DEVELOPING A COMPREHENSIVE PRIVACY PROGRAM
A STEP-BY-STEP GUIDE

HIGHER EDUCATION VERSION

Daniel J. Solove
John Marshall Harlan Research Professor of Law
The George Washington University
Washington D.C.

I. WHAT IS PRIVACY?

Many commentators have lamented that the meaning of "privacy" is vague and elusive. I contend that we should understand privacy is an umbrella term for a group of related yet distinct things. Privacy is about respecting the desires of individuals where compatible with the aims of the larger community. Privacy is not just about what people expect but about what they desire. Privacy is not merely an individual right – it is an important component of any flourishing community.

With regard to schools, some of the privacy issues include:

> ***Cyberbullying*** **--** Cyberbullying occurs when students use the Internet (blogs, social media, texting, etc.) to harass, humiliate, or torment other students.
>
> ***Gossip*** -- Students or employees can spread harmful, embarrassing, or discrediting information about other students or school employees.
>
> ***Defamation*** -- Students or employees can spread false rumors about others.
>
> ***Data Security Breaches*** -- Personal information maintained in school record systems can be leaked, lost, stolen, or improperly accessed.
>
> ***Improper Disclosure*** -- Personal information about students, employees, or other individuals can be improperly disclosed to others or the public.
>
> ***Breach of Confidentiality*** -- Secrets learned in confidence can be improperly revealed. Sometimes, these secrets should be revealed, such as when there is a duty to reveal such secrets when there is a health or safety threat.
>
> ***Unreasonable Searches*** -- School officials could engage in an improper search of a student or employee – either (1) without sufficient justification or suspicion of wrongdoing or (2) too broad or intrusive to achieve the purposes of the search. In addition to the Fourth Amendment, which regulates public schools, there are statutes that regulate *both* public and private schools.

Surveillance -- The school's use of surveillance cameras or monitoring of its computer network can cause problems if not appropriately limited or subjected to oversight.

Privacy is a broader concept than data security. Data security involves measures to keep data secure, but privacy involves the overall protection and control of personal data. Data security depends upon privacy because the policies and procedures that an institution has regarding protection and control of data have significant implications for data security.

II. WHAT IS A COMPREHENSIVE PRIVACY PROGRAM?

To protect privacy adequately, all schools should develop a comprehensive privacy program.

A comprehensive privacy program is an orderly and thorough way to address all of the school's privacy risks by:

- identifying the risks
- adding or revising policies
- providing guidelines to employees to prevent mishaps
- training employees about how to deal with privacy issues
- keeping updated about new legal and technological developments

"My school has a program for following the Family Educational Rights and Privacy Act (FERPA). Is that sufficient as a comprehensive privacy program?"

No. Schools must do more than just follow FERPA, which covers just a fraction of the privacy issues schools must face. The Act does not address alumni and donor records, employee information, searches and surveillance of students, confidential information not maintained in records, cyberbullying, data retention and destruction, data security, sexting, and countless other issues. Dozens of other federal and state laws apply to schools.

A comprehensive privacy program should ensure the privacy of everyone in the school community is protected -- students, employees, families, alumni, donors, applicants, and others.

III. WHAT ARE PRIVACY AND DATA SECURITY RISKS?

A privacy or data security risk includes any potential problems involving the collection, use, or disclosure of personal data by the school or by others within the school community. Privacy and data security are often viewed as separate things, and they indeed are distinct, yet they are also interrelated. The grandest of technical measures to protect privacy are all for naught if a person wrongly discloses data.

According to estimates, a privacy or data security incident costs on average around $9 million.

There are several types of risk from a privacy/security incident:

Legal Compliance – Failure to comply with privacy laws and regulations can result in significant legal sanctions, liability, fines, and other unpleasant consequences. There are dozens of federal and state laws that apply to schools.

Regulatory agencies are stepping up enforcement. For example, the Department of Health and Human Services (HHS) started issuing significant fines after the 2009 HITECH Act dramatically increased the fines for HIPAA violations. Fines can go up to $1.5 million per provision of HIPAA violated, and many incidents involve multiple provisions violated.

State attorneys general have enforcement power for state privacy/security laws plus they can enforce certain federal laws too (HIPAA, COPPA). Privacy and security laws are expanding in their coverage. HIPAA was recently expanded rather broadly.

Reputational Injuries – Having a privacy/security incident can severely damage the reputation of a school.

Financial Injuries – Privacy and security violations can lead to costly litigation, large damage awards, and expensive and burdensome legal requirements (data security breach notification).

Damage to Student Well-Being – Leaked or improperly-disclosed data can cause significant harm to students as can failure to respond to incidents where students are violating each other's privacy (cyberbullying, online gossip, etc.).
Damage to Employee Well-Being – Privacy/security incidents can affect and harm employees

Soured Relationships – Incidents or even poor privacy practices that have not involved an actual mishap can sour relationships between schools and parents, applicants, donors, alumni, and others. These relationships are essential for schools.

Time and Resources – One of the largest often under-appreciated risks involves the extensive amount of time and resources needed to respond to a privacy/security incident.

IV. HOW DOES A SCHOOL DEVELOP A COMPREHENSIVE PRIVACY PROGRAM?

There are three broad phases of developing a comprehensive privacy program:

Below is a brief overview of each phase. A more comprehensive discussion follows later.

A. Initial Steps

To begin, several initial steps must be undertaken, which will be described in detail below. The school needs to

(1) *Designate a Point Person* – A school should choose a privacy point person to oversee the program.

(2) *Assemble a Privacy Team* – The point person should ideally find a group of other people to assist.

(3) *Identify Data Stewards and Custodians* – The point person and team should identify the data stewards and custodians at the school.

(4) *Learn the Privacy Landscape* – The point person and any team members should learn the basics of privacy.

(5) *Articulate Privacy Principles* – A school should identify its guiding privacy principles

B. Launching the Program

There are four basic steps to launching the comprehensive privacy program:

(6) *Assessment* – The assessment involves examining a school's policies and practices regarding privacy to identify potential risks and points for improvement.

(7) *Implementation* – Implementation involves making changes to policies and practices. It involves adding new policies, revising old policies, instituting guidelines, and conducting data inventories.

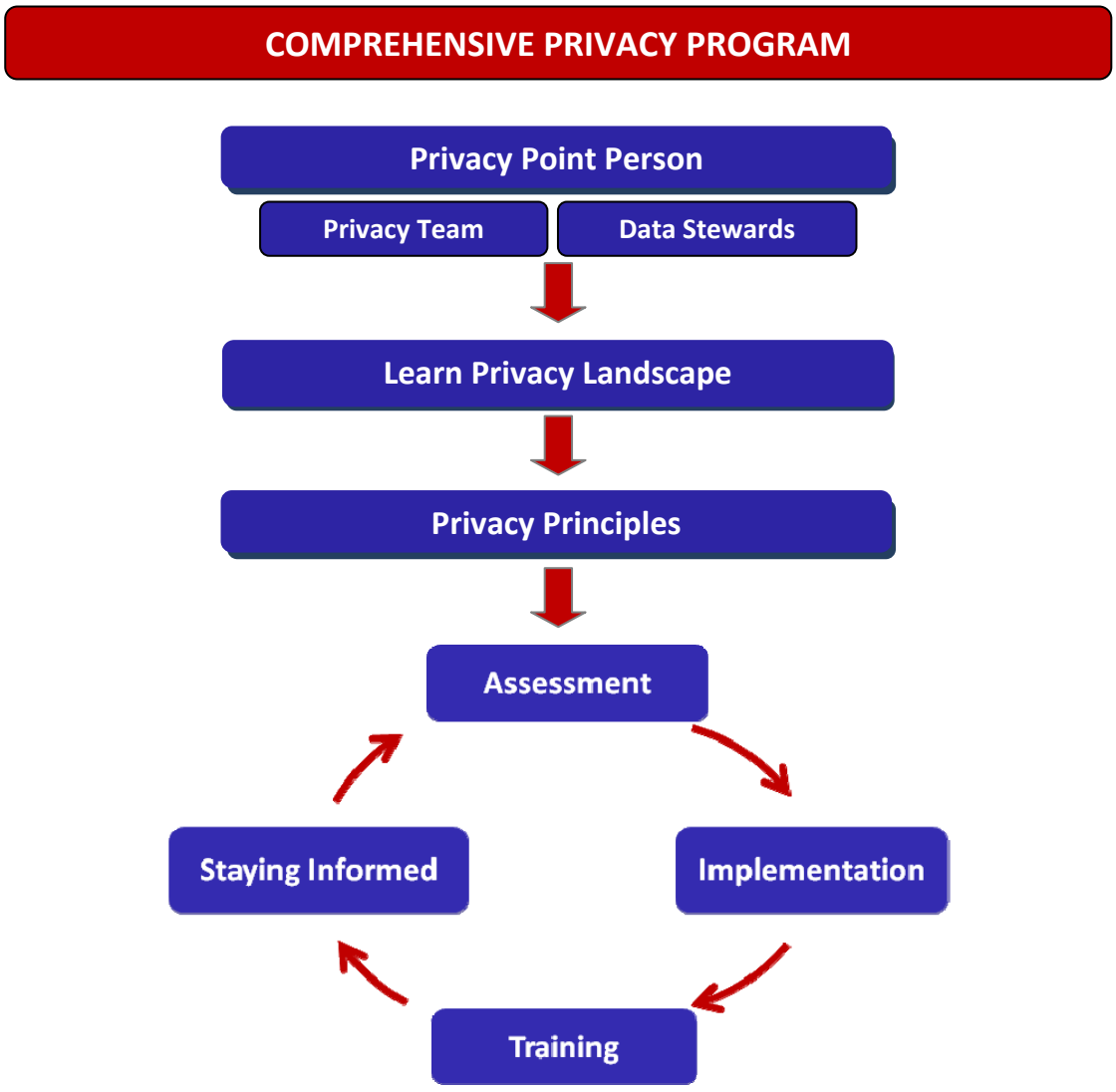
(8) *Training* – Employees should be provided training to raise awareness about privacy and to learn about how to avoid privacy mishaps.

(9) *Staying Informed* -- The privacy point person, the privacy team, and the various data stewards and custodians should keep up-to-date about new developments in privacy law and technology. They should strive for continuing education in privacy.

C. Maintaining the Program

A privacy program is an ongoing cycle, not a static thing. Thus, the last step is ongoing, and it involves repeating Steps (6) through (9):

(10) *Repeat.* The cycle should be repeated each year, with an assessment, followed by implementation, training, and information.



PHASE I

INITIAL STEPS

1. Designate a Privacy Point Person

A privacy point person is a person at a school who has an understanding of how the school is addressing all privacy issues. The point person knows the various "data stewards" (those people in a school system who are in charge of various repositories of personal data) and “data custodians” (those who maintain the data). The point person also fields questions about privacy from various school employees, students, and others -- and he or she knows to whom to send people for answers.

A privacy point person is our term for a school equivalent to a Chief Privacy Officer (CPO). Many other types of organizations (banks, hospitals, businesses, government agencies) have a CPO who oversees how that organization is handling privacy issues.
Schools have as much personal information as other organizations and face privacy issues of great complexity. Yet most schools lack CPOs.

A CPO does the following:

- keeps up with the law and regulations affecting the organization
- works on a plan to ensure the organization effectively protects privacy
- assesses all the types of personal information the organization collects and how it is maintained, used, and disclosed
- ensures that all employees are appropriately trained
- conducts routine assessments of the organization's implementation and compliance with its policies, and identifies weaknesses and problems to be resolved.
- is available for consultation about privacy issues that arise

Only a small fraction of institutions of higher education have CPOs. According to an article by Fred H. Cate, a distinguished professor at Indiana University, colleges and universities “lag far behind industry in appointing privacy and security officers.”[1] Professor Cate goes on to note that: “Although colleges and universities accounted for more than one-third of the publicly reported information security breaches in 2005 and the first half of 2006, they provide scant training in privacy and security issues, especially outside of the technological arena, and rarely audit for compliance.”[2]

Even if a school lacks the resources to hire a CPO, at the very least someone should be designated as the privacy point person. That person should be very familiar with the school’s policies pertaining to privacy and should be available to handle any questions or complaints.

---

[1] Fred H. Cate, *The Security and Privacy Vacuum in Higher Education*, EDUCAUSE Review (Sept./Oct. 2006).
[2] *Id.*

Based on my knowledge of privacy litigation in other contexts (business, government, medical), I believe that much of it might have been averted through better contact and responsiveness with individuals. There is no substitute for the human touch – a person who will listen to concerns and take them seriously.

Even more importantly, a more comprehensive and systematic approach to privacy will help schools avert privacy debacles and costly litigation. With the appropriate policies, oversight, auditing, and training, schools can dramatically limit their exposure to very damaging privacy mistakes, ones that can hurt students, harm the school's reputation, embroil the school in expensive litigation, and ensnare teachers, officials, or staff in legal trouble.

2. Assemble a Privacy Team

It can be challenging for one person to develop a comprehensive privacy program, even with the help of TeachPrivacy. Of course, it can be done, but we recommend that the point person form a team to assist.

I recommend your team include a representative from as many of the following as possible:

- IT (i.e. Chief Information Security Officer)
- General Counsel's Office
- Central Administration (i.e. Dean of Students)
- Student Conduct
- HR
- Records Office/Registrar
- Other Data Stewards (see the next step for more information)

Forming a robust privacy team will certainly be challenging. People are very busy. But a privacy team will help a school with the development of a comprehensive privacy program and will pay dividends down the road in terms of prevention of privacy mishaps and risk reduction.

3. Identify the Data Stewards

A **data steward** is a person responsible for a repository of personal data. This person is the one who manages it, sets policy regarding access and use, etc.

You should identify all data stewards and have their contact information handy. This is important for at least two reasons:

1. In the event of a data security breach or privacy mishap, being able to quickly reach out to all relevant data stewards is essential.

2. Having a person responsible for each repository of data helps ensure that no repositories of data lack oversight.

WHO ARE THE DATA STEWARDS?

- Records office or registrar
- Student life or student affairs
- Human resources
- IT
- Library
- Law enforcement unit
- Alumni office
- Admissions office
- Financial or business office
- Financial aid office
- Student health services

Note that the list of data stewards above is just a partial list. To identify data stewards, examine each department in your school and determine whether it maintains personal data.

4. Learn the Privacy Landscape

I recommend that the point person and privacy team familiarize themselves about privacy. They should gain a basic awareness of privacy – what privacy is and why it matters, as well as information about the various privacy issues schools must face. They should also have a general understanding of the privacy laws that are pertinent to schools. This understanding need not be a lawyerly one; it can consist of knowing what the laws are and roughly what they cover.

5. Articulate Privacy Principles

In order to develop a comprehensive privacy program, a school should articulate a statement about guiding principles with respect to privacy. What are the central goals and values the school wants to promote with regard to privacy?

There are many different sets of privacy principles that have been developed over the years. One set is the Fair Information Practices (FIPs) which were developed in 1973 in a report prepared by a federal agency. These practices recommended transparency about the personal information maintained about people, access rights to people's data, restricting the use of a person's data for

a different purpose without consent, rights to correct a record, and greater data security. The FIPs inspired privacy laws around the world.

Another famous set of privacy principles are the Organization of Economic Cooperation and Development (OECD) Guidelines, which involve eight principles articulated in 1980. Laws around the world have adopted basic privacy principles. The EU Data Protection Directive embodies privacy principles, as do certain U.S. laws. Various organizations have also articulated privacy principles, such as the Generally Accepted Privacy Principles (GAPP) developed by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants.

Below are a set of privacy principles that I believe should serve as useful ideals for schools to aspire to when developing a comprehensive privacy program.

I. INDIVIDUAL RIGHTS

Consent

To the maximum extent possible consistent with the various interests the school is trying to achieve, the school should ask for people's consent before collecting, using, or disclosing personal information.

For every policy regarding the collection, use, or disclosure of personal data, the school should evaluate whether a rule involving obtaining consent beforehand would be feasible or counterproductive.

Notice and Transparency

The school should be as transparent as possible about its policies involving the collection, use, and disclosure of personal information.

The school should provide notice when violations of its privacy policies affect individuals.

Limitation

The collection, use, and disclosure of personal information should be as limited as possible in order to achieve articulable purposes.

Excessive data collection or disclosure should be eliminated.

The purposes for collecting, using, or disclosing personal data should be of substantial importance.

Restriction on Secondary Use

Generally, the school should not use a person's data for any different purposes beyond those for which the data was initially collected. If the school desires to use a person's data for new purposes, the school should first procure that person's consent. Exceptions to this rule should be expressly delineated in the school's policies.

The aggregation of data to produce new insights about individuals should be considered a secondary use.

Confidentiality

The school should maintain the confidentiality of data supplied by individuals unless there is a compelling reason to breach confidentiality.

Restriction on Disclosure

Whenever the school discloses personal data, it should ensure that such disclosure remains as limited as possible and is only done for compelling reasons. Disclosures of personal information should only be made after substantial consideration of all the interests involved.

The reasons for disclosure must be delineated in policies clearly promulgated in advance.

Data Retention and Destruction

Personal data should not be retained once there is no longer a need for it.
The school should examine the types of information it maintains and set a schedule for when such records will no longer be needed and should be destroyed.
When disposed, personal data should be properly destroyed or deleted.

II. DUTIES AND RESPONSIBILITIES

Self-Awareness

The school should keep an inventory of (1) the kinds of data it collects, uses, and maintains; (2) the purposes for which this information is collected; (3) the employees who have access to it; (4) with whom it is shared; and (5) how it is protected.

Vigilance

The school should remain vigilant about its privacy policies and practices, routinely assessing its policies and their implementation.

Security

The school should keep data secure by using physical, technical, and procedural safeguards.

The school should keep track of which employees have access to which types of personal data.

The school should ensure employees are properly trained about data security.

Whenever transported or transmitted beyond school premises, sensitive data should be kept in encrypted format and password-protected.

Responsibility and Accountability

The school should designate individuals who will oversee that the policies are followed.

The school should have a mechanism for enforcement against violations of policy.

The school should have procedures in place to prevent violations and abuses.

The school should have procedures in place for investigating and responding to potential violations of privacy policies.

Training and Implementation

The school should ensure that privacy is more than just having good policies but also involves practices. The policies should be effectively implemented, and employees should be trained about how to respect privacy.

Protecting privacy should be engrained in a school's culture, not just stated abstractly in the text of policies.

III. THE SCHOOL COMMUNITY

Respect for Each Other's Private Life

The school should provide an atmosphere of mutual respect, where members of the community do not infringe upon each other's privacy or well-being.
To the maximum extent possible consistent with freedom of speech, the school should take steps to ensure that members of the community are not engaging in expression that causes harm to others.

Education and Guidance of Students

The school should help its students by teaching them how to protect their own privacy and respect the privacy of others.

PHASE II

LAUNCHING THE PROGRAM

Once you have completed the initial steps, you're ready to begin. The central engine of a comprehensive privacy program is the assessment, and it's the next step you should undertake.

6. Assessment

The assessment process is something I strongly recommend schools undertake on a periodic basis. Most organizations with a Chief Privacy Officer (CPO) conduct such assessments. Ask any CPO, and he or she will tell you about the profound importance of the assessment process.

The assessment process also requires an assessment of how well the school is following its policies. More broadly, the assessment is the time for schools to reassess their policies in light of recent developments in law and practice.

Why Are Assessments Important?

A privacy assessment is of great value to a school in ensuring that it:

- keeps its privacy policies up to date
- remains aware of the information it is collecting, how it is using and disclosing this information
- remains aware of new legal and regulatory developments
- ensures employees are properly trained and are diligently following the policies
- ensures that privacy policies are effectively implemented
- identifies weaknesses in privacy policies, practices, implementation, and compliance and seeks to improve them

The assessment is essential on a routine basis, as it is very easy for privacy policy to drift. In a 1994 study of how various organizations (including banks and insurance companies) addressed privacy, all of them "exhibited a remarkably similar approach: the policy-making process, which occurred over time, was a wandering and reactive one." Jeff Smith, a professor of business administration and the author of the study, noted that policy tended to drift over time, and he quoted one executive at a health insurance company: "We've been lazy on the privacy [issues] for several years now, because we haven't had anybody beating us over the head about them."[3]

A privacy assessment is important because privacy practices at organizations have a tendency to drift. Professor Jeff Smith's study of privacy policies at several major entities revealed that "in the absence of continual vigilance on the part of executives and an infrastructure stronger than any observed at the sites in this study, a 'policy/practice gap' can be expected, in which the actual organizational practices are at variance with the official policies."[4]

Many schools lack of a systemic approach toward addressing privacy issues. Sometimes these problems arise because employees are not adequately trained. Sometimes the problem stem from different departments of a school having divergent privacy practices. .

A privacy assessment ensures the kind of systemic and sustained vigilance necessary to deal with privacy issues. Thus, doing just one assessment and then never repeating the process is not likely to lead to the most meaningful risk reduction. Repeat assessments will ensure that practices continue to improve rather than drift back to their old troublesome ways.

[3] H. Jeff Smith, *Managing Privacy: Information Technology and Corporate America* 55, 67 (1994).
[4] *Id.* at 95.

7. Implementation

It's now time for action. Review your assessment and determine which items you would like to change, what you think is feasible in the short term and long term, and then figure out a strategy for getting it accomplished.

Please note that it is highly unusual for a school to make radical changes in just one year. A comprehensive privacy program is typically *built over the course of many years.* It takes time to get "buy in." It takes time to change or add policies. Even accomplishing a few of our recommendations on our assessment report is a success. We hope to be back in subsequent years to renew our recommendations and help you find ways to advance your privacy program. Over time, it *will happen* as more "buy in." In the experience of many organizations, "buy in" is a slow process but once people buy in, they're in. There's very little "buy out."

Get "Buy In" from the Top

At many institutions, not all the top school officials understand the importance of having a comprehensive privacy program.

This is common for CPOs at major companies. Typically, those at the top will finally "get it" when there is a major privacy mishap. Unfortunately, it is too late at this juncture.

Privacy risks are often not instantly recognized and appreciated. You must spend effort getting top school officials to understand privacy risks and their magnitude.

Get Horizontal "Buy In"

In addition to "buy in" at the top, you need "buy in" from the various data stewards. In some cases, some data stewards may not be cooperative and see you as a threat to their domain.

The ideal comprehensive privacy program has all data stewards involved, with each playing a key role. The privacy point person need not be an overlord – instead, the point person should govern loosely, connecting the data stewards and custodians, providing advice, improving coordination and sharing of information about practices and procedures. The point person is the glue that holds it all together. The relationship is horizontal, not vertical. Ideally, a consensus will develop about which things should be changed.

Gain Visibility

The privacy point person should gain visibility in the school community. People must know about the point person in order to seek guidance or voice concerns.

Data Inventory

The school should perform a data inventory so that it is aware of all the types of personal information it collects and maintains, as well as how that information is handled. Student data at schools is often dispersed among many different employees and school officials.

A data inventory consists of a spreadsheet or set of forms that contain the following information about each "data set." A "data set" is a particular group of records. A data set might consist of the library records or the records of student performance or the alumni office records. For each data set, an inventory should include answers to the following questions:

The Nature of the Data
• What types of data are being kept?
• How sensitive is each type of data?

Responsibility for the Data
• Who is the custodian of the data?
• Where is the data stored?
• Who is responsible for it?

Means of Storage
• How is it stored?
• How long is it kept?
• What types of controls are in place to protect it?

Purpose and Use
• What was the purpose for its collection?
• How is it being used?

Access
• Who has access to the data?
• What responsibilities are imposed on those with access to the data?

8. Training

Training is an essential element of effective privacy policy. Policies are mere words on a page without implementation and training. Policies need to be understood in order to be followed. One of the most important things many companies do to ensure they are effectively protecting privacy is to have annual training of employees.

Why Train?

Training employees is one of the most important things a school can do to protect privacy. Most privacy mishaps occur not because of technical problems but due to the human factor. In case after case, investigations of privacy mishaps revealed a lack of training to be a key cause.

A review of the thousands of reported privacy and security incidents across many industries has revealed a common theme. A sizeable majority of incidents happen because of a lack of guidance and awareness about privacy and security. An article in the Wall Street Journal aptly said that an organization's biggest data security risk is "you." Data security is not just a technical problem but a human problem.

Who Should be Trained?

Everyone. The privacy and security incidents at schools are not confined to only particular types of employees. Some were caused by staff, some by administrative officials, some by faculty.

When and How Often Should Personnel Be Trained?

All new employees should be trained soon after being hired. All existing employees who have been trained should be given refresher lessons each year. As nearly anyone in education knows, the most effective education isn't once and done, but something that ideally occurs over time. Education is a continual process. People quickly forget after a while, and "refresher" training is necessary to keep them informed. At most large organizations, privacy and data security training are a topic for annual training.

For schools with student employees – in the registrar's office, in residence halls as monitors, as teaching assistants, etc. – there should be a training program for these students.

How to Reach Faculty?

Faculty are particularly challenging to train. Faculty resist being forced to take training. The solution: Roll out the training as "education" not "training." Faculty routinely listen to lectures by other professors. If training were cast in this way and didn't speak down to its audience, faculty would be responsive. Faculty want to be educated, not trained.

General Training Pedagogy

As one who has taught both offline as well as online, I have formed some strong beliefs about online training pedagogy.

1. Offline training doesn't readily translate to online. Just recording a bunch of lectures and putting them online doesn't work very well. This is because people's attention spans are shorter online. The classroom environment enhances learning a lot and cannot readily be replicated online. But online training can be effective if it is short and interactive. Training must be designed to fit the medium.
2. Long training sessions that last hours are wasted. Anything beyond 30-40 minutes is likely going to be lost. Longer doesn't necessarily translate into more information retained.
3. Training should use the time-tested tools of effective education: stories, interaction and humor (whenever possible). As a law school professor, the two most effective ways to teach law are the case method and problem method. The case method involves discussing specific cases rather than rules in the abstract. Students learn so much better when discussing concrete cases. The problem method involves going through a hypothetical situation with students and applying rules. This, too, is very effective. Merely stating rules in the abstract doesn't work at all. Interaction is also key, because people learn better when they are active rather than passive. Of course, information must be conveyed, and so there must be some lecture component, but there should also be some interactivity.
4. People learn in different ways. Some people learn well by listening. Others need visual stimulation. For example, I'm a visual learner. I remember concepts better when combined with images. Images linked to concepts stick better in my mind. That's why I always teach with images so visual learners can better remember material.
5. Some degree of variation can enhance learning. I've seen training materials where everything looks the same. It is great for consistency, but not for learning, because everything blends together. We remember most what is distinctive. For example, think of what you remember most from your classes in school? Was it the common day that you

experienced day-in day-out? Or was it the special classes such as field trips or where special things were brought into class?

6. Training should make you think and make you care. People should not just be told what to do and what not to do. Good education demonstrates why it all matters and why people should care. As a law professor, I know that reciting rules to students is not really teaching them. They need to learn *why the rules matter.* They need to learn the purpose of the rules and see how they work in real situations. They need to care about the rules.
7. Key points must be emphasized and reinforced. A common mistake is for training programs to get bogged down in minor details that aren't essential, and to test on these minor details because they are trickier. It is true that the test will be harder this way, but there's a big problem: These aren't the key details that are the primary learning objective. Recall those school exams that had questions on some obscure points buried in the reading. These exam questions are a waste because these points are not important. The most effective teaching gets learners to realize and learn the most important information, because over time, the minor details will be forgotten. Thus, the training should reinforce and test on the most important points.

9. Staying Informed

This step basically involves keeping informed. Continue to educate yourself about privacy and follow new developments.

PHASE III

MAINTAINING THE PROGRAM

10. Repeat

As I indicated before, a comprehensive privacy program is a continuing cycle, not a once-and-done wave of the wand. First, a privacy program often must be built over a period of time. It is rare for a school to develop a comprehensive privacy program in just one year. Second, to maintain a privacy program, annual assessments are needed to ensure that policies don't become outdated, that practices don't start to drift, that people remain trained and aware. Third, privacy law and technology are changing very rapidly, so it is important to stay current.

06B. DATA PRIVACY AND DATA SECURITY COMPLIANCE ISSUES

MAJOR STATE DATA BREACH LAW VARIATIONS

November 6 – 8, 2013

Gerald Ferguson
BakerHostetler

The following standard definitions of Personal Information and Breach of Security (based on the definition commonly used by most states) are used for ease of reference, and any variations from the common definition are noted:

> **Personal Information**: An individual's first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state-issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media. In addition, Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
>
> **Breach of Security**: The unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information.

The following is a list of states which have significant variations from standard requirements of state breach notification statutes:

Please note that the following summary of state data breach statutes are not intended to be and should not be used as a substitute for reviewing the statutory language, nor do they constitute legal advice.

States in Which Definition for "Personal Information" is Broader than the General Definition	
Alaska	Personal Information of Alaska residents. In addition: passwords, personal identification numbers, or other access codes for financial accounts.
Arkansas	Personal Information of Arkansas residents. In addition: medical information.
California	General Breach Notification Statute: Personal Information of California residents. In addition: medical information; health insurance information. Medical Information Specific Breach Notification Statute: For clinics, health facilities, home health agencies, and hospices licensed pursuant to sections 1204, 1250, 1725, or 1745 of the California Health and Safety Code, the state's Medical Information Breach Notification statute may apply. The statute applies to patients' medical information. "Medical information" means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or Social Security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.
Georgia	Personal Information of Georgia residents. In addition: a password and any of the data elements not in connection with the name if any of the other data elements alone would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.
Iowa	Personal Information of Iowa residents. In addition: a 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; unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.
Kansas	Personal Information of Kansas residents. In addition: an account number or credit card/debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account.
Maine	Personal Information of Maine residents. In addition: a password, if any of the other data elements alone would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose

States in Which Definition for "Personal Information" is Broader than the General Definition	
	information was compromised.
Maryland	Personal Information of Maryland residents. In addition: an individual Taxpayer Identification Number.
Massachusetts	Personal Information of Massachusetts residents. In addition: financial account information with or without password or security code information. This includes non-electronic personal information.
Missouri	Personal Information of Missouri residents. In addition: a unique electronic identifier or routing code in combination with required security code, access code, or password that would permit access to an individual's financial account; medical and health insurance information, including an individual's medical history, mental or physical condition, treatment or diagnosis, health insurance policy number and any other unique identifier used by a health insurer.
Nebraska	Personal Information of Nebraska residents. In addition: a unique electronic identification number or routing code, in combination with any required security code, access code, or password; or unique biometric data, such as finger print, voice print, or retina or iris image, or other unique physical representation.
New Hampshire	Medical Information Unauthorized Disclosure Notification Statute: For persons, corporations, facilities, or institutions either licensed in New Hampshire or otherwise lawfully providing health care services, the state's Medical Information Unauthorized Disclosure Notification statute may apply. The statute applies to protected medical information from §§262 and 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (codified at 42 U.S.C. § 300gg and 29 U.S.C § 1181 et seq. and 42 USC 1320d et seq. (2010)).
New Jersey	Personal Information of New Jersey residents. In addition: 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.
New York	The law applies to "private information," which means personal information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person, in combination with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or non-driver identification card number; or (3) 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. The law statute covers "private information," which is personal information consisting of any information in combination with any one or more of the following data elements: (1) social security number; (2) driver's license number or non-driver identification card

States in Which Definition for “Personal Information” is Broader than the General Definition	
	number; or (3) 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. “Personal information” means any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person. Private information does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.
North Carolina	A person’s first name or initial and last name, in combination with any one or more of the following: (1) Social Security number; (2) driver’s license or State ID number; (3) account number, credit or debit card number, in combination with security or access codes or passwords to an individual’s financial account; (4) biometric data; (5) finger prints; (6) other information that would permit access to a person’s financial account or resources. Personal Information does not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parents’ legal surname prior to marriage, or a password unless this information would permit access to a person’s financial account or resources.
North Dakota	“Personal information" means an 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: (1) the individual's social security number; (2) the operator's license number assigned to an individual by the department of transportation; (3) a nondriver color photo identification card number assigned to the individual by the department of transportation; (4) 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; (5) the individual's date of birth; (6) the maiden name of the individual's mother; (7) medical information; (8) health insurance information; (9) an identification number assigned to the individual by the individual's employer; or

States in Which Definition for "Personal Information" is Broader than the General Definition	
	(10) the individual's digitized or other electronic signature.
Ohio	Personal Information of Ohio residents, excluding publicly available information that is lawfully available to the general public from federal, state, or local government records or any of the following media that are widely distributed: 1) any news or editorial advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television; 2) any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media; 3) any publication designed for and distributed to members of any bona fide associations or charitable or fraternal nonprofit corporation; 4) any type of media similar in nature to any item, entity, or activity identified above.
Oregon	A consumer's first name or first initial and last name in combination with any one or more of the following data elements 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: (1) Social Security number; driver license number or state identification card number issued by the Department of Transportation; (2) passport number or other United States issued identification number; or (3) 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. Personal information also includes any of the data elements or any combination of the data elements described above when not combined with the consumer's first name or first initial and last name and when the data elements are not rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised. Personal information DOES NOT include information, other than a Social Security number, in a federal, state or local government record that is lawfully made available to the public.
South Carolina	Personal Information of South Carolina residents. ddition: 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.
Texas	The statute applies to "Sensitive personal information", which includes Personal Information of Texas residents. In addition: information that identifies an individual and relates to: 1) the physical or mental health or condition of the individual;

States in Which Definition for "Personal Information" is Broader than the General Definition	
	2) the provision of health care to the individual; or 3) payment for the provision of health care to the individual.
Vermont	"Personally identifiable information" of Vermont residents, which means an 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, redacted, or otherwise protected: (i) Social Security number; (ii) motor vehicle operator's license number or non-driver identification card number; (iii) 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; (iv) account passwords or personal identification numbers or other access codes for a financial account.
Virginia	Personal Information Breach Notification Statute: Personal Information of Virginia residents. In addition: medical information. Medical Information Breach Notification Statute: For an authority, board, bureau, commission, district or agency of the state or of any political subdivision of the state, or agencies in the state supported wholly or principally by public funds, the state's Medical Information Breach Notification statute may apply. The statute applies to Medical information. "Medical information" means the first name or first initial and last name with any of the following elements: (1) any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (2) an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
Wisconsin	An individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: (1) the individual's Social Security number; (2) the individual's driver's license number or state identification number; (3) the number of the individual's 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; (4) DNA profile; (5) the individual's unique biometric data, including fingerprint, voice print,

States in Which Definition for "Personal Information" is Broader than the General Definition	
	retina or iris image, or any other unique physical representation.
Wyoming	"Personal identifying information", which includes the 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.
District of Columbia	A person's first name or first initial and last name, or phone number, or address, in combination with one of the following: (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 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.
Puerto Rico	At least the name or first initial and the surname of a person, together with any of the following data so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code: (1) Social Security number; (2) driver's license number, voter's identification or other official identification; (3) bank or financial account numbers of any type with or without passwords or access code that may have been assigned; (4) names of users and passwords or access codes to public or private information systems; (5) medical information protected by the HIPAA; (6) tax information; (7) work-related evaluations.

States that Trigger Notification by Access	
Connecticut	"Breach of security" means unauthorized access to or unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information when access to the personal information has

States that Trigger Notification by Access	
	not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.
New Jersey	"Breach of security" means 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.
Puerto Rico	"Violation of the system's security" means any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. This includes both access to the data banks through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings.

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered	
Alaska	Notice is not required if, after an investigation and written notice to the Attorney General, the entity determines that there is not a reasonable likelihood that harm to the consumers has or will result. The determination must be documented in writing and maintained for five years.
Arizona	Notice is not required if the breach does not materially compromise the security of the personal information maintained or if the entity or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur.
Arkansas	Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.
Colorado	Notification is not required if after a good-faith, prompt and reasonable investigation, the entity determines that misuse of personal information about a Colorado resident has not occurred and is not likely to occur.
Connecticut	Notification is not required if, after a reasonable investigation and consultation with relevant law enforcement agencies, it is determined that there is no reasonable likelihood of harm to customers.
Delaware	Notification is only required if an investigation determines that the misuse of

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered	
	information about a Delaware resident has occurred or is reasonably likely to occur.
Florida	Notification is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for 5 years.
Hawaii	Notification is not required if the entity determines after a reasonable investigation that there is no reasonable likelihood of harm.
Idaho	Notification required if the security, confidentiality, or integrity of the personal information for one or more persons is materially compromised and an investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur.
Indiana	Notification required 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, identity theft, or fraud affecting the Indiana resident.
Iowa	Notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial 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.
Kansas	Any entity to which the statute applies shall, when it becomes aware of any breach of the security of the system, 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.
Louisiana	Notification is not required if after reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers.
Maine	Notification is not required if after conducting a good-faith, reasonable and prompt investigation, the entity determines that there is not a reasonable likelihood that the personal information has been or will be misused.
Maryland	Notification is not required if after a good-faith, reasonable and prompt

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered	
	investigation the entity determines that the personal information of the individual was not and will not be misused as a result of the breach. If after the investigation is concluded, the entity determines that notification is not required, the entity shall maintain records that reflect its determination for three years after the determination is made.
Massachusetts	The breach must create a substantial risk of identity theft or fraud against a resident of the commonwealth or 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.
Michigan	The person or agency does not have to provide notice if 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, one or more residents of Michigan. In making this determination, a person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.
Mississippi	Notification is not required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.
Missouri	Notification is not required if, after an appropriate investigation by the person or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the documentation shall be maintained for five years.
Montana	Notification required if the unauthorized acquisition of computerized data materially compromises the security, confidentiality, or integrity of personal information and causes or is reasonably believed to cause loss or injury to a Montana resident.
Nebraska	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.
New Hampshire	For Personal Information Breach Notification Statute: Notification is not required if it is determined that misuse of the information has not occurred and is not reasonably likely to occur.
New Jersey	Notification is not required if the business or public entity establishes that misuse of the information is not reasonably possible (must retain a record of this decision for five years).
New York	In determining whether information has been acquired, or is reasonably

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered	
	believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others: (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or (2) indications that the information has been downloaded or copied; or (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
North Carolina	Notification not required if a breach does not result in illegal use of personal information, is not reasonably likely to result in illegal use, or there is no material risk of harm to a consumer.
Ohio	Notification required only 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.
Oklahoma	Notification required if the breach causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.
Oregon	For a person that owns the data, notification is not required 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.
Pennsylvania	Notification required only if the access and acquisition materially compromises the security or confidentiality of personal information.
Rhode Island	Notification of a breach is not required 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.
South Carolina	Notification required when personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person, and 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.
Tennessee	Notification required for unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder.

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered	
Utah	Notification required if misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur
Vermont	Notice of a security breach is not required if the data collector establishes that misuse of personal information is not reasonably possible and the data collector provides notice of the determination and a detailed explanation for said determination to the Vermont attorney general or to the department of banking, insurance, securities, and health care administration. If the data collector later gathers facts to indicate that the misuse of personal information is reasonably possible, then notice is required.
Virginia	Notification required if the entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.
Washington	A person, business, or 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.
West Virginia	Notification required only if the individual or entity reasonably believes the breach has caused or will cause identity theft or other fraud to any resident of this State.
Wisconsin	Notification is not required if the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.
Wyoming	Notification is required when unauthorized acquisition of computerized data 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 this state. Residents must be notified of a breach of the security of the system when, after a good faith, reasonable, and prompt investigation, the individual or commercial entity determines that the misuse of personal identifying information about the residents has occurred or is reasonably likely to occur.

States that Require Notice to Attorney General or State Agency	
Alaska	If an entity determines after an investigation that the breach does not create a reasonable likelihood that harm to the consumers has or will result, it must document this determination and provide notice of the determination to the Attorney General.
California	General Breach Notification Statute: Any person who notifies more than 500 California residents as a result of a single breach must electronically submit a

States that Require Notice to Attorney General or State Agency	
	single sample copy of the notification letter to the Attorney General. Medical Information Specific Breach Notification Statute: The California Department of Health Services must be notified no later than 5 business days after the unauthorized access, use, or disclosure has been detected by the licensee.
Connecticut	If notice of a breach of security is required to be provided to affected individuals, the person must also provide notice of the breach to the Attorney General not later than the time when notice is provided to residents. Pursuant to Bulletin IC-25 (Aug. 18, 2010), all licensees and registrants of the Connecticut Insurance Department are required to notify the Department of any information security incident which affects any Connecticut residents as soon as the incident is identified, but no later than five calendar days after the incident is identified.
Hawaii	If the breach involves over 1000 persons, the Hawaii Office of Consumer Protection must be notified of the timing, content and distribution of the notice.
Idaho	If the entity is a public agency, it must notify the Attorney General within 24 hours of discovery. The agency must also 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.
Illinois	Any state agency that collects personal information and has had a breach of security of the system data or written material shall submit a report within five 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 agency that has submitted a report under the statute 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.
Indiana	The Attorney General must be notified regarding a breach.
Louisiana	When notice must be given to Louisiana citizens, the entity must 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 names of all Louisiana citizens affected. Notice to the state Attorney General shall be timely if received within 10 days of the distribution of notice to LA citizens. Each day notice is not received by the state Attorney General shall be deemed a separate violation.
Maine	The Attorney General or Department of Professional and Financial Regulation if the entity is governed by that body must be notified regarding a breach.

States that Require Notice to Attorney General or State Agency	
Maryland	The Attorney General must be notified prior to notification of individuals.
Massachusetts	The Attorney General, Director of Consumer Affairs and Business Regulation, must be notified regarding a breach. Upon receipt of notice, the Director of Consumer Affairs and Business Regulation will identify any relevant Consumer Reporting Agency or state agency that needs to be notified to the notifying party.
Missouri	If 1,000 or more persons are affected, then the Attorney General must be notified regarding the timing, distribution and content of notice to individuals.
New Hampshire	A person engaged in trade or commerce shall notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the Attorney General's office. Notice to the Attorney General's office must include the anticipated date of the notice to the individuals and the approximate number of individuals in the state who will be notified. The names of the individuals entitled to receive notice do not have to be disclosed.
New Jersey	The Division of State Police in the Law Department of Law and Public Safety must be notified regarding a breach prior to notifying customers.
New York	The Attorney General, Consumer Protection Board, and the state Office of Cyber Security and Critical Infrastructure must be notified regarding a breach via form notice.
North Carolina	The Consumer Protection Division of the Attorney General's Office must be notified of the nature of the breach, the number of consumers affected, 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 via form notice.
Puerto Rico	The Department of Consumer Affairs must be notified regarding a breach as expeditiously as possible (within a non-extendable 10 days after the violation of the system is detected, parties shall inform the Department of Consumer Affairs, which shall make a public announcement of the fact within 24 hours of receiving information).
South Carolina	If 1,000 or more persons are affected, the Consumer Protection Division of the Department of Consumer Affairs must be notified regarding a breach.
Vermont	Once notice is made to consumers, the Attorney General must be notified of the number of Vermont consumers affected and provided a copy of the notice. A second copy of the consumer notification letter, with personally identifiable information that was subject to the breach redacted, can also be provided to the attorney general which will be used for any public disclosure of the breach. In the event a data collector provides notice to more than 1,000 consumers at one time pursuant to this section, the data collector shall notify, without unreasonable delay, all consumer reporting agencies. In notice to a consumer reporting agency, the data collector must include the timing, distribution, and

States that Require Notice to Attorney General or State Agency	
	content of the notices being sent to the affected consumers.
Virginia	Personal Information Breach Notification Statute: The Office of the Attorney General must be notified following discovery of a breach of personal information. In the event an individual or entity provides notice to more than 1,000 persons at one time, they must notify, without unreasonable delay, both the Office of the Attorney General and all consumer reporting agencies of the timing, distribution, and content of the notice sent to affected residents. Medical Information Breach Notification Statute: The Office of the Attorney General and the Commissioner of Health must be notified following discovery of a breach of medical information. The entity must notify both the subject of the medical information and any affected resident of the Commonwealth, if those are not the same person. In the event an entity provides notice to more than 1,000 persons at one time, they must notify, without unreasonable delay, the Office of the Attorney General and the Commissioner of Health of the timing, distribution, and content of the notice sent to affected individuals.

States that Require Notification within a Specific Time Frame (other than the general provision that notification must be given in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement).	
California	Medical Information Specific Breach Notification Statute: For clinics, health facilities, home health agencies, and hospices licensed pursuant to sections 1204, 1250, 1725, or 1745 of the California Health and Safety Code, the state's Medical Information Breach Notification statute may apply. The statute requires licensees to notify both affected patients and the California Department of Health Services no later than 5 business days after the unauthorized access, use, or disclosure has been detected by the licensee.
Connecticut	Pursuant to Bulletin IC-25 (Aug. 18, 2010), all licensees and registrants of the Connecticut Insurance Department are required to notify the Department of any information security incident which affects any Connecticut residents as soon as the incident is identified, but no later than five calendar days after the incident is identified.
Florida	Notice must be provided without unreasonable delay; no later than 45 days; law enforcement can delay notification.
Maine	If, after the completion of an investigation, notification is required under this section, 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.

States that Require Notification within a Specific Time Frame (other than the general provision that notification must be given in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement).	
Ohio	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 activities.
Vermont	Notice of the security breach to a consumer shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after discovery.
Wisconsin	Notice shall be provided within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination as to reasonableness shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.

States That Permit a Private Cause of Action	
Alaska	A person injured by a breach may bring an action against a non-governmental agency under the Unfair or Deceptive Act or Practices, AS 45.50.471 – 45.50.561.
California	Any customer injured by a violation of the general breach notification statute may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated this title may be enjoined.
Louisiana	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.
Maryland	Consumers may bring actions under Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act.
Massachusetts	Massachusetts consumers may seek damages under Chapter 93A, which allows for certain instances of treble damages.
Nevada	A private right of action exists for the data collector. A data collector that provides the requisite notice may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector.
New Hampshire	Persons injured as a result of a violation may bring an action for damages and for such equitable relief as the court deems necessary and proper. A prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees. An aggrieved individual whose health records were wrongly disclosed may bring a civil action under RSA 332-I:4 or RSA 332-I:5 and, if successful, shall be awarded special or general damages of not less than $1,000 for each

States That Permit a Private Cause of Action	
	violation, and costs and reasonable legal fees.
North Carolina	Provides a private right of action only if individual is injured as a result of the violation. Damages set at a maximum of up to $5,000, per incident, and provides for treble damages within this range. Injunctive relief also available.
Oregon	Compensation can be ordered by the state upon a finding that enforcement of the rights of consumers by private civil action would be so burdensome or expensive as to be impractical.
South Carolina	A resident of SC who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may: institute a civil action to recover damages in case of a willful and knowing violation; institute a civil action to recover only actual damages resulting from a violation in case of a negligent violation; seek an injunction to enforce compliance; and recover attorney's fees and court costs, if successful.
Tennessee	A violation under the data breach notification statute may also be a violation of the Tennessee Consumer Protection Act, which could give rise to a private cause of action.
Texas	A violation under the data breach notification statute may also be a violation of the Texas Deceptive Trade Practices Act, which could give rise to a private cause of action.
Virginia	Though generally enforced by the Attorney General, nothing in the data breach notification statute will preclude recovery of economic damages.
Washington	Any customer injured by a violation may institute a civil action to recover damages.
District of Columbia	Any District of Columbia resident injured by a violation may institute a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees. Actual damages shall not include dignitary damages, including pain and suffering.
Puerto Rico	Consumers may bring actions apart from the statute.
Virgin Islands	Any customer injured by a violation may commence a civil action to recover damages.

States With an Encryption Safe Harbor	
Alaska	The statute only applies to unencrypted information or encrypted information when the encryption key has also been disclosed.
Arizona	Notification requirement only applies where personal information was unencrypted.
Arkansas	Statute only applies to unencrypted data elements.

States With an Encryption Safe Harbor	
California	Notification under the general breach notification statute only applies where unencrypted personal information was acquired, or is believed to acquired, by an unauthorized person.
Colorado	Statute applies only to the disclosure of unencrypted computerized data.
Connecticut	A breach of security only occurs when access to the personal information has not been secured by encryption or by any other method or technology that renders personal information unreadable or unusable.
Delaware	The statute applies to unencrypted computerized data.
Florida	The statute applies to unencrypted information.
Georgia	The statute applies to unencrypted personal information.
Hawaii	The statute applies only to disclosure of unencrypted or unredacted information.
Idaho	The statute applies to unencrypted personal information.
Illinois	The statute applies to not encrypted personal information.
Indiana	The statute does not apply to encrypted information, provided that the unauthorized recipient of the information does not also get an encryption key.
Iowa	The statute does not cover personal information if it is "encrypted, redacted, or otherwise altered in such a manner that the name or data elements are unreadable."
Kansas	The statute is triggered by disclosure of unencrypted or unredacted information.
Louisiana	Notification requirement only applies where the personal information was not encrypted or redacted.
Maine	The statute only applies to disclosure of information that is not encrypted.
Maryland	The statute only applies to disclosure of personal information that has not been encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable.
Massachusetts	No notice is required as long as the data acquired or used is encrypted, and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information has not been acquired.
Michigan	A person or agency does not have to give notice if the resident's data was encrypted or redacted, and the person gaining unauthorized access did not have the encryption key.
Minnesota	A person or business must give notice of a security breach if personal information is acquired. Personal information does not include encrypted data.
Mississippi	Does not cover encrypted data.

States With an Encryption Safe Harbor	
Missouri	Personal information does not include information that is redacted, altered, or truncated such that no more than five digits of a social security number or the last four digits of a driver's license number, state identification card number, or account number is accessible as part of the personal information.
Montana	The statute applies only to disclosures of unencrypted information.
Nebraska	Notice is not required if data is encrypted or redacted.
Nevada	If the data is encrypted, notice is not required.
New Hampshire	If the data elements are encrypted, notification is not required.
New Jersey	Statute applies to personal information that has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.
New York	When the private information is encrypted and the encryption key has not been acquired, there is no duty to notify.
North Carolina	Notification requirement only applies where the personal information acquired is unencrypted and unredacted.
North Dakota	Notification is not required when data has been secured by encryption or by any other method or technology that renders the electronic files, media, or data bases unreadable or unusable.
Ohio	If the data is encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable, notification is not required.
Oklahoma	Notification is not required for encrypted or redacted information unless the encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state.
Oregon	If data is encrypted or redacted, notice is not required.
Pennsylvania	Notification is not required when encrypted or redacted information is accessed and acquired. Notice is required, however, if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.
Rhode Island	If the information is encrypted, notice is not required.
South Carolina	If data is rendered unusable through encryption, redaction, or other methods, notice to consumers is not required.
Tennessee	Notification requirement only applies where personal information was unencrypted.

States With an Encryption Safe Harbor	
Texas	"Sensitive personal information" only applies to data items that are not encrypted.
Utah	If the personal information is encrypted or protected by another method that renders the data unreadable or unusable, notice is not required.
Vermont	Data is not considered personal information if both the individual's name and the combined data element (i.e. social security number) are encrypted, redacted, or protected by another method that renders them unreadable or unusable.
Virginia	The unauthorized acquisition of encrypted or redacted data, without access to the encryption key, does not trigger the notice requirement under this statute.
Washington	If both an individual's first name or first initial and last name and accompanying data element (i.e. social security number) are encrypted, notice is not required.
West Virginia	If encrypted or redacted information is accessed and acquired and the person does not have access to the encryption key, notice is not required.
Wisconsin	If one of the data elements linked to an individual's name is encrypted, redacted, or altered in a manner that renders the element unreadable, it is not considered personal information, meaning no notice is required.
Wyoming	If both an individual's first name or first initial and last name and combined data element (i.e. social security number) are redacted, the data is not considered personal identifying information, and notice is not required.
District of Columbia	The acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party is not considered a breach of the security system.
Guam	Notification requirement does not apply to encrypted data unless the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of Guam.
Puerto Rico	This statute is triggered only when unencrypted information is disclosed.
Virgin Islands	Statute applies only where personal information was unencrypted.

States Where the Statute is Triggered by a Breach of Security in Electronic and/or Paper Records	
Alaska	"Breach of security" means unauthorized acquisition, or reasonable belief of unauthorized acquisition, or personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector. "Acquisition" includes: acquisition by photocopying, facsimile, or other paper-based method; a device including a computer, that can read, write or store information that is represented in

States Where the Statute is Triggered by a Breach of Security in Electronic and/or Paper Records	
	numerical form; or a method not identified by this paragraph.
Hawaii	This statute applies to 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.
Indiana	Breach of the security of data means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.
Massachusetts	Breach of security is 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. Data is any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.
North Carolina	Statute applies to any business that owns or licenses personal information in any form (whether computerized, paper or otherwise) or any business that maintains or possesses records or data containing personal information that the business does not own or license.
Wisconsin	This statute does not define a "breach of security", and its definition of "personal information" is not restricted to computerized information alone.

STATE DATA BREACH LAW COMPARISON

The following standard definitions of Personal Information and Breach of Security (based on the definition commonly used by most states) are used for ease of reference, and any variations from the common definition are noted:

Personal Information: An individual's first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state-issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media. In addition, Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Breach of Security: The unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information.

Please note that the following summary of state data breach statutes are not intended to be and should not be used as a substitute for reviewing the statutory language, nor do they constitute legal advice. If you find these charts helpful and require legal counsel, please contact BakerHostetler's Privacy and Data Protection Team www.bakerlaw.com/PrivacyDataProtection. Our blog can be found at: www.dataprivacymonitor.com.

The requirements for specific states are set forth on the following pages:

[1] Alabama, Kentucky, New Mexico, South Dakota, the Northern Marianas Islands, and American Samoa do not currently have a data breach statute.

State Statute	Alaska Alaska Stat. Tit. 45.48.010 et seq.
Personal Information Definition	Personal Information of Alaska residents. In addition: passwords, personal identification numbers, or other access codes for financial accounts.
Persons Covered	Any person doing business, government agency or person with more than 10 employees that owns, licenses or maintains unencrypted personal information about Alaska residents.
Encryption/ Notification Trigger	The statute only applies to unencrypted information or encrypted information when the encryption key has also been disclosed. **Standard for Triggering:** The statute is triggered when a covered person discovers or is notified of a breach of security. "Breach of security" means unauthorized acquisition, or reasonable belief of unauthorized acquisition, or personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector. "Acquisition" includes: acquisition by photocopying, facsimile, or other paper-based method; a device including a computer, that can read, write or store information that is represented in numerical form; or a method not identified by this paragraph. Notice is not required if, after an investigation and written notice to the Attorney General, the entity determines that there is not a reasonable likelihood that harm to the consumers has or will result. The determination must be documented in writing and maintained for five years.
Specific Content Requirements	N/A
Timing	Notification must be provided in the most expeditious time possible and without unreasonable delay, but may be delayed upon determination of law enforcement. If such a delay occurs, notification must be made after law enforcement determines that will not interfere with an investigation. If a breach of the security of the information system containing personal information of a state resident that is maintained by an information recipient occurs, the information recipient is not required to comply with AS 45.48.010 - 45.48.030. However, immediately after the information recipient discovers the breach, the information recipient shall notify the information distributor who owns the personal information or who licensed the use of the personal information to the information recipient about the breach and cooperate with the information distributor as necessary to allow the information distributor to comply with this statute. In this subsection, "cooperate" means sharing with the information distributor information relevant to the breach, except for confidential business information or trade secrets.
Penalty/Private Right	Governmental agencies are liable to the state for a civil penalty of up to $500 for each state resident who was not notified, but the total civil penalty

State Statute	Alaska Alaska Stat. Tit. 45.48.010 et seq.
of Action	may not exceed $50,000, and may be enjoined from further violations. If an information collector who is not a government agency violates AS 45.48.010-45.48.090 with regard to the personal information of a state resident, the violation is an unfair or deceptive act or practice under AS 45.50.471-45.50.561. The information collector is not subject to civil penalties imposed under 45.50.551 but is liable to the state for a civil penalty of up to $500 for each state resident who was not notified under AS 45.48.010-45.48.090, except that the total civil penalty may not exceed $50,000; and damages that may be awarded against the information collector under AS 45.50.531 are limited to actual economic damages that do not exceed $500. The Department of Administration may enforce (a) of the section against a government agency.
Other Provisions	If over 1,000 Alaska residents must be notified, the information collector must also notify all nationwide consumer reporting agencies (unless the information collector is subject to the Gramm-Leach-Bliley Financial Modernization Act).

State Statute	**Arizona** Ariz. Rev. Stat. § 44-7501 (2006), as amended (2007).
Personal Information Definition	Personal Information of Arizona residents.
Persons Covered	Any person that conducts business in Arizona and owns or licenses unencrypted computerized data or who maintains data that includes personal information that becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's personal information.
Encryption/ Notification Trigger	Notification requirement only applies where personal information was unencrypted. **Standard for Triggering:** The statute is triggered when the result of a reasonable investigation reveals that there has been a breach of the security system. "Breach of the security system" means unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security of personal information maintained by a person as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual. Notice is not required if the entity or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur.
Specific Content Requirements	N/A
Timing	In the most expedient manner possible without unreasonable delay subject to the needs of the law enforcement and any measures necessary to determine the nature and scope of the breach, to identify the individuals affected or to restore the reasonable integrity of the data system. A person that maintains unencrypted computerized data that includes personal information that the person does not own shall notify and cooperate with the owner or the licensee of the information of any breach of the security of the system following discovery of the breach without unreasonable delay. Cooperation shall include sharing information relevant to the breach of the security of the system with the owner or licensee. The person that owns or licenses the computerized data shall provide notice to the individual pursuant to this section. The person that maintained the data under an agreement with the owner or licensee is not required to provide notice to the individual pursuant to this section unless the agreement stipulates otherwise. Notification may be delayed if it would impede a criminal investigation.
Penalty/Private Right of Action	The section may be enforced only by the Attorney General, who may bring an action to obtain actual damages for a willful and knowing violation, and a civil penalty not to exceed $10,000 per breach or series of similar breaches discovered in a single investigation.
Other Provisions	N/A

State Statute	**Arkansas** Ark. Code Ann. §§ 4-110-101–108 (2005).
Personal Information Definition	Personal Information of Arkansas residents. In addition: medical information.
Persons Covered	Any person or business that acquires, owns, licenses or maintains computerized data that includes personal information about Arkansas residents.
Encryption/ Notification Trigger	The statute only applies to unencrypted data elements. **Standard for Triggering:** The statute is triggered upon discovery or notification of a Breach of the security of the system if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business. Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.
Specific Content Requirements	N/A
Timing	For persons/businesses that acquire, own or license data, disclosure shall be made in the most expedient time and manner 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 reasonable integrity of the data system. For persons/businesses that maintain computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Penalty/Private Right of Action	Any violation of this statute is punishable by action of the Attorney General. Any person who knowingly and willfully commits an unlawful practice under [the Personal Information Protection Act] shall be guilty of a Class A misdemeanor. The Attorney General has the authority, acting through the Consumer Counsel, to file an action for civil enforcement of the provisions of this chapter, including, but not limited to, the seeking of restitution and the seeking of an injunction prohibiting any person from engaging in any deceptive or unlawful practice prohibited by this statute.
Other Provisions	N/A

State Statute	California Cal. Civ. Code §§ 1280.15, 1798.29, 1798.80, 1798.82, 1798.84 (2003), as amended (2012).
Personal Information Definition	General Breach Notification Statute: Personal Information of California residents. In addition: medical information and health insurance information. Medical Information Specific Breach Notification Statute: Patients' medical information. "Medical information" means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or Social Security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.
Persons Covered	General Breach Notification Statute: Any state agency, person, or business that conducts business in California and own, licenses, or maintains computerized data that includes personal information. Medical Information Specific Breach Notification Statute: Clinics, health facilities, home health agencies, and hospices licensed pursuant to sections 1204, 1250, 1725, or 1745 of the California Health and Safety Code.
Encryption/ Notification Trigger	General Breach Notification Statute: The statute does not apply to encrypted personal information. **Standard for Triggering:** General Breach Notification Statute: The statute is triggered upon discovery or notification of a breach of the security of the system. "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the entity. Medical Information Specific Breach Notification Statute: The statute is triggered by any unlawful or unauthorized access to, or use or disclosure of a patient's medical information. "Unauthorized" means the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1 of the Civil Code) or any other statute or regulation governing the lawful access, use, or disclosure of medical information. Internal paper records, electronic mail, or facsimile transmissions inadvertently misdirected within the same facility or health care system within the course of coordinating care or delivering services shall not constitute unauthorized access to, or use or disclosure of, a patient's medical information.

State Statute	California Cal. Civ. Code §§ 1280.15, 1798.29, 1798.80, 1798.82, 1798.84 (2003), as amended (2012).
Specific Content Requirements	General Breach Notification Statute: Breach notification to CA residents must be written in plain language and include at least the following elements: (1) the date of the notice; (2) the name and contact information of the person reporting a breach; (3) a list of the types of personal information likely impacted; and (4) if the breach exposed a Social Security number or a driver's license or CA identification card number, the toll-free telephone numbers and addresses of the major credit reporting agencies. The notice must also include the following information if such information is possible to determine before sending the notice: (1) the date, estimated date, or date range of the breach; (2) whether notification was delayed as a result of a law enforcement investigation; and (3) a general description of the breach incident.
Timing	General Breach Notification Statute: Disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. If an entity maintains computerized data that includes personal information that the entity does not own, the entity must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Medical Information Specific Breach Notification Statute: Affected patients and the California Department of Health Services must be notified no later than 5 business days after the unauthorized access, use, or disclosure has been detected by the licensee. This notice can be delayed for law enforcement purposes so long as the delay is documented in accordance with the requirements of section 1280.15(c) of the California Health and Safety Code.
Penalty/Private Right of Action	General Breach Notification Statute: Any customer injured by a violation of § 1798.82 may institute a civil action to recover damages. Also, any business that violates or proposes to violate § 1798.82 may be enjoined. Safe Harbor Exception for a record custodian who properly disposes of records: (1) A cause of action shall not lie against a business for disposing of abandoned records containing personal information by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means. (2) The Legislature finds and declares that when records containing personal information are abandoned by a business, they often end up in the possession of a storage company or commercial landlord. Medical Information Specific Breach Notification Statute: The California Department of Health Services may impose the following penalties against

State Statute	California Cal. Civ. Code §§ 1280.15, 1798.29, 1798.80, 1798.82, 1798.84 (2003), as amended (2012).
	licensees who violate section 1280.15: (1) $25,000 per patient whose information was unlawfully or without authorization accessed, used or disclosed, and up to $17,500 per subsequent occurrence. In determining the amount of the penalty, the Department must consider the entity's history of compliance with this section and related state and federal legislation, the extent to which the entity detected the violations and took corrective actions, and factor's outside the entity's control which may have prevented compliance; (2) entities that fail to report the incident to the State Department of Health Services or the affected patients within the 5 day time period absent lawful delay are subject to a penalty of $100 per day; and (3) the total penalties imposed may not exceed $250,000 per reported event.
Other Provisions	General Breach Notification Statute: Any person who notifies more than 500 California residents as a result of a single breach must electronically submit a single sample copy of the notification letter to the Attorney General. Medical Information Specific Breach Notification Statute: The California Department of Health Services must be notified no later than 5 business days after the unauthorized access, use, or disclosure has been detected by the licensee.

State Statute	Colorado Colo. Rev. Stat. Ann. § 6-1-716 (2006); as amended (2010).
Personal Information Definition	Personal Information of Colorado residents.
Persons Covered	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; an individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license . . .
Encryption/ Notification Trigger	The statute only applies to the disclosure of unencrypted computerized data. **Standard for Triggering:** The statute is triggered when an individual or commercial entity becomes aware of a breach of the security of the system containing a Colorado resident's personal information. "Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Notification is not required if after a good-faith, prompt and reasonable investigation, the entity determines that misuse of personal information about a Colorado resident has not occurred and is not likely to occur.
Specific Content Requirements	N/A
Timing	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. An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a Colorado resident occurred or is likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets.
Penalty/Private Right of Action	The Attorney General may bring an action in law or equity to address violations of this statute and for other relief that may be appropriate to ensure compliance with this statute or to recover direct economic damages resulting from a violation, or both.
Other Provisions	N/A

State Statute	Connecticut Conn. Gen. Stat. § 36a-701b (2005); as amended (2012)
Personal Information Definition	Personal Information of Connecticut residents.
Persons Covered	Any person, business or agency that conducts business in Connecticut, and who, in the ordinary course of such entity's business, owns, licenses, or maintains computerized data that includes personal information.
Encryption/ Notification Trigger	A breach of security only occurs when access to the personal information has not been secured by encryption or by any other method or technology that renders personal information unreadable or unusable. **Standard for Triggering:** The statute is triggered upon discovery of a breach of security. "Breach of security" means 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. Notification is not required if, after a reasonable investigation and consultation with relevant law enforcement agencies, it is determined that there is no reasonable likelihood of harm to customers.
Specific Content Requirements	N/A
Timing	The disclosure shall be made without unreasonable delay, consistent with any measures necessary to determine the nature and scope of the breach, to identify individuals affected, or to restore the reasonable integrity of the data system. Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery, if the personal information was, or is reasonably believed to have been accessed by an unauthorized person.
Penalty/Private Right of Action	Failure to comply with this statute constitutes unfair trade practices for the purposes of § 42-110b, and is enforced by the Attorney General.
Other Provisions	The Connecticut Attorney General must be notified following a breach of security no later than the time when notice is provided to affected residents. Pursuant to Bulletin IC-25 (Aug. 18, 2010), all licensees and registrants of the Connecticut Insurance Department are required to notify the Department of any information security incident which affects any Connecticut residents as soon as the incident is identified, but no later than five calendar days after the incident is identified. Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state regulator is sufficient for compliance.

State Statute	Delaware Del. Code Ann. tit. 6, § 12B-101–104 (2005).
Personal Information Definition	Personal Information of Delaware residents.
Persons Covered	An individual or commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware, or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license.
Encryption/ Notification Trigger	The statute only applies to unencrypted computerized data. **Standard for Triggering:** The statute is triggered when an individual or entity covered by the statute becomes aware of a breach of the security of the system, and as a result of the breach, misuse of information about a Delaware resident has occurred or is likely to occur. "Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.
Specific Content Requirements	N/A
Timing	Notice must 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. An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a Delaware resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.
Penalty/Private Right of Action	Pursuant to the enforcement duties and powers of the Consumer Protection Division of the Department of Justice under Chapter 25 of Title 29, the Attorney General may bring an action in law or equity to address 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 statute are not exclusive and do not relieve an individual or a commercial entity subject to this statute from compliance with all other applicable provisions of law.
Other Provisions	N/A

State Statute	Florida Fla. Stat. Ann. § 817.5681 (2005).
Personal Information Definition	Personal Information of Florida residents.
Persons Covered	Any person who conducts business in Florida and maintains computerized data in a system that includes personal information and any person who maintains computerized data that includes personal information on behalf of another business entity.
Encryption/ Notification Trigger	The statute only applies to unencrypted information. **Standard for Triggering:** The statute is triggered upon a determination of the breach of the security system. "Breach of the security of the system" means unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person. Notification is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for 5 years.
Specific Content Requirements	N/A
Timing	Notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement . . .or subject to any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system. Notification must be made no later than 45 days following the determination of the breach unless otherwise provided in this section. Any entity that maintains computerized data that includes personal information on behalf of another business entity shall disclose to the business entity for which the information is maintained any breach of the security of the system as soon as practicable, but no later than 10 days following the determination, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The entity that maintains the data on behalf of another business entity and the business entity on whose behalf the data is maintained may agree who will provide the notice, if any is required, provided only a single notice for each breach of the security system shall be required. If agreement regarding notification cannot be reached, the entity which has the direct business relationship with the Florida resident shall be subject to these provisions.

State Statute	Florida Fla. Stat. Ann. § 817.5681 (2005).
Penalty/Private Right of Action	Any owner or licensor of personal information 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, as follows: (1) In the amount of $1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,000 for each 30-day period or portion thereof for up to 180 days; (2) If notification is not made within 180 days, any person required to make notification who fails to do so is subject to an administrative fine of up to $500,000. Anyone who maintains information who is required to notify the owner or licensor of the information who fails to do so within 10 days after the determination of a breach or receipt of notification from law enforcement is liable for an administrative fine not to exceed $500,000, as follows: (1) In the amount of $1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,000 for each 30-day period or portion thereof for up to 180 days; (2) If disclosure is not made within 180 days, any person required to make disclosures who fails to do so is subject to an administrative fine of up to $500,000.
Other Provisions	N/A

State Statute	Georgia Ga. Code Ann. § 10-1-910–912 (2005), as amended (2007).
Personal Information Definition	Personal Information of Georgia residents. In addition: a password and any of the data elements not in connection with the name if any of the other data elements alone would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.
Persons Covered	Any information broker or data collector that maintains computerized data or any person or business that maintains computerized data on behalf of an information broker or data collector. “Data collector” means any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity; provided, however, that the term “data collector” shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information. “Information broker” means any person or entity 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 third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.
Encryption/ Notification Trigger	The statute only applies to unencrypted personal information. **Standard for Triggering:** The statute is triggered when a person covered by the statute becomes aware of a breach of the security of the system. “Breach of the security of the system” means unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker or data collector. Good faith acquisition or use of personal information by an employee or agent of an information broker or data collector for the purposes of such information broker or data collector is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
Specific Content Requirements	N/A
Timing	Notice must be given in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own shall notify the information broker or data collector of any breach of the security of the system within 24 hours following discovery, if the personal information was,

State Statute	Georgia Ga. Code Ann. § 10-1-910–912 (2005), as amended (2007).
	or is reasonably believed to have been acquired by an unauthorized person.
Penalty/Private Right of Action	N/A
Other Provisions	In the event that an information broker or data collector discovers circumstances requiring notification of more than 10,000 residents one time, the information broker or data collector shall also notify, without unreasonable delay, all consumer reporting agencies.

State Statute	Hawaii Haw. Rev. Stat. § 487N-1–4 (2006).
Personal Information Definition	Personal Information of Hawaii residents.
Persons Covered	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 and to any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii.
Encryption/ Notification Trigger	The statute only applies to disclosure of unencrypted or unredacted information. **Standard for Triggering:** The statute is triggered upon discovery or notification of a security breach. "Security breach" means 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 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 shall constitute a security breach. Notification is not required if the business determines after a reasonable investigation that there is no reasonable likelihood of harm.
Specific Content Requirements	The notice shall be clear and conspicuous and shall include a description of the following: (1) the incident in general terms; (2) the type of personal information that was subject to the unauthorized access and acquisition; (3) the general acts of the business or government agency to protect the personal information from further unauthorized access; (4) a telephone number that the person may call for further information and assistance, if one exists; and (5) advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.
Timing	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, the scope of the breach, and to restore the reasonable integrity, security, and confidentiality of the data system. Any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, shall notify the owner or licensee of the personal information of any security breach immediately following discovery of the breach.

State Statute	**Hawaii** Haw. Rev. Stat. § 487N-1–4 (2006).
Penalty/Private Right of Action	Any business that violates any provision of this chapter shall be subject to 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. Any business that violates any provision of this chapter shall be liable to the injured party in 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. The penalties provided in this section shall be cumulative to the remedies or penalties available under all other laws of this State.
Other Provisions	Notice of the timing, content and distribution of the notice must be given to the Hawaii office of Consumer Protection if over 1,000 persons are affected.

State Statute	**Idaho** Idaho Code Ann. § 28-51-104–107 (2006).
Personal Information Definition	Personal Information of Idaho residents.
Persons Covered	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 or an agency; individual or a commercial entity that maintains computerized data that includes personal information that the agency, individual or the commercial entity does not own or license.
Encryption/ Notification Trigger	The statute only applies to unencrypted personal information. **Standard for Triggering:** The statute is triggered when a person covered by the statute becomes aware of a breach of the security of the system. "Breach of the security of the system" means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one or more persons maintained by an agency, individual or a commercial entity. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident.
Specific Content Requirements	N/A.
Timing	Notice must 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, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system. An entity that maintains computerized data that includes personal information that the entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of the breach, if misuse of PI about an ID resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach. 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.
Penalty/Private Right of Action	In any case in which an agency's, commercial entity's or individual's primary regulator has reason to believe that an agency, individual or commercial entity fails to give, the primary regulator may bring a civil action to enforce compliance with that section and enjoin that agency, individual or commercial entity from further violations.

State Statute	Idaho Idaho Code Ann. § 28-51-104–107 (2006).
	Any agency, individual, or commercial entity that intentionally fails to give notice in accordance with section 28-51-105, Idaho Code, shall be subject to a fine of not more than twenty-five thousand dollars ($25,000) per breach of the security of the system. Any governmental employee that intentionally discloses personal information not subject to disclosure otherwise allowed by law, is guilty of a misdemeanor and, upon conviction thereof, shall be punished by a fine of not more than two thousand dollars ($2,000), or by imprisonment in the county jail for a period of not more than one (1) year, or both.
Other Provisions	Only public agencies are required to provide notice to the Idaho Attorney General, and they must do so within 24 hours. The agency must also 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.

State Statute	Illinois 815 Ill. Comp Stat. Ann. 530/1–/30 (2006)
Personal Information Definition	Personal Information of Illinois residents.
Persons Covered	Any data collector that owns or licenses personal information concerning an Illinois resident and any data collector that maintains computerized data that includes personal information that the data collector does not own or license. “Data collector” means government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.
Encryption/ Notification Trigger	The statute only applies to personal information that is not encrypted. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach of the security system. “Breach of security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.
Specific Content Requirements	Notice must include contact information for credit reporting agencies and the Federal Trade Commission, along with a statement that the individual can obtain information from these sources about fraud alerts and security freezes. Notice must not include information concerning the number of Illinois residents affected by the breach.
Timing	Notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. Any entity that maintains computerized data that includes personal information that the entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Penalty/Private Right of Action	Violations constitute an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act. Violations are subject to a civil penalty of not more than $100 for each individual with respect to whom personal information is disposed of in violation. A civil penalty may not exceed $50,000 for each instance of improper disposal. The Attorney General may impose a civil penalty after notice to the person accused of violating this section. In addition, the Attorney General may bring an action in the circuit court to remedy a violation, seeking appropriate relief.

State Statute	**Illinois** 815 Ill. Comp Stat. Ann. 530/1–/30 (2006)
Other Provisions	Any state agency that collects personal information and has had a breach of security of the system data or written material shall submit a report within five 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 agency that has submitted a report under the statute 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. Data collectors or service providers who maintain or store but do not own or license personal information must cooperate with the data owner or licensor with respect to breaches of personal information in the service provider's care. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

State Statute	Indiana Ind. Code Ann. §§ 24-4.9 et seq.; § 4-1-11 et seq. (2006), as amended (2009)
Personal Information Definition	Personal Information of Indiana residents, including: a Social Security number that is not encrypted or redacted.
Persons Covered	Businesses and state agencies who are data base owners or a person who maintains computerized data. "Data base owner" means a person that owns or licenses computerized data that includes personal information.
Encryption/ Notification Trigger	The statute does not apply to encrypted information, provided that the unauthorized recipient of the information does not also get an encryption key. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach of the security of data. "Breach of the security of data" means unauthorized acquisition of computerized data that has been transferred to another medium, including paper, microfilm, or a similar media, even if the transferred data are no longer in a computerized format. Persons/Businesses: Breach defined as unauthorized acquisition of unencrypted personal information by an unauthorized user, or acquisition of encrypted personal information by an unauthorized person with access to the encryption key. Disclosure is required by the persons/businesses if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft, or fraud affecting the Indiana resident. State Agencies: a breach is defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a state or local agency. Disclosure is required by state agency if personal information was or is reasonably believed to have been acquired by an unauthorized person.
Specific Content Requirements	N/A
Timing	Persons/Businesses: A person required to make a disclosure or notification under this chapter shall make the disclosure or notification without unreasonable delay. For purposes of this section, a delay is reasonable if the delay is: (1) necessary to restore the integrity of the computer system; (2) necessary to discover the scope of the breach; or (3) in response to a request from the Attorney General or a law enforcement agency to delay disclosure because disclosure will: (A) impede a criminal or civil investigation; or (B) jeopardize national security. State Agencies: Notice must be made without unreasonable delay;

State Statute	Indiana Ind. Code Ann. §§ 24-4.9 et seq.; § 4-1-11 et seq. (2006), as amended (2009)
	consistent with: (1) legitimate needs of law enforcement; (2) any measures necessary to determine the scope of the breach; and (3) any measures necessary to restore the reasonable integrity of the data system. An entity that maintains computerized data that includes personal information but that does not own or license the personal information shall notify the owner of the personal information if the entity discovers that personal information was or may have been acquired by an unauthorized person. A person required to make a disclosure or notification under this chapter shall make the disclosure or notification as soon as possible after: (1) delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach; or (2) the Attorney General or a law enforcement agency notifies the person that delay will no longer impede a criminal or civil investigation or jeopardize national security.
Penalty/Private Right of Action	A person that is required to make a disclosure or notification in accordance with IC 24-4.9-3 and that fails to comply with any provision of this article commits a deceptive act that is actionable only by the Attorney General under this chapter. A failure to make a required disclosure or notification in connection with a related series of breaches of the security of data constitutes one (1) deceptive act. The Attorney General may bring an action under this chapter to obtain any or all of the following: (1) An injunction to enjoin future violations of IC 24-4.9-3. (2) A civil penalty of not more than one hundred fifty thousand dollars ($150,000) per deceptive act. (3) The Attorney General's reasonable costs in: (A) the investigation of the deceptive act; and (B) maintaining the action.
Other Provisions	If a data base owner is required to notify, the data base owner must also disclose the breach to the Attorney General.

State Statute	**Iowa** Ia.Code Ann. §§ 715C.1 et. seq. (2008).
Personal Information Definition	Personal Information of Iowa residents. In addition: a 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; unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.
Persons Covered	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 or who maintains or otherwise possesses personal information on behalf of another person.
Encryption/ Notification Trigger	Data is not covered personal information if it is encrypted, redacted, or otherwise altered in such a manner that the name or data elements are unreadable. **Standard for Triggering:** The statute is triggered upon discovery of a breach of security or upon notification of a breach of security by a data licensee. "Breach of security" means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. Notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial 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.
Specific Content Requirements	Notice must include, at a minimum, all of the following: (a) a description of the breach of security. (b) the approximate date of the breach of security. (c) the type of personal information obtained as a result of the breach of security. (d) contact information for consumer reporting agencies. (e) advice to the consumer to report suspected incidents of identity theft to local law enforcement or the Attorney General.
Timing	The consumer notification must be made in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data. Any person who maintains or otherwise possesses personal information on behalf of another person shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach of security if a consumer's personal information was included in the information that was breached.

State Statute	**Iowa** Ia.Code Ann. §§ 715C.1 et. seq. (2008).
Penalty/Private Right of Action	Violations are an unlawful practice under Iowa's Consumer Fraud Statute. Consequences include damages for injury and a fine of up to $40,000 per violation.
Other Provisions	N/A

State Statute	**Kansas** Kan. Stat. Ann. §§ 50-7a01 & 7a02 (2006).
Personal Information Definition	Personal Information of Kansas residents. In addition: an account number or credit card/debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account.
Persons Covered	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 or an individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license.
Encryption/ Notification Trigger	The statute only applies to unencrypted or unredacted information. **Standard for Triggering:** The statute is triggered when a person becomes aware of any breach of the security of the system. "Breach of the security of the system" means 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. Any entity to which the statute applies shall, when it becomes aware of any breach of the security of the system, 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.
Specific Content Requirements	N/A
Timing	Notice must 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. An entity that maintains computerized data that includes personal information that the entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the data following discovery of a breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.

State Statute	**Kansas** Kan. Stat. Ann. §§ 50-7a01 & 7a02 (2006).
Penalty/Private Right of Action	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. 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.
Other Provisions	N/A

State Statute	**Louisiana** La. Rev. Stat. § 51:3071-3077 (2005) L.A.C. 16:III.701
Personal Information Definition	Personal Information of Louisiana residents.
Persons Covered	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 who discovers a breach in the security system containing such data as well as any agency or person that maintains computerized data that includes personal information that the agency or person does not own.
Encryption/ Notification Trigger	Notification requirement only applies where the personal information was not encrypted or redacted. **Standard for Triggering:** The statute is triggered upon discovery of a breach of the security of the system containing personal information. "Breach of the security of the system" is defined as compromise of the computerized data such that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information. Notification is not required if after reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers.
Specific Content Requirements	N/A
Timing	Notification must be provided 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, prevent further disclosures, and restore integrity of the data system. Notification may be delayed if law enforcement determines that notification would impede a criminal investigation. Any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity that maintains computerized data that includes personal information that the agency or person does not own shall notify the owner or licensee of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of the security system.
Penalty/Private Right of Action	A civil action may be brought to recover actual damages resulting from the failure to disclose in a timely manner to a person that there was a breach of the security system resulting in disclosure of the person's personal information. Failure to provide timely notice may be punishable by a fine not to exceed $ 5,000 per violation. Notice to the Consumer Protection Section of 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.

State Statute	**Louisiana** La. Rev. Stat. § 51:3071-3077 (2005) L.A.C. 16:III.701
Other Provisions	The Consumer Protection Section of the Louisiana Attorney General must be notified regarding a breach within 10 days of distribution of notice to affected individuals. Notice shall include names of all Louisiana citizens affected.

State Statute	Maine Me. Rev. Stat. Ann. tit. 10, § 1346–49 (2005); as amended (2006).
Personal Information Definition	Personal Information of Maine residents. In addition: a password, if any of the other data elements alone would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.
Persons Covered	Information brokers and other persons as well as third party entities that maintain computerized data. "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.
Encryption/ Notification Trigger	The statute only applies to disclosure of information that is not encrypted. **Standard for Triggering:** The statute is triggered when a person covered by the statute becomes aware of a breach of the security of the system. “Breach of the security of the system” is defined as the compromise of the computerized data such that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition, release, use and access to personal information. Notification is not required if after conducting a good-faith, reasonable and prompt investigation, the entity determines that there is not a reasonable likelihood that the personal information has been or will be misused.
Specific Content Requirements	N/A
Timing	Notice must be made as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data in the system. If, after the completion of an investigation required by subsection 1, notification is required under this section, 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. A third party entity that maintains, on behalf of a person, computerized data that includes personal information that the 3rd-party entity does not own shall notify the person maintaining personal information of a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Penalty/Private Right of Action	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. 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 statute for all other persons.
Other Provisions	Notice must be provided to the Attorney General or Department of Professional and Financial Regulation if the entity is governed by that body.

State Statute	**Maryland** Md. Code Ann., Com. Law § 14-3501–3508 (2007).
Personal Information Definition	Personal Information of Maryland residents. In addition: an individual Taxpayer Identification Number.
Persons Covered	A business that owns or licenses computerized data that includes personal information of an individual residing in the State; a business that maintains computerized data that includes personal information that the business does not own or license.
Encryption/ Notification Trigger	The statute only applies to disclosure of personal information that has not been encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable. **Standard for Triggering:** The statute is triggered when an entity to which the statute applies discovers or is notified of a breach of the security of the system. "Breach of the security of the system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by an entity. Notification is not required if after a good-faith, reasonable and prompt investigation the entity determines that the personal information of the individual was not and will not be misused as a result of the breach. If after the investigation is concluded, the entity determines that notification is not required, the entity shall maintain records that reflect its determination for three years after the determination is made.
Specific Content Requirements	The notification required under subsection (b) of this section shall include: (1) to the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired; (2) contact information for the business making the notification, including the business' address, telephone number, and toll-free telephone number if one is maintained; (3) the toll-free telephone numbers and addresses for the major consumer reporting agencies; and (4)(i) the toll-free telephone numbers, addresses, and website addresses for: 1. the Federal Trade Commission; and 2. the Office of the Attorney General; and (ii) a statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft.
Timing	Notification shall be given as soon as reasonably practicable after the business conducts the investigation required under paragraph (1) of this subsection. An entity that maintains computerized data that includes personal information that the entity does not own or license shall notify the owner or licensee of the personal information of a breach of the security of the system if it is likely that the breach has resulted or will result in the misuse of personal information of an individual residing in MD. Notification required by a third-party entity shall be given as soon as reasonably practicable after

State Statute	**Maryland** Md. Code Ann., Com. Law § 14-3501–3508 (2007).
	the entity discovers or is notified of the breach of the security of a system. A third-party entity shall share with the owner or licensee information relative to the breach.
Penalty/Private Right of Action	A violation of this subtitle: (1) is an unfair or deceptive trade practice within the meaning of Title 13 of this article; and (2) is subject to the enforcement and penalty provisions contained in Title 13 of this article.
Other Provisions	Maryland requires businesses to follow reasonable procedures to guard against data breaches: (a) In this section, “customer” means an individual residing in MD who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business. (b) When a business is destroying a customer's records that contain personal information of the customer, the business shall take reasonable steps to protect against unauthorized access to or use of the personal information, taking into account: (1) the sensitivity of the records; (2) the nature and size of the business and its operations; (3) The costs and benefits of different destruction methods; and (4) Available technology. Notification to the Attorney General is required prior to notifying individuals.

State Statute	**Massachusetts** Mass. Gen. Laws Ann. ch. 93H, §§ 1–6 (2007). Mass. Gen. Laws Ann. ch. 93A, § 4 (2007).
Personal Information Definition	Personal Information of Massachusetts residents. In addition: financial account information with or without password or security code information. This includes non-electronic personal information.
Persons Covered	A person or agency that maintains, stores, owns or licenses personal information about a resident of the commonwealth, and that knows or has reason to know of a breach of security or that 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.
Encryption/ Notification Trigger	Encryption is a safe harbor to the definition of breach of security. **Standard for Triggering:** The statute is triggered when the person or agency knows or has reason to know of a breach of security or 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. "Breach of security" means 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. "Data" means any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics. The breach must create a substantial risk of identity theft or fraud against a resident of the commonwealth or 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.
Specific Content Requirements	Notice to be provided to Massachusetts residents shall include, but not be limited to: (1) the consumer's right to obtain a police report; (2) how a consumer requests a security freeze and the necessary information to be provided when requesting a security freeze; and (3) any fees required to be paid to any of the consumer reporting agencies, provided the said notification doesn't include the nature of the unauthorized acquisition or the number of Massachusetts residents affected by it. The contents of notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents affected by said breach or unauthorized access or use. Notice provided to the AG, director of consumer affairs, and consumer reporting agencies or state agencies, if any, shall include, but not be limited to: (1) the nature of the breach of security or unauthorized acquisition or use; (2) the number of residents of Massachusetts affected by such incident at the time of notification; and (3) any steps the entity has taken or plans to take relating to the incident.

State Statute	**Massachusetts** Mass. Gen. Laws Ann. ch. 93H, §§ 1–6 (2007). Mass. Gen. Laws Ann. ch. 93A, § 4 (2007).
Timing	Notice must be given as soon as practicable without unreasonable delay. A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of MA, shall provide notice, as soon as practicable and without unreasonable delay, when such entity (i) knows or has reason to know of a breach of security or (ii) when the entity 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 owner or licensor.
Penalty/Private Right of Action	The Attorney General may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate. Mass. Gen. Laws Ann. ch. 93A, § 4 permits the Attorney General to bring an action in the commonwealth's name. The Attorney General may seek injunctive relief, a $5,000 penalty for each violation, and reasonable costs and attorney's fees.
Other Provisions	Notification must be made to the Attorney General, Director of Consumer Affairs and Business Regulation. Upon receipt of notice, the Director of Consumer Affairs and Business Regulation will identify any relevant Consumer Reporting Agency or state agency that needs to be notified to the notifying party. **Regulations to safeguard personal information**: This provision requires the department of consumer affairs and business regulation, the supervisor of records, and relevant Massachusetts governmental entities to create rules and regulations designed to safeguard the personal information of residents of the commonwealth. **Responsibilities of Director of Consumer Affairs and Business Regulation:** Upon receipt of the person or agency's notice of a breach or unauthorized access, the director of consumer affairs and business regulation shall identify the relevant consumer reporting or state agencies, and forward the names of these agencies to the notifying person or agency. **Applicability of other state and federal laws:** A person or agency is not relieved from the duty to comply with requirements of any applicable or special law or federal law regarding the protection and privacy of personal information provided: (1) following the applicable law's procedures means compliance with this chapter, and (2) the person or agency notifies the Attorney General and director of the office of consumer affairs and business regulation of the breach, including any steps the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines.

State Statute	Michigan Mich. Comp. Laws Ann. §§ 445.63, 445.65, 445.72 (2006).
Personal Information Definition	Personal Information of Michigan residents.
Persons Covered	A person or agency that owns or licenses data included in a database that discovers a security breach, or receives notice of a security breach; a person or agency that maintains a database that includes data that the person or agency does not own or license that discovers a breach of the security of the database.
Encryption/ Notification Trigger	A person or agency does not have to give notice if the resident's data was encrypted or redacted, and the person gaining unauthorized access did not have the encryption key. **Standard for Triggering:** The statute is triggered upon discovery or notification of a security breach. "Security breach" and/or "breach of the security of the database" mean 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. The person or agency does not have to provide notice if 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, one or more residents of Michigan. In making this determination, a person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.
Specific Content Requirements	Notice must be written or communicated in a clear and conspicuous manner and contain the following: (1) a description of the security breach in general terms; (2) a description of the type of personal information that is the subject of the unauthorized access or use; (3) a general description of what the agency or person providing the notice has done to protect data from further security breaches; (4) a telephone number where a notice recipient may obtain assistance or additional information; and (5) a reminder to notice recipients of the need to remain vigilant for incidents of fraud and identity theft.
Timing	A person or agency shall provide any notice required under this section without unreasonable delay. However, a person or agency may delay providing notice if it is necessary to determine the scope of the security breach and restore the reasonable integrity of the database, or if a law enforcement agency determines that providing notice would impede an investigation or jeopardize homeland or national security. An entity that maintains a database that includes data that the entity does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the security breach, unless the entity determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity

State Statute	Michigan Mich. Comp. Laws Ann. §§ 445.63, 445.65, 445.72 (2006).
	theft with respect to one or more residents of Michigan.
Penalty/Private Right of Action	A person that knowingly fails to provide any notice of a security breach may be ordered to pay a civil fine of not more than $250 for each failure to provide notice. The aggregate liability for civil fines for multiple violations shall not exceed $750,000. The Attorney General or a prosecuting attorney may bring an action to recover a civil fine. A person that provides notice of a security breach when a security breach has not occurred, with the intent to defraud, is guilty of a misdemeanor punishable as follows: (a) Except as otherwise provided under subdivisions (b) and (c), by imprisonment for not more than 93 days or a fine of not more than $250.00 for each violation, or both. (b) For a second violation, by imprisonment for not more than 93 days or a fine of not more than $500.00 for each violation, or both. (c) For a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than $750.00 for each violation, or both.
Other Provisions	N/A

State Statute	**Minnesota** Minn. Stat. Ann. §§ 325E.61, 8.31 (2005), as amended (2007).
Personal Information Definition	Personal Information of Minnesota residents.
Persons Covered	Any person or business that conducts business in the State of Minnesota, and that owns or licenses data that includes personal information, and discovers a breach of the security of the data. Any person or business that maintains data that includes personal information that the person or business does not own, and discovers a breach of the security of the data.
Encryption/ Notification Trigger	Personal information does not include encrypted data. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach of the security of the system. "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.
Specific Content Requirements	N/A
Timing	Notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system. Any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Penalty/Private Right of Action	The Attorney General shall enforce this section by seeking injunctive relief and/or a civil penalty for the state not to exceed $25,000.
Other Provisions	For a breach affecting over 500 people (1,000 for state agencies), consumer reporting agencies must be notified within 48 hours. When notifying a consumer reporting agency, a person or business must include the timing, distribution, and content of the notices being sent to the Minnesota residents. This section does not apply to any "financial institution" as defined by United States Code, title 15, section 6809(3).

State Statute	**Mississippi** Miss. Code Ann. § 75-24-29 (2010).
Personal Information Definition	Personal Information of Mississippi residents.
Persons Covered	Any person who conducts business in this state and who, in the ordinary course of the person's business functions, owns, licenses or maintains personal information of any resident of this state.
Encryption/ Notification Trigger	The statute does not apply to encrypted data. **Standard for Triggering:** The statute is triggered by any breach of security. “Breach of security” means 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 Notification is not required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.
Specific Content Requirements	N/A
Timing	If required, disclosure must be made without unreasonable delay subject to 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. Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation or national security and the law enforcement agency has made a request that the notification be delayed. A person who maintains computerized data which includes personal information that the person does not own or license shall notify the owner or licensee of the information of any breach of security as soon as practical following its discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes
Penalty/Private Right of Action	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.
Other Provisions	N/A

State Statute	Missouri Mo. Rev. Stat. § 407.1500 (2009).
Personal Information Definition	Personal Information of Missouri residents. In addition: a unique electronic identifier or routing code in combination with required security code, access code, or password that would permit access to an individual's financial account; medical and health insurance information, including an individual's medical history, mental or physical condition, treatment or diagnosis, health insurance policy number and any other unique identifier used by a health insurer.
Persons Covered	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; any person that maintains or possesses records or data containing personal information of residents of Missouri that the person does not own or license; or any person that conducts business in Missouri that maintains or possesses records or data containing personal information of a resident of Missouri that the person does not own or license.
Encryption/ Notification Trigger	Personal information does not include encrypted data or information that is redacted, altered, or truncated such that no more than five digits of a Social Security number, or the last four digits of a driver's license number, state identification card number, or account number is accessible as part of the personal information. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach of security. "Breach of security" means 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. Notification is not required if, after an appropriate investigation by the person or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the documentation shall be maintained for five years.
Specific Content Requirements	The Notice shall, at minimum, include a description of the following: (a) the incident in general terms; (b) the type of personal information that was obtained as a result of the breach of security; (c) a telephone number that the affected consumer may call for further information and assistance, if one exists; (d) contact information for consumer reporting agencies; and (e) advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.
Timing	For an owner of personal information, the disclosure notification shall be: (a) made without unreasonable delay; (b) consistent with the legitimate needs of law enforcement, as provided in this section; and (c) consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the

State Statute	**Missouri** Mo. Rev. Stat. § 407.1500 (2009).
	reasonable integrity, security, and confidentiality of the data system. For any person that maintains or possesses records or data containing personal information of residents of Missouri that the person does not own or license, or any person that conducts business in Missouri that maintains or possesses records or data containing personal information of a resident of Missouri that the person does not own or license, shall notify the owner or licensee of the information of any breach of security immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in this section.
Penalty/Private Right of Action	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.
Other Provisions	If 1,000 or more persons are affected, both the Attorney General and Consumer Reporting Agencies must be notified of the timing, distribution and content of notice sent to affected individuals.

State Statute	**Montana** Mont. Code Ann. §§ 30-14-1701–02 & 1704 (2005), as amended (2009).
Personal Information Definition	Personal Information of Montana residents.
Persons Covered	Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information; any person or business that maintains computerized data that includes personal information that the person or business does not own.
Encryption/ Notification Trigger	The statute only applies to unencrypted information. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach of security. "Breach of security" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information and causes or is reasonably believed to cause loss or injury to a Montana resident.
Specific Content Requirements	N/A
Timing	Notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data system immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person.
Penalty/Private Right of Action	Whenever the Montana Attorney General has reason to believe that a person has violated this part and that proceeding would be in the public interest, the department may bring an action in the name of the state against the person to restrain by temporary or permanent injunction or temporary restraining order the use of the unlawful method, act, or practice upon giving appropriate notice to that person pursuant to 30-14-111(2). A violation of this part is a violation of 30-14-103, and the penalties for a violation of this part are as provided in 30-14-142; including a civil fine of not more than $10,000 for each violation.
Other Provisions	N/A

State Statute	**Nebraska** Neb. Rev. Stat. §§ 87-802 to -806 (2006).
Personal Information Definition	Personal Information of Nebraska residents. In addition: a unique electronic identification number or routing code, in combination with any required security code, access code, or password; or unique biometric data, such as finger print, voice print, or retina or iris image, or other unique physical representation.
Persons Covered	An individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska; an individual or commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license.
Encryption/ Notification Trigger	Notice is not required if data is encrypted or redacted. **Standard for Triggering:** The statute is triggered when a covered person becomes aware of a breach of the security of the system and conducts a reasonable and prompt investigation, in good faith, to determine the likelihood that personal information has been or will be used for an unauthorized purpose. "Breach of the security of the system" means unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. 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.
Specific Content Requirements	An individual or commercial entity that maintains the data shall provide the owner or licensee of the data information relevant to the breach, not including information proprietary to the individual or commercial entity.
Timing	Notice to residents must be made as soon as possible 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. An individual or a commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach if use of personal information about a Nebraska resident for an unauthorized purpose occurred or is reasonably likely to occur. Cooperation includes, but is not limited to, sharing with the owner or licensee information relevant to the breach, not including information proprietary to the individual or commercial entity.
Penalty/Private Right of Action	The Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of this act.
Other Provisions	N/A

State Statute	**Nevada** Nev. Rev. Stat. §§ 603A.010–.920 (2005); as amended (2007); Nev. Rev. Stat. § 603A.210 (2005); as amended Nev. Rev. Stat. § 603A.215 (2009)
Personal Information Definition	Personal Information of Nevada residents, excluding: 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.
Persons Covered	Any data collector that owns or licenses computerized data that includes personal information of a Nevada resident. Any data collector that maintains computerized data that includes personal information that the data collector does not own. "Data collector" means any governmental agency, institution of higher education, corporation, financial institute 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.
Encryption/ Notification Trigger	The statute only applies to unencrypted data. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach of the security of the system. "Breach of the security of the system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector.
Specific Content Requirements	N/A
Timing	A data collector that owns or licenses the information must give notice to affected residents 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. A data collector that maintains the data must give notice to the owner or licensee of the information immediately following discovery of the breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Penalty/ Private Right of Action	A private right of action exists for the data collector. A data collector that provides the requisite notice may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. The Attorney General may bring an action against the person to obtain a temporary or permanent injunction against the violation.
Other Provisions	N/A

State Statute	New Hampshire N.H. Rev. Stat. Ann. §§ 359-C:19–C:21, 358-A:4 (2006)., 332-I:1–I:610
Personal Information Definition	Personal Information Breach Notification Statute: Personal Information of New Hampshire residents. Medical Information Unauthorized Disclosure Notification Statute: Incorporates definition of protected medical information from §§262 and 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (codified at 42 U.S.C. § 300gg and 29 U.S.C § 1181 et seq. and 42 USC 1320d et seq. (2010)).
Persons Covered	Personal Information Breach Notification Statute: Any person doing business in this state that owns or licenses computerized data that includes personal information and discovers a breach of the security of the data; and any person or business that maintains computerized data that includes personal information that the person or business does not own and discovers a breach of the security of the data. Medical Information Unauthorized Disclosure Notification Statute: Any person, corporation, facility, or institution either licensed by New Hampshire or otherwise lawfully providing health care services, including, but not limited to, a physician, hospital, office, clinic, health center or other health care facility, dentist, nurse, optometrist, pharmacist, podiatrist, physical therapist, or mental health professional, and any officer, employee, or agent of such provider acting in the course and scope of employment or agency related to or supportive of health care services.
Encryption/ Notification Trigger	Personal Information Breach Notification Statute: If the data elements are encrypted, notification is not required. **Standard for Triggering:** Personal Information Breach Notification Statute: The statute is triggered when a person who owns or licenses computerized data becomes aware of a security breach and determines that misuse of the information has occurred or is reasonably likely to occur, or if that person cannot determine the likelihood that the information has been or will be misused. The statute is also triggered when a person or business that maintains data computerized that they do not own discovers: (1) a breach of the security of the data and (2) an unauthorized person acquired the personal information. "Security breach" means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. Medical Information Unauthorized Disclosure Notification Statute: The statute is triggered by the unauthorized use or disclosure of protected health information for marketing or fundraising purposes. (RSA 332-I:4). Health care providers may be liable even if such use is permissible under federal law (HIPAA, HITECH). "Marketing" means a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." Health care providers must also provide individuals an opt-out notice before any personally identifiable health information may be used for fundraising purposes.

State Statute	New Hampshire N.H. Rev. Stat. Ann. §§ 359-C:19–C:21, 358-A:4 (2006)., 332-I:1–I:610
Specific Content Requirements	Personal Information Breach Notification Statute: The following must be included in a notice to affected individuals: (a) a description of the incident in general terms; (b) the approximate date of breach; (c) the type of personal information obtained as a result of the security breach; (d) the telephonic contact information of the person subject to this section.
Timing	Personal Information Breach Notification Statute: A person who owns or licenses the data must notify the affected individuals as soon as possible after notifying the attorney general's office. If also required to notify a consumer reporting agency, the person must notify the agency without unreasonable delay. Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was acquired by an unauthorized person. Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential or business information or trade secrets. 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. Medical Information Unauthorized Disclosure Notification Statute: The healthcare provider shall "promptly notify in writing the individual or individuals whose protected health information was disclosed." A business associate shall be responsible for the cost of such notification if the use or disclosure was by the business associate.
Penalty/ Private Right of Action	Personal Information Breach Notification Statute: Persons injured as a result of a violation may bring an action for damages and for such equitable relief as the court deems necessary and proper. A prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees. The Attorney General's office shall enforce these provisions by bringing an action in the name of the state to restrain the violation by temporary or permanent injunction, and to obtain up to $10,000 in civil penalties for each violation. Medical Information Unauthorized Disclosure Notification Statute: An aggrieved individual whose health records were wrongly disclosed may bring a civil action and, if successful, shall be awarded special or general damages of not less than $1,000 for each violation, and costs and reasonable legal fees.
Other Provisions	Personal Information Breach Notification Statute: Any person engaged in trade or commerce shall notify the regulator which has primary regulatory authority over such trade or commerce; all other persons shall notify Attorney General's office. Notice to the Attorney

State Statute	New Hampshire N.H. Rev. Stat. Ann. §§ 359-C:19–C:21, 358-A:4 (2006)., 332-I:1–I:610
	General's office must include the anticipated date of the notice to the individuals and the approximate number of individuals in the state who will be notified. The names of the individuals entitled to receive notice do not have to be disclosed. If a person is required to notify more than 1,000 consumers of a breach of security, the person shall also notify, without unreasonable delay, all consumer reporting agencies of the anticipated date of the notification to the consumers, the approximate number of consumers who will be notified, and the content of the notice. Nothing in this paragraph shall be construed to require the person to provide to any consumer reporting agency the names of the consumers entitled to receive the notice or any personal information relating to them.

State Statute	New Jersey N.J. Stat. Ann. § 56:8-163–66 (2005)
Personal Information Definition	Personal Information of New Jersey residents. In addition: 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.
Persons Covered	Any entity that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information. Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity.
Encryption/ Notification Trigger	Does not cover encrypted or otherwise unreadable data. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach of security. "Breach of security" means 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. Notification is not required if the business or public entity establishes that misuse of the information is not reasonably possible (must retain a record of this decision for five years).
Specific Content Requirements	N/A
Timing	A business or public entity that owns the data shall disclose any breach to customers 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. Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.
Penalty/ Private Right of Action	It shall be an unlawful practice and a violation of N.J. STAT. ANN. §§ 56:8-1, *et seq*. to willfully, knowingly or recklessly violate this data breach notification law. Therefore, remedies available under this chapter of the New Jersey Statutes apply to violations of the data breach notification law.
Other Provisions	A breach must be reported to the Division of State Police in the Department of Law and Public Safety prior to notifying customer.

State Statute	New York N.Y. Gen. Bus. Law § 899-aa (2005).
Personal Information Definition	The law applies to "private information," which means personal information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person, in combination with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or non-driver identification card number; or (3) 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.
Persons Covered	Any person or business which conducts business in New York, and which owns or licenses computerized data which includes private information, is covered under this statute when there has been a breach in the security of the system containing the data. Any person or business which maintains computerized data, which includes private information which such person or business does not own, is covered when there has been a breach of the security of the system.
Encryption/ Notification Trigger	When the private information is encrypted and the encryption key has not been acquired, there is no duty to notify. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach in the security of the system. "Breach in the security of the system" means unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others: (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or (2) indications that the information has been downloaded or copied; or (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
Specific Content Requirements	Notice to residents shall 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.
Timing	A person or business that owns or licenses the data must notify New York residents 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.

State Statute	New York N.Y. Gen. Bus. Law § 899-aa (2005).
	Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.
Penalty/ Private Right of Action	The Attorney General may bring an action in a court having jurisdiction to issue an injunction. The court may award damages for actual costs or losses incurred by a person entitled to notice. Whenever the court determines that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of $5,000 or up to $10,000 per instance of failed notification, provided that the latter amount shall not exceed $150,000. Any other lawful remedy available can be sought as long as such action is commenced within two years immediately after the date of the act complained of or the date of discovery of such act.
Other Provisions	The person or business must notify the state Attorney General, the Department of State, and the State Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content and distribution of the notices and approximate number of affected persons. In the event that more than 5,000 New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons.

State Statute	North Carolina N.C. Gen. Stat. §§ 75-65 (2005); as amended (2009).
Personal Information Definition	A person's first name or initial and last name, in combination with any one or more of the following: (1) Social Security number; (2) driver's license or State ID number; (3) account number, credit or debit card number, in combination with security or access codes or passwords to an individual's financial account; (4) biometric data; (5) finger prints; (6) other information that would permit access to a person's financial account or resources. Personal Information does not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parents' legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.
Persons Covered	Any business that owns or licenses personal information in any form (whether computerized, paper or otherwise) or any business that maintains or possesses records or data containing personal information that the business does not own or license.
Encryption/ Notification Trigger	Does not cover encrypted information, unless there is unauthorized access to encrypted records along with the confidential process or key. **Standard for Triggering:** The statute is triggered upon discovery or notification of a security breach. "Security breach" means 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.
Specific Content Requirements	The notice shall be clear and conspicuous and include all of the following: (1) a description of the incident in general terms; (2) a description of the type of personal information that was subject to the unauthorized access and acquisition; (3) a description of the general acts of the business to protect the personal information from further unauthorized access; (4) a telephone number for the business that the person may call for further information and assistance, if one exists; (5) advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports; (6) the toll-free numbers and addresses for the major consumer reporting agencies; and (7) the toll-free numbers, addresses, and Web site 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.
Timing	Disclosure should 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

State Statute	North Carolina N.C. Gen. Stat. §§ 75-65 (2005); as amended (2009).
	confidentiality of the data system. Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement.
Penalty/ Private Right of Action	An individual injured as a result of a violation of this section may institute a civil action. Damages set at $5,000 per incident, and provides for treble damages within this range. Injunctive relief also available.
Other Provisions	A breach must be reported to the Consumer Protection Division of the Attorney General's Office. Notification to the Attorney General must include the nature of the breach, the number of consumers affected, 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. Submission of a completed North Carolina Security Breach Reporting Form by mail or fax will satisfy this requirement.

State Statute	North Dakota N.D. Cent. Code §§ 51-30-01 to -07; 51-15-11; 51-15-07 (2005).
Personal Information Definition	An 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: (1) the individual's social security number; (2) the operator's license number assigned to an individual by the department of transportation; (3) a nondriver color photo identification card number assigned to the individual by the department of transportation; (4) 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; (5) the individual's date of birth; (6) the maiden name of the individual's mother; (7) medical information; (8) health insurance information; (9) an identification number assigned to the individual by the individual's employer; or (10) the individual's digitized or other electronic signature.
Persons Covered	Any person that conducts business in North Dakota and that owns or licenses computerized data that includes personal information. Any person that maintains computerized data that includes personal information that the person does not own.
Encryption/ Notification Trigger	Notification is not required when data has been secured by encryption or by any other method or technology that renders the electronic files, media, or data bases unreadable or unusable. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach of security. “Breach of security” means unauthorized acquisition of computerized data.
Specific Content Requirements	N/A
Timing	Notice to residents 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. A person that maintains the data must notify the owner or licensee immediately following discovery of the breach of the security of the system if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Penalty/ Private Right of Action	The Attorney General may impose a civil penalty of not more than $5,000 for each violation. The remedies, duties, prohibitions, and penalties under this particular law are not exclusive and are in addition to all other causes of action, remedies, and penalties.
Other Provisions	N/A

State Statute	Ohio Ohio Rev. Code Ann. §§ 1347.12 (state agencies), 1349.19 (persons and businesses), 1349.191–192 (2007).
Personal Information Definition	Personal Information of Ohio residents, excluding publicly available information that is lawfully available to the general public from federal, state, or local government records or any of the following media that are widely distributed: 1) any news or editorial advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television; 2) any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media; 3) any publication designed for and distributed to members of any bona fide associations or charitable or fraternal nonprofit corporation; 4) any type of media similar in nature to any item, entity, or activity identified above.
Persons Covered	Any person, including any business only if the business conducts in Ohio that owns, licenses or maintains computerized data that includes personal information. Any state agency or agency of a political subdivision.
Encryption/ Notification Trigger	If the data is encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable, it is not considered personal information, and notification is not required. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach of the security of the system. "Breach of the security of the system" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information that causes, or is reasonably likely to cause, or reasonably is believed to have caused a material risk of identity theft or other fraud to the person or property of a resident of Ohio. For a state agency, agency of a political subdivision, or person that owns, licenses, is the custodian of, or stores the data, the statute is triggered when: (1) the agency discovers a breach of the security system; (2) the agency determines that the personal information was, or is reasonably believed to have been accessed and acquired by an unauthorized person; and (3) the agency determines that the access and acquisition by the unauthorized person caused or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of the state.
Specific Content Requirements	N/A
Timing	Affected residents must be notified 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 activities and consistent with any measures necessary to determine the scope of the breach, including which residents' personal

State Statute	Ohio Ohio Rev. Code Ann. §§ 1347.12 (state agencies), 1349.19 (persons and businesses), 1349.191–192 (2007).
	information was accessed and acquired, and to restore the reasonable integrity of the data system. A state agency, agency of a political subdivision, or person that is the custodian of or stores the data must notify the owner or licensor of the data in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and 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 a resident of this state.
Penalty/ Private Right of Action	The Attorney General may investigate any violations of these sections and bring an action to collect a civil penalty against a person or agency for failing to comply with the statute. The Attorney General can seek a temporary restraining order, preliminary or permanent injunction, and civil penalties if it appears that a person or agency has failed or is failing to comply with §§ 1347.12 and 1349.19 of the Revised Code. Upon finding that a person or agency has failed to comply with the statute, the court shall impose a civil penalty as follows: (a) $1,000 for each day the agency or person has intentionally or recklessly failed to comply with the applicable section up to 60 days; (b) $5,000 for each day AFTER 60 days and up to 90 days that the agency or person has intentionally or recklessly failed to comply with the applicable section; (c) $10,000 for each day AFTER 90 days that the agency or person has intentionally or recklessly failed to comply with the applicable section.
Other Provisions	If more than 1000 residents are affected, consumer reporting agencies must be notified of the timing, distribution, and content of the disclosure given to the residents of the state. Notice to consumer reporting agencies must include the timing, distribution, and content of the disclosure given to the residents of the state. An obligation to notify consumer reporting agencies does not permit delaying notification to the affected residents or owner of the data.

State Statute	Oklahoma Okla. Stat. tit. 24 § 161 et seq. (2008) Okla. Stat. tit. 74 § 3113.1 (2006) (public agencies)
Personal Information Definition	Personal Information of Oklahoma residents.
Persons Covered	Individuals or entities that own or licenses computerized data that includes personal information. "Entity" includes 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. Any state agency, board, commission or other unit or subdivision of state government that owns or licenses computerized data that includes personal information, and any state agency, board, commission or other unit or subdivision of state government that maintains computerized data that includes personal information that the state agency, board, commission or other unit or subdivision of state government does not own.
Encryption/ Notification Trigger	Notification is not required for encrypted or redacted information unless the encrypted information is accessed and acquired in an unencrypted form or involves a person with access to the encryption key. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach of the security of the system. "Breach of the security of the system" means 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. For public agencies, the statute is triggered upon the discovery or notification of any breach of the security of a system when unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Specific Content Requirements	N/A
Timing	Notice to residents shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required shall be made after the law enforcement agency determines that it will not compromise the investigation. An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was or if the entity reasonably believes was accessed

State Statute	Oklahoma Okla. Stat. tit. 24 § 161 et seq. (2008) Okla. Stat. tit. 74 § 3113.1 (2006) (public agencies)
	and acquired by an unauthorized person. Any state agency, board, commission or other unit or subdivision of state government that maintains computerized data that includes personal information that the state agency, board, commission or other unit or subdivision of state government does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Penalty/ Private Right of Action	A violation that results in injury or loss to residents of this state may be enforced by the Attorney General or a district attorney in the same manner as an unlawful practice under the Oklahoma Consumer Protection Act. The Attorney General or a district attorney shall have exclusive authority to bring an action and may obtain either actual or a civil penalty not to exceed One Hundred Fifty Thousand Dollars ($150,000.00) per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation. A violation by a state-chartered or state-licensed financial institution shall be enforceable exclusively by the primary state regulator of the financial institution.
Other Provisions	N/A

State Statute	Oregon Or. Rev. Stat. §§ 646A.602, 646A.604, 646A.624 (2011).
Personal Information Definition	A consumer's first name or first initial and last name in combination with any one or more of the following data elements, 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: (1) Social Security number; driver license number or state identification card number issued by the Department of Transportation; (2) passport number or other United States issued identification number; or (3) 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. Personal information also includes any of the data elements or any combination of the data elements described above when not combined with the consumer's first name or first initial and last name and when the data elements are not rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised. Personal information DOES NOT include information, other than a Social Security number, in a federal, state or local government record that is lawfully made available to the public.
Persons Covered	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. Any person that maintains or otherwise possesses personal information on behalf of another person.
Encryption/ Notification Trigger	If data is encrypted or redacted, notification is not required. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach of security. "Breach of security" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the person. For a person that owns the data, notification is not required 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.
Specific Content Requirements	Notice shall include at a minimum: (a) a description of the incident in general terms; (b) the approximate date of the breach of security; (c) the type of personal information obtained as a result of the breach of security; (d) contact information of the person subject to the statute;

State Statute	Oregon Or. Rev. Stat. §§ 646A.602, 646A.604, 646A.624 (2011).
	(e) contact information for national consumer reporting agencies; and (f) advice to the consumer to report suspected identity theft to law enforcement, including the Federal Trade Commission.
Timing	A person that owns, maintains or otherwise possesses the data must notify consumers 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. Any person that maintains or otherwise possesses personal information on behalf of another person shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach of security if a consumer's personal information was included in the information that was breached.
Penalty/ Private Right of Action	Compensation can be ordered by the state upon a finding that enforcement of the rights of consumers by private civil action would be so burdensome or expensive as to be impractical. In addition to other penalties and enforcement provisions provided by law, any person who violates or who procures, aids or abets in a violation of the data breach notification law shall be subject to a penalty of not more than $1,000 per violation, but no more than $500,000 total, which shall be paid to the General Fund of the State Treasury.
Other Provisions	If a person discovers a breach of security affecting more than 1,000 consumers that requires disclosure under this section, the person shall notify, without unreasonable delay, all consumer reporting agencies. Notice to consumer reporting agencies must include the timing, distribution and content of the notification given by the person to the consumers. The notice must also include the police report number, if available.

State Statute	**Pennsylvania** 73 Pa. Stat. Ann. §§ 2301–2308, 2329 (2006). 201-4, 201-4.1, 201-8 (West 2012).
Personal Information Definition	Personal Information of Pennsylvania residents.
Persons Covered	An entity that maintains, stores or manages computerized data that includes personal information. "Entity" means a State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth. A vendor that maintains, stores or manages computerized data on behalf of another entity.
Encryption/ Notification Trigger	Notice is required if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption, or if the security breach involves a person with access to the encryption key. **Standard for Triggering:** The statute is triggered when the entity discovers any breach of the security of the system. "Breach of the security of the system" means 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 this Commonwealth.
Specific Content Requirements	N/A
Timing	An entity shall give notice to affected residents and consumer reporting agencies, if necessary, without unreasonable delay. A vendor that maintains, stores, or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.
Penalty/ Private Right of Action	The Attorney General has exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.
Other Provisions	When an entity notifies more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, of the timing, distribution and number of notices. Notice to consumer reporting agencies must include the timing, distribution and number of notices.

State Statute	Rhode Island R.I. Gen. Laws §§ 11-49.2-3–49.2-7 (2005).
Personal Information Definition	Personal Information of Rhode Island residents.
Persons Covered	Any state agency or person that owns, maintains or licenses computerized data that includes personal information. Any state agency or person that maintains computerized unencrypted data that includes personal information that the state agency or person does not own.
Encryption/ Notification Trigger	If the information is encrypted, notice is not required. **Standard for Triggering:** The statute is triggered by discovery or notification of a breach of the security of the system which poses a significant risk of identity theft and the personal information was, or is reasonably believed to have been, acquired by an unauthorized person or a person without authority to acquire the information. "Breach of the security of the system" means unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the state agency or person. Notification of a breach is not required 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.
Specific Content Requirements	N/A
Timing	Notice must be provided to affected residents 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. Any state agency or person that maintains computerized unencrypted data that includes personal information that the state agency or person does not own shall notify the owner or licensee of the information of any breach of the security of the data which poses a significant risk of identity theft immediately, following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Unless otherwise provided, the notification must be prompt and reasonable following the determination of the breach.
Penalty/ Private Right of Action	Each violation is a civil violation for which a penalty of not more than $100 per occurrence and not more than $25,000 may be adjudged against a defendant.
Other Provisions	N/A

State Statute	South Carolina S.C. CODE § 1-11-490 (2008); S.C. CODE § 39-1-90 (2009).
Personal Information Definition	Personal Information of South Carolina residents. In addition: 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.
Persons Covered	Any person (business or individual) or agency that does business in South Carolina and owns, maintains, or licenses computerized data that includes personal identifying information about a resident of South Carolina.
Encryption/ Notification Trigger	If data is rendered unusable through encryption, redaction, or other methods, notice is not required. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach of the security of the system "Breach of the security of the system" means 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.
Specific Content Requirements	N/A
Timing	Consumers must be given notice 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. An agency or person maintaining computerized data or other data that includes personal identifying information that the agency does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.
Penalty/ Private Right of Action	A resident who is injured by a violation of the statute, in addition to and cumulative of all other rights and remedies available at law, may: institute a civil action to recover damages in case of a willful and knowing violation; institute a civil action to recover only actual damages resulting from a violation in case of a negligent violation; seek an injunction to enforce compliance; and recover attorney's fees and court costs, if successful. A person or agency that knowingly and willfully violates the data breach notification laws is subject to an administrative fine up to $1,000 for each resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs.
Other Provisions	A person that maintains its own notification procedures as part of an information security policy for the treatment of personal identifying information and is otherwise consistent with the timing requirements of this section is considered to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with its

State Statute	South Carolina S.C. CODE § 1-11-490 (2008); S.C. CODE § 39-1-90 (2009).
	policies in the event of a breach of security of the system A financial institution that is subject to and in compliance with the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice is considered to be in compliance with the data breach notification laws. A breach must be reported to the Consumer Protection Division of the Department of Consumer Affairs if 1,000 or more persons affected.

State Statute	Tennessee Tenn. Code Ann. §§ 47-18-2105 to -2107 (2005).
Personal Information Definition	Personal Information of Tennessee residents.
Persons Covered	Any information holder. "Information holder" means any person or business that conducts business in Tennessee, or any agency of the State of Tennessee or any of its political subdivisions, that owns, licenses, or maintains computerized data that includes personal information.
Encryption/ Notification Trigger	Notification requirement only applies where personal information was unencrypted. **Standard for Triggering:** The statute is triggered upon discovery of notification of a breach of the security of the system. "Breach of the security of the system" means unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder.
Specific Content Requirements	N/A
Timing	Notification must be provided 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. Any information holder that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Penalty/ Private Right of Action	Any customer of the information holder who is a person or business entity may institute a civil action to recover damages and enjoin the person or business entity from further action in violation. However, customer cannot be an agency of the state or any political subdivision of the state. In addition, a violation can subject the violator to a civil penalty of $10,000; $5,000 per day that a person's identity has been assumed; or ten times the amount obtained or attempted to be obtained through the identity theft, whichever is greater. The Attorney General can also seek injunctions, and get attorneys' fees. A violation under this statute may also be a violation of the Tennessee Consumer Protection Act.
Other Provisions	N/A

State Statute	Texas Tex. Bus. & Com. Code § 521.002 and 521.053 (2007); as amended (2012).
Personal Information Definition	The statute applies to "Sensitive Personal Information" which includes Personal Information of Texas residents. In addition: 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.
Persons Covered	A person who conducts business in this state and owns, licenses or maintains computerized data that includes sensitive personal information.
Encryption/ Notification Trigger	Sensitive personal information only includes data items that are not encrypted unless the encryption key is also breached. **Standard for Triggering:** The statute is triggered upon discovery or the receipt of notification of a breach of system security. "Breach of system security" means 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.
Specific Content Requirements	N/A
Timing	Disclosure should be made as quickly as possible or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. However, disclosure may be delayed at the request of law enforcement agency that determines that the notification will impede a criminal investigation. Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Penalty/ Private Right of Action	The Attorney General may bring a civil suit for damages or an injunction. A person who violates the statute is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. A person who fails to take reasonable action to comply with notification requirements is liable to the state for a civil penalty of not more than $100 for each individual to whom notification is due for each consecutive day the person fails to take reasonable action to notify with a maximum penalty of $250,000 for a single breach. If it appears to the Attorney General that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the attorney general may bring an action in the name of the state against the person to restrain the violation by a temporary restraining order or by a permanent or temporary injunction.

State Statute	Texas Tex. Bus. & Com. Code § 521.002 and 521.053 (2007); as amended (2012).
	A violation of this statute is also a deceptive trade practice under the Texas Deceptive Trade Practices Act.
Other Provisions	Affected individuals residing in states with no data breach notification statutes (currently: Alabama, Kentucky, New Mexico, and South Dakota) must be notified in accordance with Texas law. If an entity must notify over 10,000 individuals of a breach, the entity must notify each consumer reporting agency of the timing, distribution, and content of the notices without unreasonable delay. Businesses must implement and maintain reasonable procedures, including appropriate corrective action, to protect from unlawful use or disclosure of sensitive personal information, such as shredding, erasing, or other similar means of modifying sensitive personal information to make it unreadable or indecipherable. This section does not apply to a financial institution.

State Statute	Utah Utah Code Ann. §§ 13-44-101 – 301 (2006); as amended (2009).
Personal Information Definition	Personal Information of Utah residents, excluding: information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.
Persons Covered	Any person that conducts business in the state and owns, maintains or licenses computerized information that contains personal information.
Encryption/ Notification Trigger	If the personal information is encrypted or protected by another method that renders the data unreadable or unusable, it is not protected, and notice is not required. **Standard for Triggering:** The statute is triggered when a person covered by the statute becomes aware of a breach of system security, at which time they must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes. "Breach of system security" means unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.
Specific Content Requirements	N/A
Timing	A person required to provide notification shall provide the notification in the most expedient time possible without unreasonable delay, considering legitimate investigative needs of law enforcement, after determining the scope of the breach of system security, and after restoring the reasonable integrity of the system. A person who maintains computerized data that includes personal information that the person does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur. Cooperation includes sharing information relevant to the breach with the owner or licensee of the information.
Penalty/ Private Right of Action	The statute does not create a private right of action, but likewise does not affect any private right of action that may exist under other law, including contract or tort. A person who violates this subchapter is subject to a civil fine of: (a) No greater than $2,500 for a violation or series of violations concerning a specific consumer; and (b) No greater than $100,000 in the aggregate for related violations concerning more than one consumer. The Attorney General may also seek injunctive relief.

State Statute	Utah Utah Code Ann. §§ 13-44-101 – 301 (2006); as amended (2009).
Other Provisions	Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business, and destroy, or arrange for the destruction of records containing personal information that are not to be retained by the person. The destruction of records shall be by shredding, erasing, or otherwise modifying the personal information to make the information indecipherable.

State Statute	**Vermont** Vt. Stat. Ann. tit. 9, §§ 2430, 2435 (2006); as amended (2008); as amended (2012).
Personal Information Definition	Personally identifiable information of Vermont residents. “Personally identifiable information” means an 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, redacted, or otherwise protected: (i) Social Security number; (ii) motor vehicle operator’s license number or non-driver identification card number; (iii) 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; (iv) account passwords or personal identification numbers or other access codes for a financial account.
Persons Covered	Any data collector that owns or licenses computerized personally identifiable information that includes personal information concerning a consumer, or that maintains or possesses computerized data containing personally identifiable information of a consumer that the data collector does not own or license or any data collector that acts or conducts business in Vermont that maintains or possesses records or data containing personally identifiable information that the data collector does not own or license. “Data collector” includes, but is not limited to, the 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.
Encryption/Notification Trigger	Data is not considered personally identifiable information if both the individual’s name and the combined data element are encrypted, redacted, or protected by another method that renders them unreadable or unusable. **Standard for Triggering:** The statute is triggered upon discovery or notification of a security breach. “Security breach” means the unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data. In determining whether personally identifiable information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others: (i) indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information; (ii) indications that the information has been downloaded or copied; (iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

	(iv) that the information has been made public. Notice of a security breach is not required if the data collector establishes that misuse of personal information is not reasonably possible and the data collector provides notice of the determination and a detailed explanation for said determination to the Vermont attorney general or to the department of banking, insurance, securities, and health care administration. If the data collector later gathers facts to indicate that the misuse of personal information is reasonably possible, then notice is required.
Specific Content Requirements	Notice shall be clear and conspicuous, and shall include a description of the following: (a) the incident in general terms; (b) the type of personally identifiable information that was subject to the security breach; (c) the general acts of the data collector to protect the personally identifiable information from further unauthorized access or acquisition; (d) a telephone number, toll-free if available, that the consumer may call for further information and assistance; (e) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; (f) the approximate date of the security breach.
Timing	Notice of the security breach to a consumer shall be made in the most expedient possible and without unreasonable delay, but not later than 45 days after discovery. Within 14 business days of the discovery of the incident, the Attorney General must be provided the date of the security breach, date of discovery, a preliminary description of the breach.
Penalty/ Private Right of Action	The Attorney General and state's attorney shall have sole and full authority to investigate potential violations and to enforce, prosecute, obtain, and impose remedies for any violation.
Other Provisions	Once notice is made to consumers, the Attorney General must be notified of the number of Vermont consumers affected and provided a copy of the notice. A second copy of the consumer notification letter, with personally identifiable information that was subject to the breach redacted, can also be provided to the attorney general which will be used for any public disclosure of the breach. For Vermont-regulated financial institutions, notice should be made instead to the Department of Financial Regulation. In the event a data collector provides notice to more than 1,000 consumers at one time pursuant to this section, the data collector shall notify, without unreasonable delay, all consumer reporting agencies. In notice to a consumer reporting agency, the data collector must include the timing, distribution, and content of the notices being sent to the affected consumers.

State Statute	**Virginia** Va. Code Ann. § 18.2-186.6 (2008). Va. Code Ann. § 32.1– 127.1:05 (2011)
Personal Information Definition	Personal Information Breach Notification Statute: Personal Information of Virginia residents. Medical Information Breach Notification Statute: Medical information. “Medical information” means the first name or first initial and last name with any of the following elements: (1) any information regarding an individual’s medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (2) an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.
Persons Covered	Personal Information Breach Notification Statute: An individual or entity that owns or licenses computerized data that includes personal information, and an individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license. "Entity" means 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. "Individual" means a natural person. Medical Information Breach Notification Statute: An entity that owns or licenses computerized data that includes medical information, and an entity that maintains computerized data that includes medical information that the entity does not own or license. “Entity” means any authority, board, bureau, commission, district or agency of the state or of any political subdivision of the state, including cities, towns and counties, municipal councils, governing bodies of counties, school boards and planning commissions; boards of visitors of public institutions of higher education; and other organizations, corporations, or agencies in the state supported wholly or principally by public funds. The statute does not apply to: (i) a person or entity who is a "covered entity" or "business associate" under HIPAA (42 USC § 1320d et seq.) and is subject to requirements for notification in the case of a breach of protected health information (42 USC 17932 et seq.); or (ii) a person or entity who is a non-HIPAA-covered entity subject to the Health Breach Notification Rule promulgated by the Federal Trade Commission pursuant to 42 USC § 17937 et seq.

State Statute	**Virginia** Va. Code Ann. § 18.2-186.6 (2008). Va. Code Ann. § 32.1– 127.1:05 (2011)
Encryption/ Notification Trigger	Neither statute applies to encrypted, redacted, or altered information that is rendered unusable unless the encrypted data is accessed and acquired in unencrypted form or in combination with the encryption key. **Standard for Triggering:** Personal Information Breach Notification Statute: The statute is triggered when a person covered by the statute discovers or is notified of a breach of the security of the system. "Breach of the security of the system" means 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. Medical Information Breach Notification Statute: The statute is triggered upon discovery or notification of a breach of the security of the system. "Breach of the security of the system" means unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of medical information maintained by an entity.
Specific Content Requirements	Personal Information Breach Notification Statute: Notice must include a description of the following: (1) the incident in general terms; (2) the type of personal information that was subject to the unauthorized access and acquisition; (3) the general acts of the entity to protect the personal information from further unauthorized access; (4) a telephone number that the person may call for further information and assistance, if one exists; and (5) advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. Medical Information Breach Notification Statute: Notice must include a description of the following: (1) the incident in general terms; (2) the type of medical information that was subject to the unauthorized access and acquisition; (3) the general acts of the entity to protect the medical information from further unauthorized access; (4) a telephone number that the person may call for further information and assistance, if one exists.

State Statute	Virginia Va. Code Ann. § 18.2-186.6 (2008). Va. Code Ann. § 32.1– 127.1:05 (2011)
Timing	Notice under both statutes must be given without unreasonable delay. Reasonable delay includes time to allow the individual or entity to determine the scope of the breach of the security of the system, to restore the integrity of the system, or to comply with law enforcement if a law enforcement agency believes notice will impede a criminal or civil investigation, or homeland or national security. Personal Information Breach Notification Statute: An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system. Medical Information Breach Notification Statute: An entity that maintains computerized data that includes medical information that the entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system.
Penalty/ Private Right of Action	Personal Information Breach Notification Statute: The Attorney General may bring an action to address violations by imposing a civil penalty not to exceed $150,000 per breach of the security of the system. Nothing shall limit an individual from recovering direct economic damages from a violation of this law. A violation by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator. A violation of this section by an individual or entity regulated by the State Corporate Commission's Bureau of Insurance shall be enforced exclusively by the State Corporation Commission.
Other Provisions	Personal Information Breach Notification Statute: The Office of the Attorney General must be notified following discovery of a breach of personal information. In the event an individual or entity provides notice to more than 1,000 persons at one time, they must notify, without unreasonable delay, both the Office of the Attorney General and all consumer reporting agencies of the timing, distribution, and content of the notice sent to affected residents. Medical Information Breach Notification Statute: The Office of the Attorney General and the Commissioner of Health must be notified following discovery of a breach of medical information. The entity must notify both the subject of the medical information and any affected resident of the Commonwealth, if those are not the same person. In the event an entity provides notice to more than 1,000 persons at one time, they must notify, without unreasonable delay, the Office of the Attorney General and the Commissioner of Health of the timing, distribution, and content of the notice sent to affected individuals.

State Statute	**Washington** Wash. Rev. Code Ann. §§ 19.255.010, 19.255.020 (2005) Wash. Rev. Code Ann. §§ 42.56.010, 42.56.590 (2005); as amended (2007).
Personal Information Definition	Personal Information of Washington residents.
Persons Covered	Any person, business, or agency that conducts business in this state and that owns or licenses computerized data that includes personal information of residents of Washington, and any person, business, or agency that maintains computerized data that includes personal information.
Encryption/ Notification Trigger	If both an individual's first name or first initial and last name and accompanying data element are encrypted, notice is not required. **Standard for Triggering:** The statute is triggered upon discovery or notification of a breach in the security of the system. "Breach in the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. A person, business, or 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.
Specific Content Requirements	N/A
Timing	Notice must be given to residents in the most expedient time possible and without unreasonable delay, consistent with 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. Any person or business or agency that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Penalty/ Private Right of Action	Any customer injured by a violation may institute a civil action to recover damages. Any person, business, or agency that violates, proposes to violate, or has violated this statute may be enjoined. The rights and remedies available are cumulative to each other and to any other rights and remedies available under the law.
Other Provisions	N/A

State Statute	**West Virginia** W. Va. Code Ann. §§ 46A-2A-101–104 (2008).
Personal Information Definition	Personal Information of West Virginia residents.
Persons Covered	An individual or entity that owns or licenses computerized data that includes personal information, and an individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license. "Entity" includes 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.
Encryption/ Notification Trigger	If encrypted or redacted information is accessed and acquired and the person does not have access to the encryption key, notice is not required. **Standard for Triggering:** the statute is triggered upon discovery or notification of a breach of the security of the system. "Breach of the security of the system" means 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 this state.
Specific Content Requirements	The notice shall include: (1) 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; (2) 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: (A) what types of information the entity maintained about that individual or about individuals in general; and (B) whether or not the entity maintained information about that individual; (3) 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. When notifying consumer reporting agencies, an individual or entity must include information on the timing, distribution, and content of the notices being sent to the affected residents.
Timing	An individual or entity that owns or licenses data must notify a resident of the security breach without unreasonable delay, unless: (1) 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;

State Statute	**West Virginia** W. Va. Code Ann. §§ 46A-2A-101–104 (2008).
	(2) the individual or entity needs to take any measures necessary to determine the scope of the breach; or (3) the individual or entity needs time to restore the reasonable integrity of the system. An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was or the entity reasonably believes was accessed and acquired by an unauthorized person.
Penalty/ Private Right of Action	Failure to comply constitutes an unfair or deceptive act of practice, which may be enforced by the Attorney General. The Attorney General shall have exclusive authority to bring action. No civil penalty may be assessed in an action unless the court finds that the defendant has engaged in a course of repeated and willful violations. No civil penalty shall exceed $150,000 per breach of security of the system or series of breaches of a similar nature that are discovered in a single investigation. A violation by a licensed financial institution shall be enforceable exclusively by the financial institution's primary functional regulator.
Other Provisions	If an entity is required to notify more than 1,000 persons of a breach, the entity shall also notify, without unreasonable delay, all consumer reporting agencies of the timing, distribution and content of the notices. The entity must not provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients. This subsection shall not apply to an entity that is subject to Title V of the Gramm Leach Bliley Act, 15 U.S.C. 6801, et seq.

State Statute	Wisconsin Wis. Stat. Ann. § 134.98 (2006); as amended (2008).
Personal Information Definition	An individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: (1) the individual's Social Security number; (2) the individual's driver's license number or state identification number; (3) the number of the individual's 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; (4) DNA profile; (5) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.
Persons Covered	An entity whose principal place of business is located in Wisconsin or an entity that maintains or licenses personal information in Wisconsin, and knows personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information; or an entity whose principal place of business is not located in Wisconsin, but who knows that personal information pertaining to a resident of Wisconsin has been acquired by a person whom the entity has not authorized to acquire the information. "Entity" means a person, other than an individual, including 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 as well as a city, village, town, or county 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; or (d) lends money to a resident of this state.
Encryption/ Notification Trigger	If one of the data elements linked to an individual's name is encrypted, redacted, or altered in a manner that renders the element unreadable, no notice is required. **Standard for Triggering:** The statute is triggered when a person or entity knows that a person whom the entity has not authorized to acquire personal information has acquired the personal information. 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. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the 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

State Statute	Wisconsin Wis. Stat. Ann. § 134.98 (2006); as amended (2008).
	the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident of this state who is the subject of the personal information. If a person, other than an individual, that stores personal information pertaining to a resident of this state, but does not own or license the personal information, knows that the personal information has been acquired by a person whom the person storing the personal information has not authorized to acquire the personal information, and the person storing the personal information has not entered into a contract with the person that owns or licenses the personal information, the person storing the personal information shall notify the person that owns or licenses the personal information of the acquisition as soon as practicable. An entity is not required to provide notice of the acquisition of personal information if the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.
Specific Content Requirements	Notice to the subject of acquired personal information shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information. Upon written request by a person who has received notice, the entity that provided the notice shall identify the personal information that was acquired.
Timing	Notice shall be provided within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination as to reasonableness shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.
Penalty/ Private Right of Action	Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or breach of a legal duty.
Other Provisions	If a person or entity must notify 1,000 or more individuals, the entity must notify all consumer reporting agencies of the timing, distribution, and content of the notices sent to the individuals. The statute does not apply to an entity subject to privacy and security requirements of 15 U.S.C. § 6801-6827, or a person that has a contractual obligation to such entity, if the entity or person has in effect a policy concerning breaches of information security. Likewise, the statute does not apply to an entity described in 45 CFR § 164.104(a), if the entity complies with the requirements of 45 CFR part 164.

State Statute	Wyoming Wyo. Stat. Ann. §§ 40-12-501, 40-12-502 (2010).
Personal Information Definition	"Personal identifying information", which includes the 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.
Persons Covered	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; and any person who maintains computerized data that includes personal identifying information on behalf of another business entity.
Encryption/ Notification Trigger	If both an individual's first name or first initial and last name and combined data element are redacted, notice is not required. **Standard for Triggering:** The statute is triggered when an individual or entity becomes aware of a breach of the security of the system and, after a prompt, reasonable, and good faith investigation, the individual or commercial entity determines that the misuse of personal identifying information about the residents has occurred or is reasonably likely to occur. "Breach of security" means unauthorized acquisition of computerized 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 this state.
Specific Content Requirements	Notice shall include a toll free number that the individual may use to contact the person collecting the data, or his agent; and from which the individual may learn the toll free contact telephone numbers and addresses for the major credit reporting agencies.
Timing	Notice to residents shall be given as soon as possible, 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. Any person who maintains computerized data that includes personal identifying information on behalf of another business entity shall disclose to the business entity for which the information is maintained any breach of the security of the system as soon as practicable following the determination that personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person. The person who maintains the data on behalf of another business entity and the business entity on whose behalf the data is maintained may agree which person or entity will provide any required notice, provided only a single notice for each breach of the security of the system shall be required. If

	agreement regarding notification cannot be reached, the person who has the direct business relationship with the resident of this state shall provide notice.
Penalty/ Private Right of Action	The Attorney General may bring an action in law or equity to address any violation and for other relief that may be appropriate to ensure proper compliance, to recover damages, or both.
Other Provisions	N/A

State Statute	District of Columbia D.C. Code § 28-3851 to 28-3853 (2007).
Personal Information Definition	A person's first name or first initial and last name, or phone number, or address, in combination with one of the following: (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 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.
Persons Covered	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 and who discovers a breach of the security of the system; and 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 and who discovers a breach of the security of the system.
Encryption/ Notification Trigger	The acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party is not considered a breach of the security system. **Standard for Triggering:** The statute is triggered when the person or entity discovers a breach of the security system. "Breach of the security of the system" means unauthorized acquisition of computerized or other electronic 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.
Specific Content Requirements	N/A
Timing	Notice must be provided in the most expedient time possible and without unreasonable delay. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation, but must be made as soon as possible after law enforcement determines the notification will not compromise an investigation. 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 shall notify the owner or licensee of the information of any breach of the security of the system in the most expedient time possible following discovery.
Penalty/ Private Right of Action	Any District of Columbia resident injured by a violation may institute a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees. Actual damages shall not include dignitary damages, including pain and suffering. The Attorney General may petition the Superior Court of the District of Columbia for injunctive relief and/or restitution. The Attorney General may

State Statute	District of Columbia D.C. Code § 28-3851 to 28-3853 (2007).
	recover a civil penalty of $100 for each resident not provided notice, attorney's fees for pursuing the action, and costs.
Other Provisions	N/A

State Statute	Puerto Rico 10 L.P.R.A. § 4051; 10 L.P.R.A. § 4052 (2005), as amended (2008).
Personal Information Definition	At least the name or first initial and the surname of a person, together with any of the following data so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code: (1) Social Security number; (2) driver's license number, voter's identification or other official identification; (3) bank or financial account numbers of any type with or without passwords or access code that may have been assigned; (4) names of users and passwords or access codes to public or private information systems; (5) medical information protected by the HIPAA; (6) tax information; (7) work-related evaluations.
Persons Covered	Any entity that is the proprietor or custodian of a data bank for commercial use that includes personal information of citizens who reside in Puerto Rico. "Entity" means 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 the Commonwealth of Puerto Rico; as well as every public or private educational institution, regardless of the level of education offered by it.
Encryption/ Notification Trigger	The statute applies only where information is unencrypted. **Standard for Triggering:** The statute is triggered when there has been a violation of the system's security when the data bank whose security has been violated contains all or part of the personal information file and the same is not protected by a cryptographic code but only by a password. "Violation of the system's security" means <u>any situation in which it is detected that access has been permitted to unauthorized persons or entities</u> to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. This includes both access to the data banks through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings.
Specific Content Requirements	The notice of breach of the security of the system shall be submitted in a clear and conspicuous manner and should describe the breach of the security of the system in general terms and the type of sensitive information compromised. The notification shall also include a toll free number and an Internet site for people to use in order to obtain information or assistance. Notice can be provided in writing or by authenticated electronic means.

State Statute	**Puerto Rico** 10 L.P.R.A. § 4051; 10 L.P.R.A. § 4052 (2005), as amended (2008).
Timing	Clients must be notified as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security. Within a non-extendable term of ten (10) days after the violation of the system's security has been detected, the parties responsible shall inform the Department of Consumer Affairs, which shall make a public announcement of the fact within twenty-four (24) hours after having received the information. Any entity that as part of their operations resells or provides access to digital data banks that at the same time contain personal information files of citizens must notify the proprietor, custodian or holder of said information of any violation of the system's security that has allowed access to those files to unauthorized persons.
Penalty/ Private Right of Action	Consumers may bring actions apart from the statute. The Secretary may impose fines of $500 up to a maximum $5,000 for each violation of the provisions of this Act or its Regulations. The fines provided in this Section do not affect the rights of the consumers to initiate actions or claims for damages before a competent court.
Other Provisions	N/A

State Statute	**Virgin Islands** 14 V.I.C. § 2208, et seq.(2005).
Personal Information Definition	Personal Information of Virgin Island residents.
Persons Covered	Any agency that owns or licenses computerized data that includes personal information; any agency that maintains (but does not own) computerized data that includes personal information; and any person or business that conducts business in the Virgin Islands and that owns or licenses computerized data that includes personal information; any person or business that maintains computerized data that includes personal information the person or business does not own.
Encryption/ Notification Trigger	Statute applies only where personal information was unencrypted. **Standard for Triggering:** Any agency, person or business that owns or licenses computerized data with personal information shall disclose any breach following discovery or notification of the breach in security of the data to any resident of the V.I. whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. Breach of the security of the system means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Any agency, person or business that maintains computerized data that includes personal information the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been acquired by an unauthorized person.
Specific Content Requirements	N/A
Timing	Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. 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.
Penalty/ Private Right of Action	Any customer injured by a violation may commence a civil action to recover damages. Any business that violates, proposes to violate, or has violated this title may be enjoined. The rights and remedies available are cumulative to each other and to any other rights and remedies available under law.

State Statute	Guam Guam Code Ann. tit. IX, § 48-10 (2009)
Personal Information Definition	Personal Information of Guam Residents.
Persons Covered	An individual or entity that owns or licenses computerized data that includes personal information. An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license.
Encryption/ Notification Trigger	Does not apply to encrypted data unless the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of Guam. **Standard for Triggering:** An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of Guam whose personal information was or is 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 Guam. An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system if the personal information was, or if the entity reasonably believes was accessed and acquired by an unauthorized person.
Specific Content Requirements	N/A
Timing	An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system made without unreasonable delay. An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery. Notice 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.
Penalty/ Private Right of Action	The Office of the Attorney General has exclusive authority to bring action and may obtain either actual damages for a violation of this Chapter or a civil penalty not to exceed One Hundred Fifty Thousand Dollars ($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.
Other Provisions	N/A

The PowerPoint presentation(s) for this session are available at the following link(s):

Gerald J. Ferguson: Data Privacy and Data Security Compliance Issues

Jeffrey L. Poston: Data Privacy and Data Security Compliance Issues