehensive federal legislation dictating the nature of security practices companies must adopt, businesses should be aware of the numerous federal statements regarding data security, including Executive Orders,[4] White House policy directives,[5] FTC guidelines,[6] pending regulatory frameworks,[7] and proposed legislation[8] that could be argued to constitute a minimum standard of care. The imminent introduction of new data privacy directives in the European Union also means that companies doing business in Europe should consult counsel with international capabilities.

The following are suggested best practices for companies to follow to anticipate, prevent, and respond to a data breach.

**The authors would like to thank Weil associates Jennifer Ramos and John Stratford for their extensive contributions to this survey.*

back to Table of Contents

Best Practices in Preparing for and Responding to a Data Breach

Before a Data Breach Occurs:

- Anticipate. Catalog all confidential data owned or maintained by the company and ensure that proper security procedures are in place for keeping it safe. Conduct ongoing risk assessments, invest in state-of-the-art security measures, and hire "ethical hackers" to test data security. It is important to understand that most companies are targeted for intrusion because of exploitable security weaknesses, not because of their high profiles or the value of their confidential information.[9] Testing the integrity of the system on a regular basis is a wise investment.
- Train. Inform employees and vendors of proper security procedures and periodically review and update data security policies.
- Organize. Create a response team to implement a plan of action when a breach occurs. The team should be multi-disciplinary and composed of senior management, IT, legal, and public relations personnel. The plan should include procedures for promptly identifying and repairing the breach, investigating the cause of a breach, analyzing the implications of the breach, and notifying the necessary parties.
- Insure. Consider purchasing cyber insurance. Carefully consider the scope of coverage and exclusions under a data breach policy, including whether the policy covers costs related to lawsuits, regulatory investigations, internal investigations, notifications to affected consumers, public relations management, credit monitoring, and/or statutory penalties. A recent study showed that less than a third of companies surveyed had procured data breach insurance, but that companies were increasingly considering this option.[10]

A recent study by Ponemon Institute, LLC estimates that the average cost of a data breach to a U.S. company was $188 per record compromised.

After a Data Breach Occurs:

In the aftermath of a data breach, a company may still be investigating the cause when notification is required by applicable state and federal statutes or when an attorney general investigation begins. As such, it is important for the organization to respond quickly and proactively by assembling its response team and implementing its plan as soon as it learns of the breach.

First, take the necessary steps to secure the system to prevent further data loss, isolate any malware, and repair the breach. The data breach response team should also investigate the cause of the breach, recommend and implement corrective action, and test the integrity of the restored or alternate system.

Next, work with counsel to analyze the legal and regulatory implications of the breach. This requires an understanding of what data has been compromised, whether the data was encrypted or otherwise made inaccessible, the risk that data will be used by third parties, who will be adversely affected, who should be notified and when (including whether notification may be delayed until the integrity of the system is restored), and whether insurance will cover costs related to the breach.

back to Table of Contents

If necessary, work with outside counsel regarding potential obligations to contact law enforcement. While law enforcement or regulatory bodies may commence their own investigations, some state notification statutes require businesses to contact enforcement agencies or delay notification of consumers in the event of a breach.

Additionally, it will likely be necessary to notify the affected parties and implement a public relations plan to mitigate reputational harm. Because a company will likely be required by statute to notify customers or business partners affected by a data breach, an effective public relations plan should include model notice templates and scripts for relaying information about the incident and mitigation steps to the public in a consistent and timely manner. Companies may also consider notifying the public even if they are not legally required to do so in order to avoid subsequent negative publicity. It is important to develop relationships with vendors who have extensive expertise and can help your company anticipate potential issues and formulate best practices for notifying individuals and the public.

Anticipate and prepare for inevitable litigation. A company adversely affected by a data breach may consider filing suit against those responsible for the breach; likewise, customers or business partners affected by the breach may decide to pursue civil remedies against the company or its executives. Securities and consumer class actions are likely, although this area of the law remains unsettled. The constitutional requirement of standing is just one example of the uncertainty in this area: some courts have found that consumers lack standing to sue unless they can show a concrete injury resulting from a data breach, while others have allowed consumer class action suits to go forward after a data breach even where no customer data was actually misused. In addition, state attorneys general may institute claims against companies even where individual and class actions might fail due to lack of standing to sue or failure to identify cognizable harms.

The aftermath of the breach may also include regulatory action. State and federal authorities may launch their own investigations into the causes of the breach, not only to prosecute criminals who may have caused the breach but also for consumer protection. Such investigations could include monetary penalties and required periodic audits lasting decades. The FTC in particular has used its authority under the FTC Act in recent years to assert that a company's failure to take adequate steps to protect consumer information constitutes an unfair trade practice under the Act. For example, after a security breach in 2005 involving 40 million credit card numbers, the FTC prosecuted CardSystems Solutions, Inc. and required it to adopt stricter security measures and conduct an independent audit every other year for the next twenty years. Companies subject to investigations need counsel to work with federal agencies, like the FTC, as well as state agencies in the immediate aftermath of a breach to facilitate investigations and limit potential penalties.

Whether a company will be bringing an action against data thieves or defending against consumer class actions, suits by business partners, or regulatory investigations, it is vital to diligently prepare for litigation and to choose counsel well-versed in data privacy issues.

The likelihood of a data breach and the risks involved are so high that the possibility can no longer be ignored—companies must take the initiative to reduce the likelihood of a breach and to reduce the impact of a breach when the inevitable occurs.

back to Table of Contents

Data Breach Notification Laws

When a data breach occurs, the law may require notification of affected parties or government agencies. Navigating the tangled web of notification statutes is a particular area of concern for companies recovering from a data breach. An assortment of state and federal notification laws may apply in any data breach situation; the following is a brief summary of the federal and state law trends in this area.

Federal Law

Despite pushes for a uniform body of federal laws governing cybersecurity threats and data breaches, there is currently no law providing a uniform set of rules governing data breach notification. Depending on the type of organization and the type of data involved, however, specialized federal laws may apply.

For example, the Gramm-Leach-Bliley Act requires financial institutions to notify customers of a breach, while SEC regulations and the Sarbanes-Oxley Act have been interpreted as imposing certain reporting obligations on publicly traded companies in the wake of a data breach. Other pertinent federal laws relating to cybersecurity may include the FTC Act, the Health Insurance Portability and Accountability Act, the Health Information Technology for Economic and Clinical Health Act, the Controlling the Assault of Non-Solicited Pornography and Marketing Act, and the Children's Online Privacy Protection Act. Companies and counsel must be aware of their potential obligations under these and other federal laws.

State Law

To date, forty-seven states have enacted legislation requiring some form of notification following a data breach. Most are patterned after California's notification statute and thus share many of the same requirements. Generally, the statutes require companies to notify state residents in a timely fashion when the company becomes aware of a loss of unencrypted data containing a state resident's personal information. They also provide an exemption from compliance with the statute where a company maintains its own breach notification policy and the policy is consistent with the requirements of the statute. Some states also call for notification of the state attorney general or consumer reporting agencies, depending on the extent of the breach. If a company fails to comply with the breach notification statute, it may be subject to civil penalties enforced by the attorney general; a minority of state statutes also provide for a private cause of action.

Despite these similarities, variations exist. Some states require consumer notification whenever a breach occurs, while others only require notification if an assessment determines that misuse of the information is likely. Some states permit companies to delay notification pending an investigation to assess the breach and restore the integrity of the data, while others require notification within a certain time period. Even states permitting companies to delay notification for the purposes of investigation have different timing requirements governing when a company must notify consumers after it concludes its investigation. While many states require notice to be provided

back to Table of Contents

"without unreasonable delay," other states are much stricter, for example requiring notice to consumers within 45 days of a breach or requiring notification of the appropriate government agency within 10 days. In responding to a data breach situation, special care and expertise are required to analyze and comply with the patchwork of state laws in this area.

The following pages summarize the data breach notification laws across the United States, the District of Columbia and Puerto Rico. They detail how breach is defined in each jurisdiction and what constitutes personal information. They also specify if and when notification must be provided and possible consequences of non-compliance.

For more information, or for an electronic version of this presentation with active hyperlinks, please contact Christopher J. Cox at chris.cox@weil.com or David R. Singh at david.singh@weil.com.

1. *Chronology of Data Breaches*, Privacy Rights Clearinghouse (accessed April 7, 2014), https://www.privacyrights.org/data-breach/new.
2. *See* Ponemon Institute, LLC, *2013 Cost of Data Breach Study: Global Analysis*.
3. *See* Ross Kerber, *Cost of Data Breach at TJX Soars to $256m*, Boston Globe, Aug. 15, 2007, http://www.boston.com/business/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/?page=full.
4. *See* Exec. Order No. 13636, 78 Fed. Reg. 11,737 (2013).
5. *See* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012), available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf; White House, *Presidential Policy Directive – Critical Infrastructure Security and Resilience* (February 12, 2013), available at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
6. *See generally* FTC, *Data Security*, http://business.ftc.gov/privacy-and-security/data-security; *see also* FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
7. *See* National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
8. *See* Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014); Data Security Act of 2014, S. 1927, 113th Cong. (2014).
9. *See* Verizon, *2012 Data Breach Investigations Report* at 3.
10. *See* Ponemon Institute LLC, *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age*, August 2013.

back to Table of Contents

AK

Statute
Alaska Stat. § 45.48.010 *et seq.*

Definition of Breach

Unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information.

Definition of Personal Information

Unencrypted or unredacted information in any form consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number; or

(C) information that would allow access to financial accounts.

Covered Entities

A person doing business, a governmental agency, or a person with more than ten employees. Judicial branch government agencies are excluded.

Threshold for Notification

If a breach occurs, the covered entity must notify each state resident whose personal information was subject to the breach.

Disclosure is not required if the covered entity determines after investigation and written notification to the Attorney General that there is not a reasonable likelihood of harm to consumers whose personal information has been compromised.

Form of Notification

Notice may be provided by one of the following methods:

(A) by a written document sent to the most recent address the information collector has for the state resident;

(B) by electronic means if the information collector's primary method of communication with the state resident is by electronic means or if making the disclosure by the electronic means is consistent with the provisions regarding electronic records and signatures required for notices legally required to be in writing under 15 U.S.C. 7001 et seq. (Electronic Signatures in Global and National Commerce Act); or

(C) Substitute notice if the information collector demonstrates that the cost of providing notice would exceed $150,000, that the affected class of state residents to be notified exceeds 300,000, or that the information collector does not have sufficient contact information to provide notice.

Substitute notice consists of:

(1) electronic mail if the information collector has an electronic mail address for the state resident;

(2) conspicuously posting the disclosure on the Internet website of the information collector if the information collector maintains an Internet website; and

(3) providing a notice to major statewide media.

Notification Deadline

Notification must be made in the most expeditious time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity of the information system.

Government Agency Notification

If notification of more than 1,000 state residents is required, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.

Consequences of Non-Compliance

A government agency that violates the notification provisions is liable for a civil penalty of up to $500 for each state resident who was not notified, with the total penalty not exceeding $50,000 and injunctive relief against further violations.

For covered entities other than government agencies, the violation is an unfair or deceptive act or practice under AS 45.50.471-45.50.561 and civil penalties apply in the same amounts above. Damages under 45.50.531 are limited to actual economic damages not exceeding $500, and damages under 45.50.537 are limited to actual economic damages.

back to Table of Contents

AZ

Statute
Ariz. Rev. Stat § 44-7501

Definition of Breach

Unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information that causes or is reasonably likely to cause substantial economic loss to an individual.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

An individual's name and either:

(A) social security number;

(B) driver's license or state ID number; or

(C) information that would permit access to financial accounts.

Covered Entities

A person conducting business in Arizona that owns or licenses unencrypted computerized data that includes personal information.

Threshold for Notification

When a person that conducts business in this state and that owns or licenses unencrypted computerized data that includes personal information becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's personal information, the person shall conduct a reasonable investigation to promptly determine if there has been a breach of the security system. If the investigation results in a determination that there has been a breach in the security system, the person shall notify the individuals affected.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (consistent with statute requirements);

(C) Telephonic notice; or

(D) Substitute notice if the person demonstrates that the cost of providing notice pursuant to (1)-(3) of this subsection would exceed $50,000 or that the affected class of subject individuals to be notified exceeds $100,000, or the person does not have sufficient contact information.

Substitute notice consists of:

(1) Electronic mail notice if the person has electronic mail addresses for the individuals subject to the notice;

(2) Conspicuous posting of the notice on the website of the person if the person maintains one; and

(3) Notification to major statewide media.

Notification Deadline

Notification must be made in the most expedient manner possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity of the information system.

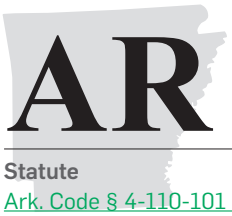
Government Agency Notification

Not required.

Consequences of Non-Compliance

Attorney General may bring an action to obtain actual damages for a willful and knowing violation and civil penalties not to exceed $10,000 per breach or per series of similar breaches uncovered in a single investigation.

back to Table of Contents



Statute
Ark. Code § 4-110-101 *et seq.*

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Unencrypted or unredacted information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number;

(C) information that would permit access to financial accounts; or

(D) medical information.

Covered Entities

A person or business that acquires, owns, or licenses computerized data that includes personal information.

Threshold for Notification

If a breach occurs, the covered entity must notify each state resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Disclosure is not required if the covered entity determines after investigation that there is no reasonable likelihood of harm to customers.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic mail notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001, as it existed on January 1, 2005); or

(C) Substitute notice if the person or business demonstrates that: the cost of providing notice would exceed $250,000; the affected class of persons to be notified exceeds 500,000; or the person or business does not have sufficient contact information.

Substitute notice consists of:

(1) Electronic mail notice when the person or business has an electronic mail address for the subject persons;

(2) Conspicuous posting of the notice on the website of the person or business if the person or business maintains a website; and

(3) Notification by statewide media.

Notification Deadline

Notification must be made in the most expedient manner possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity of the information system.

Government Agency Notification

Not required.

Consequences of Non-Compliance

Enforced by the Attorney General under the provisions of § 4-88-101 *et seq.* (the Deceptive Trade Practices Act).

back to Table of Contents

CA

Statute

Cal. Civ. Code §§ 1798.29 (agencies)
Cal. Civ. Code § 1798.80 et seq. (persons or businesses)
Cal. Civ. Code § 1280.15 (medical information)

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.

Breach does not include good faith acquisition of the information as defined by the statute.

Medical Information Statute: any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information.

Definition of Personal Information

Unencrypted information consisting of either:

(A) an individual's name in combination with

(1) social security number;

(2) driver's license or state ID number;

(3) information that would permit access to financial accounts;

(4) medical information; or

(5) health insurance information; or (effective Jan. 2014)

(B) a user name or email address in combination with a password or security question and answer that would permit access to an online account.

Medical Information Statute: any individually identifiable information, in electronic or physical form, regarding a patient's medical history, mental or physical condition, or treatment.

Covered Entities

Any agency, person, or business that owns or licenses computerized data that includes personal information.

Medical Information Statute: A clinic, health facility, home health agency, or hospice licensed pursuant to Section 1205, 1250, 1725, or 1745.

Threshold for Notification

If a breach occurs, the covered entity must notify each state resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Medical Information Statute: A clinic, health facility, home health agency, or hospice to which subdivision (a) applies shall report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to the department and the patient.

Form of Notification

Agencies, persons, and businesses can provide notice by one of the following methods:

(A) Written notice;

(B) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code); or

(C) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information.

Substitute notice for agencies consists of:

(1) Email notice when the agency has an email address for the subject persons;

(2) Conspicuous posting of the notice on the agency's Internet website page, if the agency maintains one; and

(3) Notification to major statewide media and the Office of Information Security within the California Technology Agency.

Substitute notice for persons or businesses consists of:

(1) Email notice when the person or business has an email address for the subject persons;

(2) Conspicuous posting of the notice on the Internet website page of the person or business, if the person or business maintains one; and

(3) Notification to major statewide media and the Office of Privacy Protection within the State and Consumer Services Agency.

Notification Deadline

Notification must be made in the most expedient time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity of the information system.

Medical Information Statute: notification must be made within five days after detection of the breach, except as necessary for law enforcement purposes.

Government Agency Notification

If notification of more than 500 residents is required, the covered entity must submit a single sample copy of the security breach notification to the Attorney General.

Medical Information Statute: notification must be made to state health authorities.

Consequences of Non-Compliance

Private right of action available to recover damages for violations; entities in violation of this title may also be enjoined.

Agency employees who intentionally violate this chapter will be subject to discipline.

Anyone requesting personal information from an agency under false pretenses is guilty of a misdemeanor resulting in fines and possible imprisonment.

Intentional disclosure of medical, psychiatric, or psychological information in violation of this chapter is guilty of a misdemeanor if it results in economic loss or personal injury to the individual.

Medical Information Statute: administrative penalties up to $25,000 per patient whose medical information was compromised, and up to $17,500 per subsequent occurrence. Delays in notification may be assessed at $100/day for each day of delay, but the total amount of penalties may not exceed $250,000 per reported event.

back to Table of Contents

CO

Statute
Colo. Rev. Stat. § 6-1-716

Definition of Breach

Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Unencrypted, unredacted, or otherwise unsecured information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number; or

(C) information that would allow access to financial accounts.

Covered Entities

An individual or a commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado.

Threshold for Notification

If a breach occurs, the covered entity must notify each state resident whose information was compromised unless a reasonable investigation determines that the misuse of the information has not occurred and is not reasonably likely to occur.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice to the postal address listed in the records of the individual or commercial entity;

(B) Telephonic notice;

(C) Electronic notice (consistent with the requirements of the statute); or

(D) Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $250,000, the affected class of persons to be notified exceeds 250,000 Colorado residents, or the individual or the commercial entity does not have sufficient contact information to provide notice.

Substitute notice consists of:

(1) Email notice if the individual or the commercial entity has email addresses for the members of the affected class of Colorado residents;

(2) Conspicuous posting of the notice on the website page of the individual or the commercial entity if the individual or the commercial entity maintains one; and

(3) Notification to major statewide media.

Notification Deadline

Notice shall be made in the most expedient time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity of the information system.

Government Agency Notification

If notification of more than 1,000 state residents is required, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.

Consequences of Non-Compliance

Attorney may bring an action in law or equity to address violations of this section and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law.

back to Table of Contents

CT

Statute
Conn. Gen. Stat. § 36a-701b
Connecticut Insurance Department Bulletin IC - 25

Definition of Breach

Unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

Definition of Personal Information

Information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number; or

(C) information that would allow access to financial accounts.

Covered Entities

Any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information.

Threshold for Notification

If a breach occurs, the covered entity must notify each state resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Disclosure is not required if the covered entity determines after a reasonable investigation and consultation with law enforcement that the breach will likely not result in harm to the individuals whose information was compromised.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Telephone notice;

(C) Electronic notice (provided such notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001); or

(D) Substitute notice, provided such person demonstrates that the cost of providing notice in accordance with subdivision (A), (B), or (C) of this subsection would exceed $250,000, that the affected class of subject persons to be notified exceeds 500,000 persons or that the person does not have sufficient contact information.

Substitute notice consists of:

(1) Electronic mail notice when the person has an electronic mail address for the affected persons;

(2) conspicuous posting of the notice on the website of the person if the person maintains one; and

(3) notification to major state-wide media, including newspapers, radio and television.

Notification Deadline

Notice shall be made in the most expedient time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity of the information system.

Government Agency Notification

If notice to individuals is required, simultaneous or earlier notice must be made to the Attorney General.

Any entity regulated by the Connecticut Department of Insurance must report any breach within five calendar days of the incident, whether or not the information is encrypted and whether or not the information is in computerized form, pursuant to Bulletin IC - 25.

Consequences of Non-Compliance

Failure to comply with the requirements of this section shall constitute an unfair trade practice for purposes of section 42-110b and shall be enforced by the Attorney General.

The Connecticut Department of Insurance may also impose administrative penalties for entities subject to its regulation.

back to Table of Contents

DE

Statute
Del. Code tit. § 12B-101 *et seq.*

Definition of Breach

Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number; or

(C) information that would allow access to financial accounts.

Covered Entities

An individual or a commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware.

Threshold for Notification

If a breach occurs, the covered entity must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about a Delaware resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Delaware resident.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Telephonic notice;

(C) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 of Title 15 of the United States Code); or

(D) Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $75,000, or that the affected class of Delaware residents to be notified exceeds 100,000 residents, or that the individual or the commercial entity does not have sufficient contact information to provide notice.

Substitute notice consists of:

(1) Email notice if the individual or the commercial entity has email addresses for the members of the affected class of Delaware residents;

(2) Conspicuous posting of the notice on the website page of the individual or the commercial entity if the individual or the commercial entity maintains one; and

(3) Notice to major statewide media.

Notification Deadline

Notice shall be made in the most expedient time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity of the information system.

Government Agency Notification

Not required.

Consequences of Non-Compliance

Attorney General may bring an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both. The provisions of this chapter are not exclusive and do not relieve an individual or a commercial entity subject to this chapter from compliance with all other applicable provisions of law.

back to Table of Contents

FL

Statute
Fla. Stat. § 817.5681

Definition of Breach

Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number; or

(C) information that would allow access to financial accounts.

Covered Entities

Any person who conducts business in this state and maintains computerized data in a system that includes personal information.

Threshold for Notification

If a breach occurs, the covered entity must notify each state resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Disclosure is not required if the covered entity determines after a reasonable investigation or consultation with law enforcement that the breach will likely not result in harm to the individuals whose information was compromised.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. s. 7001 or if the person or business providing the notice has a valid email address for the subject person and the subject person has agreed to accept communications electronically; or

(C) Substitute notice, if the person demonstrates that the cost of providing notice would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000, or the person does not have sufficient contact information.

Substitute notice consists of:

(1) Electronic mail or email notice when the person has an electronic mail or email address for the subject persons;

(2) Conspicuous posting of the notice on the web page of the person, if the person maintains a web page; and

(3) Notification to major statewide media.

Notification Deadline

Notice shall be made without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity of the information system. Notification must be made no later than 45 days following the determination of the breach unless otherwise provided in this section.

Government Agency Notification

If notification of more than 1,000 state residents is required, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.

Consequences of Non-Compliance

Any person required to make notification who fails to do so within 45 days following the determination of a breach or receipt of notice from law enforcement is liable for an administrative fine not to exceed $500,000 in the amount of $1,000 for each day the breach goes undisclosed for up to 30 days and $50,000 for each 30-day period thereafter for up to 180 days per breach.

back to Table of Contents

GA

Statute
Ga. Code §§ 10-1-910, -911, -912

Definition of Breach

Unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of personal information.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Unencrypted, unredacted, or otherwise unsecured information consisting of an individual's name and either

(A) social security number;

(B) driver's license or state ID number;

(C) information that would allow access to financial accounts;

(D) account passwords or personal identification numbers or other access codes; or

(E) any of the above when not in connection with an individual's name if the information compromised would be sufficient to perform or attempt to perform identity theft against the individual.

Covered Entities

Any information broker or data collector that maintains computerized data that includes personal information of individuals.

Threshold for Notification

If a breach occurs, the covered entity must notify each state resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Telephone notice;

(C) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code); or

(D) Substitute notice, if the information broker or data collector demonstrates that the cost of providing notice would exceed $50,000.00, that the affected class of individuals to be notified exceeds 100,000, or that the information broker or data collector does not have sufficient contact information to provide written or electronic notice to such individuals.

Substitute notice consists of:

(1) Email notice, if the information broker or data collector has an email address for the individuals to be notified;

(2) Conspicuous posting of the notice on the information broker's or data collector's website page, if the information broker or data collector maintains one; and

(3) Notification to major state-wide media.

Notification Deadline

The notice shall be made in the most expedient time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity, security, and confidentiality of the information system.

Government Agency Notification

If notification of more than 1,000 state residents is required, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.

Consequences of Non-Compliance

n/a

back to Table of Contents

HI

Statute
Haw. Rev. Stat. § 487N-1 *et seq.*

Definition of Breach

Unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Unencrypted information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number; or

(C) information that would permit access to financial accounts.

Covered Entities

Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes.

Threshold for Notification

If a breach occurs, the covered entity must notify each affected state resident following discovery or notification of the breach.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic mail notice (consistent with the regulation);

(C) Telephonic notice, provided that contact is made directly with the affected persons; or

(D) Substitute notice, if the business or government agency demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of subject persons to be notified exceeds 200,000, or if the business or government agency does not have sufficient contact information or consent to satisfy paragraph (A), (B), or (C), for only those affected persons without sufficient contact information or consent, or if the business or government agency is unable to identify particular affected persons, for only those unidentifiable affected persons.

Substitute notice consists of:

(1) Electronic mail notice when the business or government agency has an electronic mail address for the subject persons;

(2) Conspicuous posting of the notice on the website page of the business or government agency, if one is maintained; and

(3) Notification to major statewide media.

Notification Deadline

The notice shall be made in the most expedient time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity, security, and confidentiality of the information system.

Government Agency Notification

If notification of more than 1,000 state residents is required, the State of Hawaii office of consumer protection and all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.

A government agency shall submit a written report to the legislature within 20 days after discovery of a security breach at the government agency that details information relating to the nature of the breach, the number of individuals affected by the breach, a copy of the notice of security breach that was issued, the number of individuals to whom the notice was sent, whether the notice was delayed due to law enforcement considerations, and any procedures that have been implemented to prevent the breach from reoccurring. In the event that a law enforcement agency informs the government agency that notification may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until 20 days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security.

Consequences of Non-Compliance

Civil penalties of not more than $2,500 for each violation. The Attorney General or the executive director of the office of consumer protection may bring an action pursuant to this section. No such action may be brought against a government agency.

Private right of action available to recover an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation. The court in any action brought under this section may award reasonable attorneys' fees to the prevailing party. No such action may be brought against a government agency.

back to Table of Contents

ID

Statute
Idaho Stat. §§ 28-51-104 to -107

Definition of Breach

Illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an agency, individual or a commercial entity.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Unencrypted information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number; or

(C) information that would permit access to financial accounts.

Covered Entities

A city, county or state agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho.

Threshold for Notification

If a breach occurs, the covered entity must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident.

Form of Notification

Notice may be provided by one of the following methods:

(1) Written notice;

(2) Telephonic notice;

(3) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. section 7001); or

(4) Substitute notice, if the agency, individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $25,000, or that the number of Idaho residents to be notified exceeds 50,000, or that the agency, individual or the commercial entity does not have sufficient contact information to provide notice.

Substitute notice consists of:

(1) Email notice if the agency, individual or the commercial entity has email addresses for the affected Idaho residents;

(2) Conspicuous posting of the notice on the website page of the agency, individual or the commercial entity if the agency, individual or the commercial entity maintains one; and

(3) Notice to major statewide media.

Notification Deadline

Notice shall be made in the most expedient time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity of the information system.

Government Agency Notification

When an agency becomes aware of a breach of the security of the system, it shall, within twenty-four (24) hours of such discovery, notify the office of the Idaho Attorney General. Nothing contained herein relieves a state agency's responsibility to report a security breach to the office of the chief information officer within the department of administration, pursuant to the information technology resource management council policies.

Consequences of Non-Compliance

The primary regulator may bring a civil action to enjoin an agency, individual or commercial entity from further violations.

Any agency, individual or commercial entity that intentionally fails to give notice shall be subject to a fine of not more than twenty-five thousand dollars ($25,000) per breach of the security of the system.

back to Table of Contents

IL

Statute
815 ILCS §§ 530/1 to 530/25

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Unencrypted or unredacted information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number; or

(C) information that would permit access to financial accounts.

Covered Entities

Any data collector or state agency that owns or licenses personal information concerning an Illinois resident.

Threshold for Notification

If a breach occurs, the covered entity must notify each affected state resident at no charge following discovery or notification of the breach.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code); or

(C) Substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information.

Substitute notice consists of:

(1) email notice if the data collector has an email address for the subject persons;

(2) conspicuous posting of the notice on the data collector's website page if the data collector maintains one; and

(3) notification to major statewide media.

Notification Deadline

The notice shall be made in the most expedient time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity, security, and confidentiality of the information system.

Government Agency Notification

If notification of more than 1,000 state residents is required, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.

Any State agency that collects personal data and has had a breach of security of the system data or written material shall submit a report within 5 business days of the discovery or notification of the breach to the General Assembly listing the breaches and outlining any corrective measures that have been taken to prevent future breaches of the security of the system data or written material. Any State agency that has submitted a report under this Section shall submit an annual report listing all breaches of security of the system data or written materials and the corrective measures that have been taken to prevent future breaches.

Consequences of Non-Compliance

A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.

back to Table of Contents

IN

Statute
Ind. Code §§ 4-1-11 *et seq.*, 24-4.9 *et seq.*

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

State agencies--Information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number; or

(C) information that would allow access to financial accounts.

Person or Business--a social security number that is not encrypted or redacted; or unencrypted or unredacted information consisting of an individual's name and either:

(A) driver's license;

(B) state ID number; or

(C) information that would permit access to financial accounts.

Covered Entities

Any person or state agency that owns or licenses computerized data that includes personal information.

Threshold for Notification

State Agency:

Any state agency that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system following discovery or notification of the breach to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

Person or Business:

After discovering or being notified of a breach of the security of data, the database owner shall disclose the breach to an Indiana resident whose:

(A) unencrypted personal information was or may have been acquired by an unauthorized person; or

(B) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key; if the database owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident.

Form of Notification

Notice by a state agency can be provided either:

(A) in writing;

(B) by electronic mail, if the individual has provided the state agency with the individual's electronic mail address; or

(C) substitute notice if the cost of providing the notice required is at least $250,000; the number of persons to be notified is at least 500,000; or the agency does not have sufficient contact information.

Substitute notice for a state agency would consist of:

(1) Conspicuous posting of the notice on the state agency's website if the state agency maintains a website; and

(2) Notification to major statewide media.

Notice by a person or business can be provided by either:

(A) Mail;

(B) Telephone;

(C) Facsimile (fax);

(D) Electronic mail, if the database owner has the electronic mail address of the affected Indiana resident; or

(E) Substitute notice if required to make the disclosure to more than 500,000 Indiana residents, or if the database owner required to make a disclosure under this chapter determines that the cost of the disclosure will be more than $250,000.

Substitute notice for a person or business would consist of:

(1) Conspicuous posting of the notice on the website of the database owner, if the database owner maintains a website; and

(2) Notice to major news reporting media in the geographic area where Indiana residents affected by the breach of the security of a system reside.

Notification Deadline

The notice shall be made without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity, security, and confidentiality of the information system.

Government Agency Notification

Database owners who must notify residents must also notify the Attorney General.

If notification of more than 1,000 state residents is required, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.

Consequences of Non-Compliance

Person or Business:

Attorney General may bring an action to obtain any or all of the following:

(A) An injunction to enjoin future violations;

(B) A civil penalty of not more than one hundred fifty thousand dollars ($150,000) per deceptive act;

(C) The Attorney General's reasonable costs in the investigation of the deceptive act and maintaining the action.

back to Table of Contents

IA

Statute
Iowa Code § 715C.1, 715C.2

Definition of Breach

Unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Unencrypted, unredacted, or otherwise unsecured information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number;

(C) information that would allow access to financial accounts; or

(D) unique biometric data, such as a fingerprint, retina or iris image, or other unique representation of biometric data.

Covered Entities

Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities.

Threshold for Notification

If a breach occurs, the covered entity must notify each affected state resident following discovery or notification of the breach. Notification is not required if, after appropriate investigation or after consultation with law enforcement, it is determined that there is no reasonable likelihood of financial harm to consumers affected by the breach.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (consistent with the requirements of the statute); or

(C) Substitute notice, if the person demonstrates that the cost of providing notice would exceed $250,000, that the affected class of consumers to be notified exceeds 350,000 persons, or if the person does not have sufficient contact information to provide notice.

Substitute notice consists of:

(1) Electronic mail notice when the person has an electronic mail address for the affected consumers;

(2) Conspicuous posting of the notice or a link to the notice on the Internet website of the person if the person maintains an Internet website; and

(3) Notification to major statewide media.

Notification Deadline

The notice shall be made without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity, security, and confidentiality of the information system.

Government Agency Notification

Not required.

Consequences of Non-Compliance

Attorney General may bring an action for injunctive relief, civil penalties, and damages on behalf of a person injured by the violation.

The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under the law.

back to Table of Contents

KS

Statute
Kan. Stat. 50-7a01 *et seq.*

Definition of Breach

Unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Unencrypted or unredacted information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number; or

(C) information that would permit access to financial accounts.

Covered Entities

A person that conducts business in this state, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information.

Threshold for Notification

If a breach occurs, the covered entity shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information has occurred or is reasonably likely to occur, the person or government, governmental subdivision or agency shall give notice as soon as possible to the affected Kansas resident.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001); or

(C) Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $100,000, or that the affected class of consumers to be notified exceeds 5,000, or that the individual or the commercial entity does not have sufficient contact information to provide notice.

Substitute notice consists of:

(1) E-mail notice if the individual or the commercial entity has e-mail addresses for the affected class of consumers;

(2) conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains a web site; and

(3) notification to major statewide media.

Notification Deadline

The notice shall be made without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the reasonable integrity of the information system.

Government Agency Notification

If notification of more than 1,000 state residents is required, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.

Consequences of Non-Compliance

For violations of this section, except as to insurance companies licensed to do business in this state, the Attorney General is empowered to bring an action in law or equity to address violations of this section and for other relief that may be appropriate. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law.

For violations of this section by an insurance company licensed to do business in this state, the insurance commissioner shall have the sole authority to enforce the provisions of this section.

back to Table of Contents

KY

Statute
H.B. 232 (2014)

Definition of Breach

Unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the covered entity as part of a database regarding multiple individuals that actually causes, or leads the covered entity to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Unredacted information consisting of an Individual's first name or first initial and last name in combination with any one or more of the following data elements:

(A) Social Security number;

(B) Driver's license number; or

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password permit access to an individual's financial account.

Covered Entities

A person or business entity that conducts business in the state. State agencies or entities working with them may also be covered and follow different requirements under H.B. 5 (2014).

Threshold for Notification

If a breach occurs, the covered entity shall disclose any breach of the security of the system to any resident of Kentucky whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notification;

(B) Electronic notification (if the notification provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001); or

(C) Substitute notification, if an agency or person demonstrates that the cost of providing notification would exceed two hundred fifty thousand dollars, or that the affected class of persons to be notified exceeds five hundred thousand, or the agency or person does not have sufficient contact information.

Substitute notice shall consist of all of the following:

(1) E-mail notification when the agency or person has an e-mail address for the subject persons;

(2) Conspicuous posting of the notification on the Internet site of the agency or person, if an Internet site is maintained; and

(3) Notification to major statewide media.

Notification Deadline

The notice shall be made in the most expedient time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the reasonable integrity of the information system.

Government Agency Notification

If notification of more than 1,000 persons is required, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.

Consequences of Non-Compliance

n/a

back to Table of Contents

LA

Statute
La. Rev. Stat. § 51:3071 *et seq.*

Definition of Breach

The compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by an agency or person.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Unencrypted or unredacted information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number; or

(C) information that would permit access to financial accounts.

Covered Entities

Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information.

Threshold for Notification

If a breach occurs, the covered entity shall notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notification is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notification;

(B) Electronic notification (if the notification provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001); or

(C) Substitute notification, if an agency or person demonstrates that the cost of providing notification would exceed $250,000, or that the affected class of persons to be notified exceeds 500,000, or the agency or person does not have sufficient contact information.

Substitute notice consists of:

(1) Email notification when the agency or person has an email address for the subject persons;

(2) Conspicuous posting of the notification on the Internet site of the agency or person, if an Internet site is maintained; and

(3) Notification to major statewide media.

Notification Deadline

The notice shall be made without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the information system.

Government Agency Notification

When notice to Louisiana citizens is required pursuant to R.S. 51:3074, the person or agency shall provide written notice detailing the breach of the security of the system to the Consumer Protection Section of the Attorney General's Office. Notice shall include the names of all Louisiana citizens affected by the breach.

Failure to provide timely notice may be punishable by a fine not to exceed $5,000 per violation. Notice to the Attorney General shall be timely if received within 10 days of distribution of notice to Louisiana citizens. Each day notice is not received by the Attorney General shall be deemed a separate violation.

Consequences of Non-Compliance

A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information.

back to Table of Contents

ME

Statute
Me. Rev. Stat. tit. 10 § 1347 *et seq.*

Definition of Breach

Unauthorized acquisition, release or use of an individual's computerized data that includes personal information that compromises the security, confidentiality or integrity of personal information of the individual maintained by a person.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Unencrypted or unredacted information consisting of an individual's name and either:

(A) social security number;

(B) driver's license or state ID number;

(C) information that would permit access to financial accounts; or

(D) any of the above information without an accompanying name if the information would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

Covered Entities

Information brokers and other persons.

"Information broker" means a person who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated 3rd parties. "Information broker" does not include a governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes.

"Person" means an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity, including agencies of State Government, the University of Maine System, the Maine Community College System, Maine Maritime Academy and private colleges and universities. "Person" as used in this chapter may not be construed to require duplicative notice by more than one individual, corporation, trust, estate, cooperative, association or other entity involved in the same transaction.

Threshold for Notification

If an information broker that maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the information broker shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person.

If any other person who maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the person shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 United States Code, Section 7001); or

(C) Substitute notice, if the person maintaining personal information demonstrates that the cost of providing notice would exceed $5,000, that the affected class of individuals to be notified exceeds 1,000 or that the person maintaining personal information does not have sufficient contact information to provide written or electronic notice to those individuals.

Substitute notice consists of:

(1) Email notice, if the person has email addresses for the individuals to be notified;

(2) Conspicuous posting of the notice on the person's publicly accessible website, if the person maintains one; and

(3) Notification to major statewide media.

Notification Deadline

The notice shall be made as expediently as possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity, security, and confidentiality of the information system.

If, after the completion of an investigation, notification is required, the notification required by this section may be delayed for no longer than 7 business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.

Government Agency Notification

If notification of more than 1,000 state residents is required, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.

When notice of a breach of the security of the system is required, the person shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the Attorney General.

Consequences of Non-Compliance

The appropriate state regulators within the Department of Professional and Financial Regulation shall enforce this chapter for any person that is licensed or regulated by those regulators. The Attorney General shall enforce this chapter for all other persons.

A person that violates this chapter commits a civil violation and is subject to one or more of the following:

A fine of not more than $500 per violation, up to a maximum of $2,500 for each day the person is in violation of this chapter, except that this paragraph does not apply to State Government, the University of Maine System, the Maine Community College System or Maine Maritime Academy; equitable relief; or enjoinment from further violations of this chapter.

back to Table of Contents

Statute
Md. Code Com. Law § 14-3501 *et seq.*

Definition of Breach

The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable:

(A) A social security number;

(B) A driver's license number;

(C) A financial account number, including a credit card number or debit card number, that in combination with any required security code, access code, or password, would permit access to an individual's financial account; or

(D) An Individual Taxpayer Identification Number.

Covered Entities

A business that owns or licenses computerized data that includes personal information of an individual residing in the State.

Threshold for Notification

A business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach.

If, after the investigation is concluded, the business determines that misuse of the individual's personal information has occurred or is reasonably likely to occur as a result of a breach of the security of a system, the business shall notify the individual of the breach.

Form of Notification

Notice may be provided by one of the following methods:

(A) By written notice;

(B) By electronic mail (if consistent with the requirements of the statute);

(C) By telephonic notice; or

(D) By substitute notice if: the business demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of individuals to be notified exceeds 175,000; or the business does not have sufficient contact information to give notice in accordance with item (A), (B), or (C) of this subsection.

Substitute notice consists of:

(1) Electronically mailing the notice to an individual entitled to notification under subsection (B) above, if the business has an electronic mail address for the individual to be notified;

(2) Conspicuous posting of the notice on the website of the business, if the business maintains a website; and

(3) Notification to statewide media.

Notification Deadline

The notice shall be made as soon as reasonably practicable after the required investigation, except as necessary for law enforcement purposes or to determine the scope of the breach, identify the individuals affected, or restore the integrity of the system.

Government Agency Notification

Prior to giving the notification required under subsection (b) of this section and subject to subsection (d) of this section, a business shall provide notice of a breach of the security of a system to the Office of the Attorney General.

If notification of more than 1,000 state residents is required, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.

Consequences of Non-Compliance

A violation of this subtitle:

(A) Is an unfair or deceptive trade practice within the meaning of Title 13 of this article;

(B) Is subject to the enforcement and penalty provisions contained in Title 13 of this article.

back to Table of Contents

Statute
Mass. Gen. Laws § 93H-1 *et seq.*

Definition of Breach

The unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

A resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:

(A) social security number;

(B) driver's license number or state-issued identification card number; or

(C) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Covered Entities

A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth.

Threshold for Notification

A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the Attorney General, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (if notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 (c) of Title 15 of the United States Code; and chapter 110G); or

(C) Substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed $250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice.

Substitute notice consists of:

(1) Electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents;

(2) Clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and

(3) Publication in or broadcast through media or medium that provides notice throughout the commonwealth.

Notification Deadline

The notice shall be made as soon as practicable and without unreasonable delay, except as necessary for law enforcement purposes.

Government Agency Notification

The Attorney General and the director of consumer affairs and business regulation must be notified.

Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation.

Consequences of Non-Compliance

The Attorney General may bring an action pursuant to section 4 of chapter 93A for injunctive relief and civil penalties against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

back to Table of Contents

MI

Statute
Mich. Comp. Laws §§ 445.63, 445.72

Definition of Breach

The unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

The first name or first initial and last name linked to one or more of the following data elements of a resident of this state:

(A) social security number;

(B) driver's license number or state personal identification card number; or

(C) demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.

Covered Entities

A person or agency that owns or licenses data that are included in a database.

Threshold for Notification

Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach under subsection (2), shall provide a notice of the security breach to each resident of this state who meets one or more of the following:

(A) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person; or

(B) That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Written notice sent electronically (consistent with the requirements of the statute);

(C) Telephonic notice (consistent with the requirements of the statute); or

(D) Substitute notice, if the person or agency demonstrates that the cost of providing notice under (1)-(3) will exceed $250,000.00 or that the person or agency has to provide notice to more than 500,000 residents of this state.

Substitute notice consists of:

(1) If the person or agency has electronic mail addresses for any of the residents of this state who are entitled to receive the notice, providing electronic notice to those residents;

(2) If the person or agency maintains a website, conspicuously posting the notice on that website; and

(3) Notifying major statewide media. A notification under this subparagraph shall include a telephone number or a website address that a person may use to obtain additional assistance and information.

Notification Deadline

The notice shall be made without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the security breach and restore the reasonable integrity of the database.

Government Agency Notification

If notification of more than 1,000 state residents is required, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay. This does not apply if the person or agency is subject to the Gramm-Leach-Bliley Act.

Consequences of Non-Compliance

A person that knowingly fails to provide any notice of a security breach required under this section may be ordered to pay a civil fine of not more than $250.00 for each failure to provide notice. The Attorney General or a prosecuting attorney may bring an action to recover a civil fine under this section.

The aggregate liability of a person for civil fines for multiple violations that arise from the same security breach shall not exceed $750,000.00.

The above does not affect the availability of any civil remedy for a violation of state or federal law.

back to Table of Contents

MN

Statute
Minn. Stat. §§ 325E.61, 325E.64

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:

(A) social security number;

(B) driver's license number or Minnesota identification card number; or

(C) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Covered Entities

Any person or business that conducts business in this state, and that owns or licenses data that includes personal information.

Threshold for Notification

Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice to the most recent available address the person or business has in its records;

(B) Electronic notice (consistent with the requirements of the statute); or

(C) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information.

Substitute notice consists of:

(1) Email notice when the person or business has an email address for the subject persons;

(2) Conspicuous posting of the notice on the website page of the person or business, if the person or business maintains one; and

(3) Notification to major statewide media.

Notification Deadline

The notice must be made in the most expedient time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.

Government Agency Notification

If notification of more than 500 state residents is required, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified within 48 hours.

Consequences of Non-Compliance

Attorney General enforcement.

Where a breach involves unlawful retention of payment card information under §325E.64, the covered entity must reimburse the financial institution that issued any payment card for related costs according to that section.

back to Table of Contents

MS

Statute
Miss. Code. § 75-24-29

Definition of Breach

Unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following data elements:

(A) social security number;

(B) driver's license number or state identification card number; or

(C) an account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

Covered Entities

A person who conducts business in this state.

Threshold for Notification

A person who conducts business in this state shall disclose any breach of security to all affected individuals. The disclosure shall be made without unreasonable delay, subject to the provisions of subsections (4) and (5) of this section and the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the data system. Notification shall not be required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Telephone notice;

(C) Electronic notice (consistent with the requirements of the statute); or

(D) Substitute notice, provided the person demonstrates that the cost of providing notice in accordance with options (A)-(C) would exceed $5,000, that the affected class of subject persons to be notified exceeds 5,000 individuals or the person does not have sufficient contact information.

Substitute notice consists of:

(1) Electronic mail notice when the person has an electronic mail address for the affected individuals;

(2) Conspicuous posting of the notice on the website of the person if the person maintains one; and

(3) Notification to major statewide media, including newspapers, radio and television.

Notification Deadline

The notice must be made without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.

Government Agency Notification

Not required.

Consequences of Non-Compliance

Failure to comply with the requirements of this section shall constitute an unfair trade practice and shall be enforced by the Attorney General; however, nothing in this section may be construed to create a private right of action.

back to Table of Contents

MO

Statute
Mo. Rev. Stat. § 407.1500

Definition of Breach

Unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable:

(A) social security number;

(B) driver's license number or other unique identification number created or collected by a government body;

(C) financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;

(D) 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;

(E) medical information; or

(F) health insurance information.

Covered Entities

Any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri.

Threshold for Notification

Any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri shall provide notice to the affected consumer that there has been a breach of security following discovery or notification of the breach.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (consistent with the requirements of the statute);

(C) Telephonic notice, if such contact is made directly with the affected consumers; or

(D) Substitute notice, if: the person demonstrates that the cost of providing notice would exceed $100,000; or the class of affected consumers to be notified exceeds 150,000; or the person does not have sufficient contact information or consent to satisfy paragraphs (A)-(D) of this subdivision, for only those affected consumers without sufficient contact information or consent; or the person is unable to identify particular affected consumers, for only those unidentifiable consumers.

Substitute notice consists of:

(1) Email notice when the person has an electronic mail address for the affected consumer;

(2) Conspicuous posting of the notice or a link to the notice on the Internet website of the person if the person maintains an Internet website; and

(3) Notification to major statewide media.

Notification Deadline

The notice must be made without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Government Agency Notification

If notification of more than 1,000 state residents is required, the Attorney General's office and all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.

Consequences of Non-Compliance

The Attorney General shall have exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section and may seek a civil penalty not to exceed $150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

back to Table of Contents

MT

Statute

Mont. Code §§ 2-6-504 (state agencies)
30-14-1701 *et seq.* (businesses)

Definition of Breach

Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business or state agency or third party on behalf of the state agency and causes or is reasonably believed to cause loss or injury to a Montana resident.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted, and the information is not otherwise publicly available:

(A) social security number;

(B) driver's license number, state identification card number, or tribal identification card number (for state agencies, also includes identification numbers issued by other states); or

(C) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Covered Entities

A state agency that maintains computerized data containing personal information in the data system.

Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information.

Threshold for Notification

Upon discovery or notification of a breach of the security of a data system, a state agency that maintains computerized data containing personal information in the data system shall make reasonable efforts to notify any person whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001);

(C) Telephonic notice; or

(D) Substitute notice, if the person or business demonstrates that: the cost of providing notice would exceed $250,000; the affected class of subject persons to be notified exceeds 500,000; or the person or business does not have sufficient contact information.

Substitute notice consists of:

(1) An electronic mail notice when the person or business has an electronic mail address for the subject persons; and

(2) Conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; or

(3) Notification to applicable local or statewide media.

Notification Deadline

The notice must be made without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the reasonable integrity of the data system.

Government Agency Notification

If a business discloses a security breach to any individual pursuant to this section and gives a notice to the individual that suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual. The coordination may not unreasonably delay the notice to the affected individuals.

Consequences of Non-Compliance

Department may bring an action in the name of the state for violations; remedies include injunctive relief and civil fines as provided in 30-14-142.

back to Table of Contents

NE

Statute

Neb. Rev. Stat. § 87-801 *et seq.*

Definition of Breach

Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.

Breach does not include good faith acquisition of the information as defined by the statute or acquisition of the information pursuant to a search warrant, court order, etc.

Definition of Personal Information

Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable, and the information is not otherwise publicly available:

(A) social security number;

(B) motor vehicle operator's license number or state identification card number;

(C) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account;

(D) unique electronic identification number or routing code, in combination with any required security code, access code, or password; or

(E) unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation.

Covered Entities

An individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a Nebraska resident.

Threshold for Notification

After breach, must conduct in good faith a reasonable and prompt investigation. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Telephonic notice;

(C) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001, as such section existed on January 1, 2006); or

(D) Substitute notice, if the individual or commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $75,000, that the affected class of Nebraska residents to be notified exceeds 100,000 residents, or that the individual or commercial entity does not have sufficient contact information to provide notice.

Substitute notice consists of:

(1) Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents;

(2) Conspicuous posting of the notice on the website of the individual or commercial entity if the individual or commercial entity maintains a website; and

(3) Notice to major statewide media outlets.

But: if the individual or commercial entity required to provide notice has ten employees or fewer and demonstrates that the cost of providing notice will exceed $10,000, substitute notice under this subdivision requires all of the following:

(a) Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents;

(b) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the individual or commercial entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;

(c) Conspicuous posting of the notice on the website of the individual or commercial entity if the individual or commercial entity maintains a website; and

(d) Notification to major media outlets in the geographic area in which the individual or commercial entity is located.

Notification Deadline

Notice shall be made as soon as possible and without unreasonable delay, 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 required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.

Government Agency Notification

Not required.

Consequences of Non-Compliance

Attorney General enforcement.

Waiver of provisions of law is not permitted as contrary to public policy and is void and unenforceable.

back to Table of Contents

NV

Statute
Nev. Rev. Stat. Ann. §603A.020 *et seq.*

Definition of Breach

Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:

(A) social security number;

(B) driver's license number or identification card number; or

(C) account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.

The term does not include the last four digits of a social security number, the last four digits of a driver's license number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public.

Covered Entities

Any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information that owns or licenses such computerized data.

Threshold for Notification

Must provide notice to any resident of Nevada whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notification;

(B) Electronic notification (if the notification provided is consistent with the provisions of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq.); or

(C) Substitute notification, if the data collector demonstrates that the cost of providing notification would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000 or the data collector does not have sufficient contact information.

Substitute notification must consist of all the following:

(1) Notification by Electronic mail when the data collector has electronic mail addresses for the subject persons;

(2) Conspicuous posting of the notification on the Internet website of the data collector, if the data collector maintains an Internet website; and

(3) Notification to major statewide media.

Notification Deadline

The disclosure must 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 system data.

Notice may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification must be made after the law enforcement agency determines that the notification will not compromise the investigation.

Government Agency Notification

Not required.

Consequences of Non-Compliance

Waiver of provisions of law is not permitted as contrary to public policy and is void and unenforceable.

back to Table of Contents

NH

Statute
N.H. Rev. Stat. Ann. § 359-C:19, C:20, C:21

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

First name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted, and the information is not otherwise publicly available:

(A) social security number;

(B) driver's license number or other government identification number; or

(C) account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Covered Entities

Individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state.

Threshold for Notification

An entity, when it becomes aware of a security breach, must promptly determine the likelihood that the information has been or will be misused. Must provide notification to the affected individuals if the determination after an investigation is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made.

Form of Notification

Notice must include: a description of the incident in general terms; the approximate date of breach; the type of personal information obtained as a result of the security breach; and the telephonic contact information of the person subject to this section.

Notification to government must include the anticipated date of the notice to the individuals and the approximate number of individuals in New Hampshire who will be notified.

Notice must be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (if the agency or business' primary means of communication with affected individuals is by electronic means);

(C) Telephonic notice (provided that a log of each such notification is kept by the person or business who notifies affected persons);

(D) Substitute notice, if the person demonstrates that the cost of providing notice would exceed $5,000, that the affected class of subject individuals to be notified exceeds 1,000, or the person does not have sufficient contact information or consent to provide notice pursuant to options (A)-(C); or

(E) Notice pursuant to the person's internal notification procedures maintained as part of an information security policy for the treatment of personal information.

Substitute notice shall consist of all of the following:

(1) Email notice when the person has an email address for the affected individuals;

(2) Conspicuous posting of the notice on the person's business website, if the person maintains one; and

(3) Notification to major statewide media.

Notification Deadline

As soon as possible.

Notification may be delayed if a law enforcement agency or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security.

Government Agency Notification

(A) Attorney General's Office; or

(B) the regulator which has primary regulatory authority over such trade or commerce.

Consumer reporting agency notification if required to notify more than 1,000 people.

Consequences of Non-Compliance

(A) personal right of action, with treble damages available for willful or knowing violations of this law;

(B) Attorney General enforcement;

(C) waiver of right to damages is void and unenforceable.

back to Table of Contents

NJ

Statute
N.J. Rev. Stat. §§ 56:8-161, 56:8-163

Definition of Breach

Unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

First name or first initial and last name linked with any one or more of the following data elements, but excluding information lawfully made available to the public:

(A) social security number;

(B) driver's license number or State identification card number; or

(C) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Covered Entities

Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information.

Public entity includes the State, and any county, municipality, district, public authority, public agency, and any other political subdivision or public body in the State. Public entity does not include the federal government.

Threshold for Notification

Must disclose breach to New Jersey resident whose information was, or is reasonably believed to have been, accessed by an unauthorized person.

Disclosure is not required if the business or public entity establishes that misuse of the information is not reasonably possible.

Any determination shall be documented in writing and retained for five years.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 101 of the federal "Electronic Signatures in Global and National Commerce Act" 15 U.S.C. § 7001); or

(C) Substitute notice, if the business or public entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the business or public entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

(1) Email notice when the business or public entity has an email address;

(2) Conspicuous posting of the notice on the Internet website page of the business or public entity, if the business or public entity maintains one; and

(3) Notification to major statewide media.

Notification Deadline

Disclosure must 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.

Notice may be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.

Government Agency Notification

Must notify the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

Consumer reporting agency notification if required to notify more than 1,000 people.

Consequences of Non-Compliance

n/a

back to Table of Contents

NY

Statute
N.Y. Gen. Bus. Law § 899-aa
N.Y. State Tech. Law § 208

Definition of Breach

Unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired, and the information is not otherwise lawfully publicly available:

(A) social security number;

(B) driver's license number or non-driver identification card number; or

(C) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Covered Entities

State entities and any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information. State entities are also required to notify non-New York residents. State entities do not include: the judiciary, and all cities, counties, municipalities, villages, towns, and other local agencies.

Threshold for Notification

Must notify of any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

Form of Notification

Content of notice must include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (subject to certain restrictions);

(C) Telephone notification (provided that a log of each such notification is kept by the person or business who notifies affected persons); or

(D) Substitute notice, if a business demonstrates to the state Attorney General that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or such business does not have sufficient contact information.

Substitute notice consists of:

(1) email notice when such business has an email address for the subject persons;

(2) conspicuous posting of the notice on such business's website page, if such business maintains one; and

(3) notification to major statewide media.

Notification Deadline

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 system.

Notice may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

Government Agency Notification

(A) Attorney General;

(B) Department of State;

(C) Division of State Police; and

(D) Consumer Reporting Agencies (if notice to more than 5,000 NY residents). Must complete specific form.

http://www.dhses.ny.gov/ocs/breach-notification/

Consequences of Non-Compliance

(A) Attorney General enforcement;

(B) fine of up to $150,000 for knowing or reckless violation of breach notification law;

(C) cost of damages to person to whom notice should have been given.

back to Table of Contents

Statute
N.C. Gen. Stat. § 75-60 *et seq.*

Definition of Breach

An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

First name or first initial and last name in combination with identifying information, not otherwise publicly available, such as:

(A) Social security or employer taxpayer identification numbers;

(B) driver's license, State identification card, or passport numbers;

(C) checking account numbers;

(D) savings account numbers;

(E) credit card numbers;

(F) debit card numbers;

(G) Personal Identification (PIN) Code;

(H) electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names;

(I) digital signatures;

(J) any other numbers or information that can be used to access a person's financial resources;

(K) biometric data;

(L) fingerprints;

(M) passwords; or

(N) parent's legal surname prior to marriage.

Covered Entities

Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise).

Threshold for Notification

Must provide notice if there has been a security breach.

If the breach contains personal information consisting of electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password, notification does not need to be provided unless access to this information would permit access to a person's financial account or resources.

Form of Notification

Notice must include:

(A) a description of the incident in general terms;

(B) a description of the type of personal information that was subject to the unauthorized access and acquisition;

(C) a description of the general acts of the business to protect the personal information from further unauthorized access;

(D) a telephone number for the business that the person may call for further information and assistance, if one exists;

(E) advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports;

(F) the toll-free numbers and addresses for the major consumer reporting agencies; and

(G) the toll-free numbers, addresses, and website addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

Notice may be provided by one of the following methods:

(1) Written notice;

(2) Electronic notice (consistent with the requirements of the statute);

(3) Telephonic notice (provided that contact is made directly with the affected persons); or

(4) Substitute notice, if the business demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy notice by (1), (2), or (3) above for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons.

Substitute notice consists of:

(a) Email notice when the business has an electronic mail address for the subject persons;

(b) Conspicuous posting of the notice on the website page of the business, if one is maintained; and

(c) Notification to major statewide media.

Notification Deadline

Notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Notice shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. Notice shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

Government Agency Notification

Must notify the Consumer Protection Division of the Attorney General's Office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.

Consumer reporting agency notification if required to notify more than 1,000 people.

Consequences of Non-Compliance

(A) civil penalties;

(B) private right of action for damages.

Waiver of provisions of law is not permitted as contrary to public policy and is void and unenforceable.

back to Table of Contents

ND

Statute

N.D. Cent. Code, § 51-30-01 *et seq.*

Definition of Breach

Unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted and the information is not otherwise lawfully publicly available:

(A) social security number;

(B) license number;

(C) photo identification card number;

(D) the individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts;

(E) date of birth;

(F) mother's maiden name;

(G) medical information;

(H) health insurance information;

(I) employee identification number; or

(J) the individual's digitized or other electronic signature.

Covered Entities

Any person that conducts business in North Dakota, and that owns or licenses computerized data that includes personal information.

Threshold for Notification

Must disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of title 15 of the United States Code); or

(C) Substitute notice, if the person demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person does not have sufficient contact information.

Substitute notice consists of the following:

(1) Email notice when the person has an email address for the subject persons;

(2) Conspicuous posting of the notice on the person's website page, if the person maintains one; and

(3) Notification to major statewide media.

Notification Deadline

The disclosure must 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 to restore the integrity of the data system.

The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification must be made after the law enforcement agency determines that the notification will not compromise the investigation.

Government Agency Notification

Not required.

Consequences of Non-Compliance

Attorney General enforcement.

back to Table of Contents

OH

Statute
Ohio Rev. Code Ann. § 1349.19 *et seq.*

Definition of Breach

Unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of Ohio.

Breach does not include good faith acquisition of the information as defined by the statute or acquisition of the information pursuant to a search warrant or court order.

Definition of Personal Information

Individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable, or otherwise publicly available:

(A) social security number;

(B) driver's license number or state identification card number; or

(C) account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

Covered Entities

Any person that owns or licenses computerized data that includes personal information.

Threshold for Notification

Must 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.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (consistent with the requirements of the statute);

(C) Telephone notice; or

(D) Substitute notice in accordance with this division, if the person required to disclose demonstrates that the person does not have sufficient contact information to provide notice in a manner described above, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed $250,000, or that the affected class of subject residents to whom disclosure or notification is required exceeds 500,000 persons.

Substitute notice consists of:

(1) Electronic mail notice if the person has an electronic mail address for the resident to whom the disclosure must be made;

(2) Conspicuous posting of the disclosure or notice on the person's website, if the person maintains one; and

(3) Notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds 75% of the population of this state.

Alternate substitute notice is available if person required to notify is a business with less than ten employees and the cost of providing notice would cost more than $10,000.

Notification Deadline

Notice must be provided in the most expedient time possible but not later than 45 days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement 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.

Entity may delay notice if a law enforcement agency determines that notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the person shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security.

Government Agency Notification

Consumer reporting agency notification if required to notify more than 1,000 people.

Consequences of Non-Compliance

(A) Attorney General enforcement and investigation;

(B) fines of up to $1,000 for each day of delay in notification;

(C) intentional or reckless failure to comply with the provision for a period of more than 60 days may result in fines of up to $5,000 per day; if more than 90 days late, may be fined up to $10,000 per day.

Waiver of provisions of law is not permitted as contrary to public policy and is void and unenforceable.

back to Table of Contents

OK

Statute
Okl. Stat. tit. 24 § 161 *et seq.*

Definition of Breach

Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

First name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted, and the information is not otherwise lawfully publicly available:

(A) social security number;

(B) driver's license number or state identification card number issued in lieu of a driver's license; or

(C) financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident.

Covered Entities

Corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit.

Threshold for Notification

Must provide notification to any resident of Oklahoma whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Telephone notice;

(C) Electronic notice; or

(D) Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000 or that the affected class of residents to be notified exceeds 100,000 persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in (A)-(C).

Substitute notice consists of any two of the following:

(1) Email notice if the individual or the entity has email addresses for the members of the affected class of residents;

(2) Conspicuous posting of the notice on the Internet website of the individual or the entity if the individual or the entity maintains a public Internet website; or

(3) Notice to major statewide media.

Notification Deadline

Except to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the disclosure shall be made without unreasonable delay.

Notice required by this section may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security. Notice required by this section must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.

Government Agency Notification

Not required.

Consequences of Non-Compliance

(A) Attorney General or district attorney has power to bring action under Oklahoma Business Protection Act;

(B) may obtain actual damages or impose a civil penalty up to $150,000 per breach of the security system or series of similar breaches discovered in a single investigation.

back to Table of Contents

OR

Statute
Or. Rev. Stat. §§ 646A.602, 646A.604, 646A.624

Definition of Breach

Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the person.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Consumer's first name or first initial and last name in combination with any one or more of the following data elements, not otherwise lawfully publicly available, when the data elements are not rendered unusable through encryption, redaction or other methods, or when the data elements are encrypted and the encryption key has also been acquired:

(A) social security number;

(B) driver's license number or state identification card number issued by the Department of Transportation;

(C) passport number or other United States issued identification number; or

(D) financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account.

The information obtained must be sufficient to permit a person to commit identity theft.

Covered Entities

Any person that owns, maintains or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities.

Threshold for Notification

Notice of the breach of security must be given to any consumer whose personal information was included in the information that was breached.

Notice does not need to be provided if after an appropriate investigation or after consultation with relevant federal, state or local agencies responsible for law enforcement, the person determines that no reasonable likelihood of harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years.

The requirements of this section do not apply to: (a) a person that complies with the notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements pursuant to the rules, regulations, procedures, guidance or guidelines established by the person's primary or functional federal regulator; or (b) a person that complies with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security of personal information than that provided by this section.

Form of Notification

Notice shall include at a minimum: a description of the incident in general terms, the approximate date of the breach of security, the type of personal information obtained as a result of the breach of security, contact information of the person subject to notification, contact information for national consumer reporting agencies, and advice to the consumer to report suspected identity theft to law enforcement, including the Federal Trade Commission.

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (consistent with the requirements of the statute);

(C) Telephone notice (provided that contact is made directly with the affected consumer); or

(D) Substitute notice, if the person demonstrates that the cost of providing notice would exceed $250,000, that the affected class of consumers to be notified exceeds 350,000, or if the person does not have sufficient contact information to provide notice.

Substitute notice consists of:

(1) Conspicuous posting of the notice or a link to the notice on the Internet home page of the person if the person maintains one; and

(2) Notification to major statewide television and newspaper media.

Notification Deadline

Notification shall be made in the most expeditious time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine sufficient contact information for the consumers, determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data.

Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and that agency has made a written request that the notification be delayed. The notification required by this section shall be made after that law enforcement agency determines that its disclosure will not compromise the investigation and notifies the person in writing.

Government Agency Notification

Consumer reporting agency notification if required to notify more than 1,000 people.

Consequences of Non-Compliance

(A) possible public or private investigations by the Director of the Department of Consumer and Business Services;

(B) any person who violates or who procures, aids or abets in the violation of the section shall be subject to a penalty of not more than $1,000 for every violation, which shall be paid to the General Fund of the State Treasury, up to a maximum of $500,000.

back to Table of Contents

PA

Statute
73 Pa. Stat. Ann. § 2301 *et seq.* (West)

Definition of Breach

Unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of Pennsylvania.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted, or otherwise publicly available:

(A) social security number;

(B) driver's license number or a State identification card number issued in lieu of a driver's license; or

(C) financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

Covered Entities

A state agency, a political subdivision of Pennsylvania or an individual or a business doing business in Pennsylvania that maintains, stores or manages computerized data that includes personal information.

Threshold for Notification

Notice must be provided to a resident of Pennsylvania whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.

An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Telephonic notice (consistent with the requirements of the statute);

(C) Email notice; or

(D) Substitute notice, if the entity demonstrates one of the following: the cost of providing notice would exceed $100,000, the affected class of subject persons to be notified exceeds 175,000 or the entity does not have sufficient contact information.

Substitute notice consists of:

(1) Email notice when the entity has an email address for the subject persons;

(2) Conspicuous posting of the notice on the entity's Internet website if the entity maintains one; and

(3) Notification to major statewide media.

Notification Deadline

Except as required by law enforcement or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay.

The notification required may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. The notification required shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.

Government Agency Notification

Consumer reporting agency notification if required to notify more than 1,000 people.

Consequences of Non-Compliance

Attorney General has authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this law.

back to Table of Contents

PR

Statute
P.R. Laws Ann. tit.10 §4051 *et seq.*

Definition of Breach

When access is permitted to unauthorized persons or entities so that the security, confidentiality or integrity of the data has been compromised or when it is known or there is reasonable suspicion that a normally authorized person that had access to the data violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information.

Definition of Personal Information

Individual's name or first initial and last name along with:

(A) social security number;

(B) driver's license number, voter or other official identification;

(C) bank or financial account numbers;

(D) user names and passwords or access codes to information systems;

(E) HIPAA protected information;

(F) tax information; or

(G) work related evaluations.

Covered Entities

Every agency, board, body, examining board, corporation, public corporation, committee, independent office, division, administration, bureau, department, authority, official, instrumentality or administrative organism of the three branches of the Government; every corporation, partnership, association, private company or organization authorized to do business or operate in Puerto Rico; as well as every public or private educational institution.

Threshold for Notification

Duty to notify residents of Puerto Rico of any breach when the database breached contains in whole or in part personal information files and the files are not encrypted and only protected by a password.

Form of Notification

Clients affected by breach must be notified by direct notice (mail or electronic) or if cost would exceed $100,000 to notify, notice can be given by prominent display in certain places or communication to the media.

Notice must include description of the breach in general terms and the type of information compromised. Along with this information a toll-free number and website must be made available where the public can access further information.

Notification Deadline

Notice must be made as expeditiously as possible.

Notice to the government must be provided within 10 days. This deadline may not be extended.

Government Agency Notification

Department of Consumer Affairs

Consequences of Non-Compliance

(A) fines of up to $5,000 for each violation of the statute;

(B) private suit for damages.

back to Table of Contents

RI

Statute
R.I. Gen. Laws § 11-49.2-1 *et seq.*

Definition of Breach

Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the state agency or person.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) social security number;

(B) driver's license number or Rhode Island Identification Card number; or

(C) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Covered Entities

Any state agency or person that owns, maintains or licenses computerized data that includes personal information.

Threshold for Notification

Must notify of breach if it poses a significant risk of identity theft if the information is unencrypted and was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification does not have to be provided if after an appropriate investigation or after consultation with relevant federal, state, or local law enforcement agencies, a determination is made that the breach has not and will not likely result in a significant risk of identity theft to the individuals whose personal information has been acquired.

Any entity that maintains its own security breach procedures and otherwise complies with the timing requirements of the statute, shall be deemed to be in compliance with the security breach notification requirements of this law, provided such person notifies subject persons in accordance with such person's policies in the event of a breach of security.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code); or

(C) Substitute notice, if the state agency or person demonstrates that the cost of providing notice would exceed $25,000, or that the affected class of subject persons to be notified exceeds 50,000, or the state agency or person does not have sufficient contact information.

Substitute notice shall consist of all of the following:

(1) Email notice when the state agency or person has an email address for the subject persons;

(2) Conspicuous posting of the notice on the state agency's or person's website page, if the state agency or person maintains one; and

(3) Notification to major statewide media.

Notification Deadline

Notice must 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.

The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification shall be made after the law enforcement agency determines that it will not compromise the investigation.

Government Agency Notification

Not required.

Consequences of Non-Compliance

Each violation may be punishable by a fine up to $100 per occurrence up to a cap of $25,000.

Waiver of provisions of law is not permitted as contrary to public policy and is void and unenforceable.

back to Table of Contents

Statute
S.C. Code Ann. § 39-1-90

Definition of Breach

Unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

First name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted and is not otherwise publicly available:

(A) social security number;

(B) driver's license number or state identification card number issued instead of a driver's license;

(C) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or

(D) other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.

Covered Entities

A person conducting business in South Carolina and owning or licensing computerized data or other data that includes personal identifying information.

Threshold for Notification

Notice must be provided to a resident of South Carolina if the personal identifying information was not rendered unusable through encryption, redaction, or other method and the information is acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (consistent with the requirements of the statute);

(C) Telephonic notice; or

(D) Substitute notice, if the person demonstrates that the cost of providing notice exceeds $250,000 or that the affected class of subject persons to be notified exceeds 500,000 or the person has insufficient contact information.

Substitute notice consists of:

(1) Email notice when the person has an email address for the subject persons;

(2) Conspicuous posting of the notice on the website page of the person, if the person maintains one; and

(3) Notification to major statewide media.

Notification Deadline

The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The notification required by this section may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it no longer compromises the investigation.

Government Agency Notification

Consumer reporting agency notification if required to notify more than 1,000 people.

Consequences of Non-Compliance

(A) Department of Consumer Affairs may impose fines of up to $1,000 per affected resident for a knowing and willful violation of this section;

(B) Private right of action available.

back to Table of Contents

TN

Statute
Tenn. Code Ann. § 47-18-2107

Definition of Breach

Unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or otherwise publicly available:

(A) social security number;

(B) driver's license number; or

(C) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Covered Entities

Person or business that conducts business in this state, or any agency of the state of Tennessee or any of its political subdivisions, that owns or licenses computerized data that includes personal information.

Threshold for Notification

Entity must provide notice of breach to any resident of Tennessee whose information was, or is reasonably believed to have been, acquired by an unauthorized person.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001); or

(C) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the information holder does not have sufficient contact information.

Substitute notice consists of:

(1) Email notice, when the information holder has an email address for the subject persons;

(2) Conspicuous posting of the notice on the information holder's Internet website page, if the information holder maintains such website page; and

(3) Notification to major statewide media.

Notification Deadline

Notification must 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.

The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

Government Agency Notification

Consumer reporting agency notification if required to notify more than 1,000 people.

Consequences of Non-Compliance

Private right of action available.

back to Table of Contents

TX

Statute
Tex. Bus. & Com. Code §§ 521.002 *et seq.*

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

(A) An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted, and the information is not publicly available:

(1) social security number;

(2) driver's license number or government-issued identification number; or

(3) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

(B) information that identifies an individual and relates to:

(1) the physical or mental health or condition of the individual;

(2) the provision of health care to the individual; or

(3) payment for the provision of health care to the individual.

Covered Entities

A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information.

Threshold for Notification

Must give notice after breach occurs to the person whose information was disclosed.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (if in accordance with 15 U.S.C. § 7001); or

(C) Other notice.

Other notice may be provided where the entity demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:

(1) Electronic mail, if the person has electronic mail addresses for the affected persons;

(2) Conspicuous posting of the notice on the person's website; or

(3) Notice published in or broadcast on major statewide media.

Notification Deadline

Disclosure shall be made as quickly as possible, except if delay is requested by a law enforcement agency or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.

Government Agency Notification

Consumer reporting agency notification if required to notify more than 10,000 people.

Consequences of Non-Compliance

(A) Attorney General enforcement;

(B) civil fines of at least $2,000 but not more than $50,000 per violation;

(C) penalty of $100 per day that the entity fails to provide notification to an affected individual (up to $250,000);

(D) injunctive relief;

(E) Attorney General is entitled to recover reasonable expenses, including reasonable attorney fees, court costs, and investigatory costs, incurred in obtaining injunctive relief or civil penalties.

back to Table of Contents

UT

Statute
Utah Code Ann. §§ 13-44-102, 13-44-201

Definition of Breach

Unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.

Excludes acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner.

Definition of Personal Information

Person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable, that is not lawfully available to the general public:

(A) social security number;

(B) financial account number, or credit or debit card number;

(C) any required security code, access code, or password that would permit access to the person's account; or

(D) driver's license number or state identification card number.

Covered Entities

Person who owns or licenses computerized data that includes personal information concerning a Utah resident.

Threshold for Notification

Must provide notice to each affected Utah resident if after learning of the breach and conducting a reasonable and prompt good faith investigation of it, the entity determines that the personal information disclosed has been or will be misused for identity theft or fraud purposes.

Entities with their own notification policies consistent with the act may be exempt if they provide notification to Utah residents.

Entities primarily regulated by another state or federal agency that is in compliance with the applicable law established by that agency may also be exempt.

Form of Notification

Notice may be provided by one of the following methods:

(A) in writing by first-class mail to the most recent address the person has for the resident;

(B) electronically (if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001);

(C) by telephone (including through the use of automatic dialing technology not prohibited by other law); or

(D) by publishing notice of the breach of system security in a newspaper of general circulation; and following Utah's legal notice publication requirements.

Notification Deadline

Must provide notice in the most expedient time possible without unreasonable delay taking into account: 1) legitimate investigative needs of law enforcement; 2) investigation of the scope of the breach of system security; and 3) restoration of the reasonable integrity of the system.

Government Agency Notification

Not required.

Consequences of Non-Compliance

(A) Attorney General enforcement (investigation and adjudication);

(B) civil fines up to $2,500 for a violation or series of violations concerning a specific individual but no greater than $100,000 in the aggregate;

(C) injunctive relief;

(D) no private right of action but entity may still be liable under contract or tort for the breach.

Waiver of provisions of law is not permitted as contrary to public policy and is void and unenforceable.

back to Table of Contents

VT

Statute
Vt. Stat. Ann. tit. 9 §§ 2430, 2435

Definition of Breach

Unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information maintained by the data collector.

Factors to consider when determining if breach occurred:

(A) indications that information is in physical possession and control of unauthorized person;

(B) indication that information has been downloaded or copied;

(C) indication that information was used by unauthorized person; and

(D) information has been made public.

Definition of Personal Information

Individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons, and the information is not publicly available:

(A) social security number;

(B) motor vehicle operator's license number or nondriver identification card number;

(C) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; or

(D) account passwords or personal identification numbers or other access codes for a financial account.

Covered Entities

State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, for any purpose,whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

Threshold for Notification

Notice is not required if the entity establishes that misuse of the personal information is not reasonably possible and the entity provides notice of its determination that the misuse of the information is not reasonably possible to the Attorney General or Department of Financial Regulation (as applicable).

Entities with their own notification policies consistent with the act may be exempt if they provide the Attorney General with information regarding the date, discovery, and description of the breach.

Form of Notification

Notice may be provided by one of the following methods: mail, electronic notice (if have a valid email and meet certain criteria) or through telephone by a live person.

Notice must be clear and conspicuous and include a description of: the incident in general terms (including the date of the breach), type of personally identifiable information that was subject to the security breach, the general acts of the data collector to protect the personally identifiable information from further security breach, telephone number, toll-free if available, that the consumer may call for further information and assistance, advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

Substitute notice may be provided where cost of notice would exceed $5,000 or the entity does not have sufficient contact information. Such notice consists of (a) conspicuous posting of the notice on the data collector's website page if the data collector maintains one; and (b) notification to major statewide and regional media.

Notice to government will include the date, discovery, and preliminary description of the security breach and the number of Vermont individuals affected. Such notice will not be disclosed to anyone unless ordered by a court for good cause or if the entity provides a sample copy of the notice provided to consumers.

Notification Deadline

Notice of the security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.

To government: must give notice within 14 days, consistent with needs of law enforcement, of the data collector's discovery of the security breach or when the entity provides notice to consumers--whichever is sooner.

Government Agency Notification

Attorney General or Department of Financial Regulation (if regulated by the latter); Must notify consumer reporting agencies when notice must be provided to over 1,000 people.

Consequences of Non-Compliance

Attorney General and state's attorney (or Department of Financial Regulation, as applicable) shall have sole and full authority to investigate potential violations and to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter.

Waiver of provisions of law is not permitted as contrary to public policy and is void and unenforceable.

back to Table of Contents

VA

Statute
Va. Code Ann. §18.2-186.6

Definition of Breach

Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

First name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

(A) social security number;

(B) driver's license number or state identification card number issued in lieu of a driver's license number; or

(C) financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.

Covered Entities

Corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit.

Threshold for Notification

If a breach occurs and the entity reasonably believes it has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, the entity must disclose any breach of the security of the system following discovery or notification of the breach of the security of the system.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Telephone notice;

(C) Electronic notice; or

(D) Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described in subdivisions (A)-(C).

Substitute notice consists of all of the following:

(1) Email notice if the individual or the entity has email addresses for the members of the affected class of residents;

(2) Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and

(3) Notice to major statewide media.

Notice required by this section shall include a description of the following: the incident in general terms, the type of personal information that was subject to the unauthorized access and acquisition, the general acts of the individual or entity to protect the personal information from further unauthorized access, a telephone number that the person may call for further information and assistance, if one exists, and advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Notification Deadline

Must notify Attorney General and affected resident without unreasonable delay.

Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system.

Notice required by this section may be delayed if, after the individual or entity notifies a law enforcement agency, the law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security.

Notice shall be made without unreasonable delay after the law enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

Government Agency Notification

Office of Attorney General; Must notify consumer reporting agencies when notice must be provided to over 1,000 people.

Consequences of Non-Compliance

(A) Attorney General enforcement;

(B) penalties up to $150,000 per breach or series of breaches of a similar nature uncovered in a single investigation;

(C) private right of action;

(D) enforcement by agency that is entity's primary state regulator.

Other Notes

http://www.ag.virginia.gov/CCSWeb/Reports/Data_Breach_Notification_Req.pdf

back to Table of Contents

WA

Statute
Wash. Rev. Code §19.255.010

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

Individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) social security number;

(B) driver's license number or Washington identification card number; or

(C) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Covered Entities

Any person or business that conducts business in this state and that owns or licenses computerized data that includes personal information or any person or business that maintains computerized data that includes personal information that the person or business does not own.

Threshold for Notification

Must provide notification to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. An agency shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001); or

(C) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information.

Substitute notice consists of:

(1) Email notice when the person or business has an email address for the subject persons;

(2) Conspicuous posting of the notice on the website page of the person or business, if the person or business maintains one; and

(3) Notification to major statewide media.

Notification Deadline

For people or businesses conducting business in the state, disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in the law enforcement exception, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

Government Agency Notification

Not required.

Consequences of Non-Compliance

(A) private right of action;

(B) injunction;

(C) rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law;

(D) waiver of the provisions of this statute are void and unenforceable as contrary to public policy.

back to Table of Contents

DC

Statute
D.C. Code § 28-3851 *et seq.*

Definition of Breach

Unauthorized acquisition of data, or any equipment or device storing such data, that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.

Breach does not include good faith acquisition of the information as defined in the statute nor information that is rendered secure so as to be unusable by an unauthorized person.

Definition of Personal Information

(A) An individual's first name or first initial and last name, or phone number, or address, and any one or more of the following data elements:

(1) social security number;

(2) driver's license number or District of Columbia Identification Card number;

(3) credit card number or debit card number; or

(B) Any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account.

Covered Entities

(A) Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information.

(B) Any person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own.

Threshold for Notification

Must provide notification when there is a breach.

Form of Notification

Notification must be written, though electronic notification may be an option if a customer has consented to such form of notification.

Substitute notice may be provided where:

(A) cost of providing notice would exceed $50,000;

(B) the number of individuals to receive notice exceeds 100,000; or

(C) the entity lacks sufficient contact information.

Substitute notice consists of:

(1) email notification if emails are available;

(2) conspicuous posting of notice on webpage of entity; and

(3) notice to major local or, if applicable, national media.

Notification Deadline

The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.

Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation but shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation.

Government Agency Notification

Must notify consumer reporting agencies of the timing, distribution and content of the notices.

Consequences of Non-Compliance

(A) Attorney General may petition for equitable relief including fines of up to $100 per violation, costs of the action and attorney fees;

(B) private suit for damages, costs of the action and attorney fees.

back to Table of Contents

WV

Statute
W. Va. Code §46A-2A-101 *et seq.*

Definition of Breach

Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of West Virginia.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

First name or first initial and last name linked to any one or more of the following data elements that relate to a resident of West Virginia, when the data elements are neither encrypted nor redacted:

(A) social security number;

(B) driver's license number or state identification card number issued in lieu of a driver's license; or

(C) financial account number, or credit card, or debit card number in combination with any required security code, access code or password that would permit access to a resident's financial accounts.

Covered Entities

Corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies or instrumentalities, or any other legal entity, whether for profit or not for profit.

Threshold for Notification

Must provide notice to any resident of West Virginia if the entity knows that the breach caused or reasonably believes the breach will cause identity theft or other fraud of the resident.

Form of Notification

The notice shall include:

(A) To the extent possible, a description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person, including social security numbers, driver's licenses or state identification numbers and financial data;

(B) A telephone number or website address that the individual may use to contact the entity or the agent of the entity and from whom the individual may learn: (1) What types of information the entity maintained about that individual or about individuals in general; and (2) Whether or not the entity maintained information about that individual; and

(C) The toll-free contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a fraud alert or security freeze.

Notice may be provided by one of the following methods:

(1) Written notice;

(2) Telephonic notice;

(3) Electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures, set forth in Section 7001, United States Code Title 15, Electronic Signatures in Global and National Commerce Act); or

(4) Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000 or that the affected class of residents to be notified exceeds 100,000 persons or that the individual or the entity does not have sufficient contact information or to provide notice as described in (1)-(3).

Substitute notice consists of any two of the following:

(a) Email notice if the individual or the entity has email addresses for the members of the affected class of residents;

(b) Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; or

(c) Notice to major statewide media.

Notification Deadline

Except as provided in the law enforcement exception or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the notice shall be made without unreasonable delay.

Notice required by this section may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security.

Government Agency Notification

Must notify consumer reporting agencies when notice must be provided to over 1,000 people.

Consequences of Non-Compliance

(A) Attorney General enforcement (or the entity's primary regulator);

(B) penalties for repeated and willful violations up to $150,000.

back to Table of Contents

Statute
Wis. Stat. §134.98

Definition of Breach

Personal information acquired by an unauthorized person or if a person, other than an individual, that stores personal information pertaining to a resident of Wisconsin, but does not own or license the personal information, knows that the personal information has been acquired by an unauthorized person, and the person storing the personal information has not entered into a contract with the person that owns or licenses the personal information.

Definition of Personal Information

Individual's last name and first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information, encrypted, redacted, or altered in a manner that renders the element unreadable:

(A) social security number;

(B) driver's license number or state identification number;

(C) financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account;

(D) DNA profile; or

(E) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

Covered Entities

"Entity" means a person, other than an individual, that does any of the following:

(A) Conducts business in this state and maintains personal information in the ordinary course of business;

(B) Licenses personal information in this state;

(C) Maintains for a resident of this state a depository account; or

(D) Lends money to a resident of this state.

"Entity" includes all of the following:

(A) The state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the constitution or any law, including the legislature and the courts; and

(B) A city, village, town, or county.

Threshold for Notification

If an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each subject of the personal information.

If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information.

Notification is not required if:

(A) the breach does not create a material risk of identity theft or fraud to the subject of the personal information; or

(B) the information was acquired in good faith by an employee or agent of the entity and for a lawful purpose.

Form of Notification

The covered entity must make reasonable efforts to notify the victim (or the person that owns or licenses the personal information) that there was a breach of data containing their personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.

Notice must be provided by mail or any other means previously used to communicate with the person. If after reasonable diligence the mailing address of the person cannot be found, and the entity has not previously communicated with the person subject to the data breach, the entity must provide notice in a method reasonably calculated to provide actual notice to the person.

Notification Deadline

Must provide notice within a reasonable time, not to exceed 45 days after learning of the breach.

Reasonableness is determined based on the number of notices that must be provided and the means by which the notices will be communicated.

Law enforcement may delay notification to the victims of the breach to protect an investigation or homeland security. The notification process may begin at the end of the time period set forth by law enforcement.

Government Agency Notification

Must notify consumer reporting agencies when notice must be provided to over 1,000 people.

Consequences of Non-Compliance

Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.

back to Table of Contents

WY

Statute
Wyo. Stat. Ann. §40-12-501 *et seq.*

Definition of Breach

Unauthorized acquisition of data that materially compromises the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of Wyoming.

Breach does not include good faith acquisition of the information as defined by the statute.

Definition of Personal Information

First name or first initial and last name of a person in combination with one or more of the following data elements when either the name or the data elements are not redacted:

(A) social security number;

(B) driver's license number or Wyoming identification card number;

(C) account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person;

(D) tribal identification card; or

(E) federal or state government issued identification card.

Covered Entities

An individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming. Also, any person who maintains computerized data that includes personal identifying information on behalf of another business entity.

Threshold for Notification

Must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. If the investigation determines that the misuse of personal identifying information about a Wyoming resident has occurred or is reasonably likely to occur, notice must be provided.

Form of Notification

Notice may be provided by one of the following methods:

(A) Written notice;

(B) Electronic mail notice; or

(C) Substitute notice.

Substitute notice is an option where:

(1) cost of providing Wyoming-based persons or businesses would exceed $10,000 and providing notice to other businesses operating but not based in the state would exceed $250,000;

(2) the number of Wyoming-based businesses or individuals would exceed 10,000 and the number of businesses operating in Wyoming to be notified would exceed 500,000; or

(3) the person does not have sufficient contact information.

Substitute notice consists of:

(a) conspicuous posting on the Internet or website of the person experiencing the breach, including a toll-free number to contact the person with the data breach and the numbers for the major credit reporting agencies; and

(b) notification to major statewide media including a toll-free number where an individual can find out whether he/she is affected.

Notification Deadline

Entity shall give notice as soon as possible to the affected Wyoming resident. Notice shall be made in the most expedient time possible and without unreasonable delay, 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.

The notification required by this section may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation.

Government Agency Notification

Not required.

Consequences of Non-Compliance

The Attorney General may bring an action in law or equity to address any violation of this section and for other relief that may be appropriate to ensure proper compliance with this section, to recover damages, or both.

back to Table of Contents

Contacts

Christopher J. Cox

Partner, Silicon Valley

+1 650 802 3029 tel

chris.cox@weil.com

201 Redwood Shores Parkway

Redwood Shores, CA 94065

David R. Singh

Counsel, Silicon Valley

+1 650 802 3010 tel

david.singh@weil.com

201 Redwood Shores Parkway

Redwood Shores, CA 94065

**Admitted to practice in New York; not yet admitted to practice in California.*

back to Table of Contents

Weil

weil.com

BEIJING
BOSTON
BUDAPEST
DALLAS
DUBAI
FRANKFURT
HONG KONG
HOUSTON
LONDON
MIAMI
MUNICH
NEW YORK
PARIS
PRAGUE
PRINCETON
PROVIDENCE
SHANGHAI
SILICON VALLEY
WARSAW
WASHINGTON, DC

Weil, Gotshal & Manges, LLP