SECURITY COMPLIANCE ASSOCIATES

BREACH NOTIFICATION GUIDE

(727) 571-1141

2727 Ulmerton Road, Suite 310
Clearwater, Florida 33762

scasecurity.com

TABLE OF CONTENTS

INTRODUCTION 4

STATES

Alabama 4
Alaska 6
Arizona 7
Arkansas 9
California 10
Colorado 13
Connecticut 15
Delaware 17
Florida 19
Georgia 21
Hawaii 23
Idaho 25
Illinois 26
Indiana 28
Iowa 30
Kansas 32
Kentucky 33
Louisiana 35
Maine 37
Maryland 38
Massachusetts 41
Michigan 43
Minnesota 45
Mississippi 47
Missouri 48
Montana 50

TABLE OF CONTENTS

Nebraska 52
Nevada 54
New Hampshire 55
New Jersey 57
New Mexico 59
New York 61
North Carolina 62
North Dakota 64
Ohio 66
Oklahoma 68
Oregon 69
Pennsylvania 71
Rhode Island 73
South Carolina 75
South Dakota 77
Tennessee 79
Texas 80
Utah 82
Vermont 83
Virginia 86
Washington 88
Washington D.C. 90
West Virginia 92
Wisconsin 93
Wyoming 95

CONCLUSION 97

INTRODUCTION

Cybercrime Threats: "When", Not "IF"

Data breaches are pernicious and on the rise. Cybercrime is a growth industry that is global in scope, and in the next five years will likely cost businesses multiple trillions of dollars. This trend expands as technology becomes more integral to daily life. Cloud computing has expanded into IoT, or the Internet of Things, putting data devices at our fingertips perpetually. As the digital "surface area" of technology increases, so will the vulnerabilities cybercriminals exploit.

Primarily, vulnerabilities are fixed with patches and updates, but there's an additional wrinkle: Moore's Law. Every eighteen months, approximately, computational potentiality doubles. Gordon Moore first noticed this trend in the sixties. As of 2019, the technological "singularity" has yet to be reached; but quantum computing is here, and this shift is only a few tech expansion "cycles" away.

Even as old vulnerabilities are patched, new ones develop; and predictably, cybercrime profits will expand. The concept of the "startup" isn't foreign to black-hat techs. Today, in terms of cybercrime, the question isn't "if" you're going to be impacted, the question is "when", and what are you going to do? Essentially, you want to develop an incident response plan which takes applicable state laws into account.

Designing A Breach Response Plan

The right plan must be upgraded periodically matching technological innovation. This plan needs to have clearly defined protocols in place and you'll need to test these protocols regularly. Downtime can cost as much as $5,600 a minute for many businesses. Even if you have a plan ready, should you neglect to follow applicable laws in your state, you could be subject to prosecution from the Attorney General (AG). Accordingly, the following guide will detail laws designed to direct businesses and protect citizens in the event of a data breach.

The information contained in this guide is a result of research conducted in 2019. The regulatory landscape continues to change and the breach notification laws will likely change and evolve as well. This information should not be considered legal advice and is for informative purposes only.

ALABAMA

Statute Codes

Alabama S.B. 318 was put into law March 28, 2018 and became effective June 1 that year. Breach laws for Alabama apply to individuals or commercial entities pertaining to sensitive PI. A breach in Alabama is the unauthorized acquisition of such data

electronically. Good-faith acquisition isn't a breach if it isn't used in an unauthorized way. Releasing of public records which aren't confined by confidentiality agreements aren't unlawful either.

Legal Requirements, Purpose, and Involved Timeframes

When it comes to a business's obligation to notify affected parties, should PI have been breached which can harm those affected, notice is required to each affected party. Also, consumer reporting agencies should be notified if 1,000 or more entities are affected. This must be done as expediently as possible.

Also, 1,000 or more affected parties require entities notify the AG with matching expediency. If substantial harm is determined from a breach, the AG must be notified no later than 45 days. Thankfully, time to investigate is included in reporting windows.

PI, as defined by Alabama, refers to a person's last name and first name, or the first initial of their first name, combined with other details like SSNs, driver's license or other identification, financial information, medical history, health insurance, email addresses, or any password/PIN information. If that data is effectively encrypted, it's not classified as a PI breach. Anything lawfully public in a federal, state, or local government sense, or info widely distributed by MSM outlets, isn't included in this definition.

Penalties and Exceptions

Alabama does not allow for telephone notification. Affected parties must be notified either by email or written notice. If the cost of notifying personnel exceeds the breached party's resources (Alabama defines this as a cost in excess of $500k), more than 100,000 people have been affected, or there isn't enough contact information available to reach affected parties, substitute notification options include posting conspicuously on affected parties' websites over a thirty day period, or providing breach notification to major media broadcasting agencies including urban or rural outlets where affected parties may live.

Exceptions include entities who are subject to other laws. When said entity maintains idiosyncratic requirements reflecting those laws, gives proper notice considering those laws, and lets the AG know what happened ASAP should more than 1,000 individuals be affected, that entity is in compliance.

Other thorough laws to which an entity with associated data is subject to provide an exemption from the larger law. This is only available if the business/individual in question follows those secondary laws, provides notice accordingly, and notifies the AG when more than 1,000 persons are affected.

If law enforcement determines an investigation will be impeded, the delay is allowed. If national security may be affected, delay of notification is also allowed. In Alabama, government entities are additionally subject to this law and so must provide notice accordingly. Alabama's AG has the authority to pursue a civil action for penalties which go against these legal rulings, and this can include anything from fines to total dissolution of a given entity.

ALASKA

Statute Codes

Alaska Stat. § 45.48.010 et seq., passed under H.B. 65 and signed into law on June 13, 2008, went into effect July 1, 2009. Specific information pertaining to Alaska breach laws can be found in chapter 92, SLA 08. These requirements are referred to under the Personal Information Protection Act.

Legal Requirements and Purpose

In Alaska, any individual, local or state agency, or situation where more than ten employees are presided over by a responsible party, constitute an entity affected by this law. This is provided they license PI of Alaska residents. Application of this law extends to businesses or individuals not local to Alaska, but who manage PI on residents in the state.

A security breach transpires when unauthorized PI is acquired which compromises a resident in terms of security, integrity, or confidentiality. This data is acquired from the entity responsible for the PI without that entity's consent. Acquisition of PI that happens in good faith isn't constituted as a breach, provided the information isn't misused.

PI refers to information of any sort about an Alaskan resident which has no encryption, or which has not been redacted. It may be encrypted, but keys to such encryptions have become available through a breach. PI includes a first name and last name, or someone's first initial and last name, and data associated with that name such as SSNs, personal ID numbers, state IDs, or driver's licenses. Any account number of a financial kind, or password associated with an account, is also included. PINs, passwords, or other codes are PI.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

In the event of PI breach, the entity must let any affected Alaska residents know. Entities aren't required to report if they investigate in agreement with legal requirements and notify the AG. This is provided, of course, the investigation demonstrates consumer PI affected won't damage those it belongs to. Documentation is required and must be reasonably updated over a period of five years.

Regulatory agencies should be notified if more than 1,000 Alaska residents have PI affected by the breach. Primary consumer credit reporting groups need to be appraised of breach distribution, content affected, and associated timing.

This disclosure must take place in a reasonable timeframe. The quickest disclosure possible is specified. Allowable delays involve investigation requirements and network integrity resumption. When disclosure and notification take place, methods that are allowable under the law include telephone, written, and electronic notice--provided electronic options agree with legal definitions of the E-Sign Act (5 U.S.C. § 7001).

An entity that can demonstrate notification will cost more than $150,000, or that more than 300,000 AK residents have been affected, or there isn't enough contact information on affected parties, can use email notices, conspicuous posts on entity-run websites, and major media notification.

Associated Penalties

Entities can be fined up to $500 per resident for those who aren't notified. The maximum penalty that can be leveled is $50,000. This is a civil penalty paid to the state. Additional violations can be enjoined. In Alaska, private lawsuits are allowed. Damages are limited to economic impact and associated attorney fees. Regulatory actions are allowed, but only as pertains to government agencies.

Exceptions/Exemptions

Alaska has no HIPAA compliance exemption. Encrypted PI does not incur penalty of law (provided decryption info isn't compromised), and Alaska's judicial branch is excluded. Entities compliant to the Gramm-Leach-Bliley Act are also exempted.

If there's an investigation by law enforcement taking place, notice can be delayed should it be determined such notification would impact said investigation.

ARIZONA

Statute Codes

Breach laws in Arizona are under Ariz. Rev. Stat. § 44-7501, including S.B. 1338 (Chapter 232), and H.B. 2154 (Chapter 177). S.B. 1338 was signed into law April 26, 2006 and became effective in December of that year. H.B. 2154 was signed into law April 11, 2018 and became effective as of August 3, 2018.

Legal Requirements and Purpose

This law applies to an entity either individual or plural conducting Arizona business which maintains or licenses PI in computerized form. PI covered must either be unencrypted, unredacted, or both to be regulated under these laws. Entities that aren't local, but have PI on state residents, are subject to this statute.

A PI breach is when data acquisition that's not authorized or in good faith takes place, and computerized PI is involved.

PI is defined as the first name and last name, or a first initial associated with a last name, that is attached to other critical information. Critical information includes SSNs, driver's license or state ID numbers (pursuant to § 28-3166 and § 28-3165), financial information (credit/debit cards, account numbers, access codes, passwords, etc.), private authentication keys, health insurance numbers, medical or mental health data, passport information, tax IDs or EINs, or any unique data of a biometric kind. Additionally, usernames and email addresses coupled with passwords or security questions are PI. PI doesn't define publicly available information lawfully revealed at federal, state, or local government levels to the public, or which has been made public by media outlets.

Time Frames
Breach Reporting, Regulation Reporting, Client Notification

Arizona law requires an entity managing PI to notify affected individuals no later than 45 days from the time it's determined a breach has occurred. Notification may be delayed for prompt investigation of the breach cause, and what that investigation uncovers. If no PI is affected, or only encrypted PI has been affected, or the investigation determines no damages can be reasonably expected, notification isn't needed.

Should post-investigative determination identify 1,000 or more individuals who must be notified, then the AG must also be given written notification. There may be a form as prescribed by the AG to fill out. Also, a copy of notifications sent to individuals affected can be used. Consumer reporting agencies must also be reported for breaches involving more than 1,000 residents. Additionally, the nation's three most prominent national consumer reporting agencies must be contacted. Should entities manage information from a third party, but not own it, the third party must be contacted, and must cooperate with whichever licensee owns that data. Whoever owns that information isn't required to notify the affected individual unless there's a stipulation in the agreement.

Notice can be provided in written form, by telephone including actual contact of affected parties, or email address if it's available. The notification should include when the breach happened, what PI was affected, and contact information including phone numbers and addresses of the big three credit reporting agencies. Should the breach merely involve online credentials and nothing else, entities presiding over the information can contact affected parties via email and prompt them to change login information or take other applicable measures. If entity-furnished login information is affected, the entity must contact affected individuals as deemed appropriate, and require login data reset that is appropriately comprehensive (including security questions, passwords, or whatever else is necessary).

If notification will cost the entity $50,000 or more, or over 100,000 individuals in AZ have been affected, or there isn't enough contact information for notification, substitute contact methods include written letters to the AG demonstrating these facts, a conspicuous post on the entity's site, and statewide media notification.

Associated Penalties

Violation of this act is enforced by the AG, pursuant to ARS 44-1522. Civil penalties of $10,000 per affected individual can be enforced. Economic losses sustained by parties affected by the breach must be covered. Maximum civil penalties from a breach or a series of them aren't allowed to go higher than $500,000.

Exceptions/Exemptions

Compliance to state regulatory guidelines is sufficient. Compliance to the Gramm-Leach-Bliley Act make it so entities so-covered aren't required to concern themselves with the previously explored statutes. Entities covered under HIPAA are not required to follow these statute's provisions, provided HIPAA compliance is maintained. If an entity maintains their own PI management policy that complies with state timetables pertaining to notification, and notifies affected parties properly after a breach, this is allowed.

Notice can be delayed should local law enforcement determine that a criminal investigation will be impeded; however, within 45 days of the close of that investigation, notification must take place.

ARKANSAS

Statute Codes

The Personal Information Protection Act in Arkansas is outlined under Ark. Code § 4-110-101 et seq.: S.B. 1167, act 1526 was signed into law as of March 31, 2005, and became effective August 12, 2005.

Legal Requirements and Purpose

This law pertains to entities (including individuals, businesses or state agencies) that either acquire, own, or license computerized data containing PI. This applies specifically to Arkansas resident data, regardless if the entity is local to Arkansas.

An Arkansas security breach is when resident PI data is acquired in an unauthorized way, and not in good faith. The data must in some way compromise integrity, security, or confidentiality of affected parties.

PI is defined as a first and last name, including first initials, in combination with other pertinent information. That information can include SSNs, driver's license and ID numbers, financial data like account numbers, passwords, PINs, or anything else compromising financial activity, or medical information.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

When a breach is discovered, an entity must inform affected Arkansas residents as soon as reasonably possible. If an investigation proves no reasonable expectation of harm, notification isn't necessary. If the entity manages information owned by a third party, that third party must be notified in the event a PI breach occurs--provided it's feasible an unauthorized individual has acquired this PI.

Notice can be given in writing, or by email provided said email outreach follows the E-Sign Act (15 U.S.C § 7001). If it can be demonstrated notification will cost the entity $250,000 or more, or that more than 500,000 people have been impacted by the PI breach, or there isn't enough contact information to reach affected parties, then substitute notice options can be used. These include email notices when appropriate, conspicuously posting notification of the breach on entity-maintained websites, and notification of statewide media.

Associated Penalties

Penalties are enforced by the AG and may include associated legal action depending on AG prerogative(s).

Exceptions/Exemptions

Entities maintaining notification procedures pertaining to PI breach which are consistent with statute timing will be considered compliant to the statute. This is provided affected persons are properly notified in the event of a breach.

If local law enforcement determines notification will adversely impact their own investigation, notice may also be delayed until such time as investigation is no longer deemed in jeopardy.

CALIFORNIA

Statute Codes

In California, there are quite a few applicable breach laws covered under Cal. Civ. Code § 1798.29; 1798.80 et seq.

S.B. 1386 was signed into law September 25, 2002 and made effective July 1, 2003. S.B. 24 was signed into law August 31, 2011 and made effective January 1, 2012. S.B. 46, was signed into law September 27, 2013, and made effective January 1, 2014. AB-1710 was signed into law September 30, 2014 and made effective January 1, 2015. Additionally, A.B. 964, S.B. 570, and S.B. 34 were signed into law on October 6, 2015, and became effective January 1, 2016.

Legal Requirements and Purpose

This law applies to entities (persons, businesses, and state agencies) who own or license computerized data which includes PI. Even if the entities are located out of state, if they have PI of California residents, associated law applies to them.

A security breach takes place when a party or parties obtain access to PI without authorization. Good faith provision of PI isn't a breach, provided the PI isn't misused under the statute's guidelines. The PI breach must threaten security, integrity, or confidentiality of affected parties.

PI is defined as a first and last name, or a first initial coupled with a last name, proceeded by sensitive information. If this data is unencrypted and becomes available, that's a breach. Examples of associated sensitive information include SSNs, driver's license and state ID numbers, any financial information like account numbers, PINs, or passwords, medical information, health insurance data, or information that's been collected through a license plate recognition system that's automated. Pertaining to license plate recognition, specifically, this refers to a database resulting from cameras that utilize algorithms to categorize license and registration data. Also, PI can be a username in conjunction with an email address, password, or security question. PI doesn't include information made available lawfully to the general public at state, local, or federal levels.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Entities covered under the statute must notify affected CA residents when unencrypted PI was or is believed to have been compromised. They must notify residents if encrypted data is compromised which may include a decryption key. Reasonable suspicion of compromise also predicates notification obligation. The AG must be notified if more than 500 California residents are compromised. This is done through electronic submission of the notification as it is intended to be distributed to affected parties. This submission will constitute a sample, and not contain any contact information of affected parties. Should the entity manage data it doesn't own for a third party, they must notify that third party of any PI breach as soon as it has been discovered; or there is good reason to expect unauthorized parties have acquired access.

Notification must take place as swiftly as possible, avoiding any delay deemed unreasonable by the statute. When law enforcement or investigation requires a delay in notification, this is permissible. Restoration of a network's integrity is also a permissible delay. The means of notification may be through written or electronic notice, provided electronic outreach is in compliance with the E-Sign Act (15 U.S.C. § 7001). If an email address is breached, notice may not be provided by this method. Additional means of notification include direct notification to residents at a trusted IP address and location.

Additionally, conspicuous posts to affected parties on a website run by the entity can serve as notice, but California requires a format be followed. Such posts must include

the date the notice was put up, the entity's name and contact info, what sort of PI was compromised, when the breach occurred or was estimated to have occurred, if law enforcement impeded notification, and a description of what happened if that's legally feasible. Additionally, toll-free telephone numbers and addresses of major credit reporting agencies must be provided if SSN information or ID information is compromised. If the entity providing the breach is also its source, they must offer to provide identity theft solutions at no cost for at least a year, including necessary information for affected parties to take full advantage of this offer. This is required if SSNs or identification numbers are compromised. The entity may choose to include information about what has been done to prevent further breaches, as well as advice pertaining to what California residents can do to protect themselves in the future.

If a breach only compromised login data for an email address or something similar, notice can be sent out as an advisory for affected parties to update passwords or security questions. Additional steps may also be given to affected parties through such a notification. It is to be titled "Notice of Data Breach". Five specific headings are to be used: "What Happened", "What Information Was Involved", "What We Are Doing", "What You Can Do", and "More Information". Formatting of this notice must be designed to emphasize the sort of data breach, and how significant it is. This must be clear and obviously conspicuous. Text cannot be smaller than 10-point type. The statute provides a model that entities can use to inform such notifications.

If the breached entity can demonstrate notification cost exceeds $250,000 and 500,000 affected parties, or there isn't enough contact information, substitute notice options must include at least three specific tactics. When email addresses are available, these must be used. Additionally, for no less than 30 days, the entity's website must make a conspicuous post including a link to the notice on its most significant page. This must be in larger type than surrounding text, and contrast with the rest of the page in terms of size, color, or font as to be appropriately conspicuous. Symbols can help set it apart. Lastly, statewide media must be notified. For state agencies that are using such substitute notice tactics, the California Office Of Information Security must also be notified. This office is within the Department of Technology.

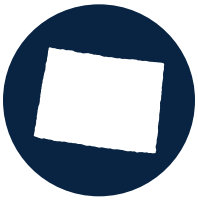
Associated Penalties

Any client of an entity that's injured by violations of this statute is entitled to civil action for damage recovery. Businesses that violate, or make a proposition to violate, or who have violated this statute could become enjoined. Waivers are not permitted.

Exceptions/Exemptions

Should an entity maintain internal notification procedures pertaining to a PI policy which conforms to timing and other guidelines of the statute, that entity will be held in compliance--provided proper notification under associated policies takes place.

HIPAA-covered entities, as of January 1, 2012, will additionally be considered compliant to state law should they be in agreement with notice guidelines in HITECH (Health Information Technology for Economic and Critical Health Act) Section 13402(f). If there's a delay for law enforcement investigation, that's allowable; provided notification takes place as fast as reasonably possible when law enforcement allows.



COLORADO

Statute Codes

Colorado data breach laws are covered under the Colorado Consumer Protection Act, including Colo. Rev. Stat. § 6-1-716. This extends to H.B. 1119, which was signed into law April 24, 2006, and which became effective on September 1, 2006, as well as HB 18-1128, which was signed into law May 29, 2018, and became effective September 1, 2018.

Legal Requirements and Purpose

Entities are defined as persons, businesses, or state agencies which either license or manage PI that has been computerized. Whether or not a given entity is located in Colorado, or conducts business there, this statute applies to them if they have information on the state's residents.

A breach is defined as when PI that could compromise its owners in terms of integrity, security, or confidentiality is acquired by unauthorized access. Good faith data distribution isn't a breach, provided the data isn't misused.

PI refers to when the first and last name, or the first initial and last name, of an individual is leaked in relation to sensitive data. A PI breach occurs if the PI isn't encrypted, if encryption keys have also been compromised, or if PI details in affected information haven't been secured, redacted, or otherwise safeguarded to be unreadable. Information attached to a resident's name includes SSNs, ID numbers (including military IDs, passports, and driver's licenses), medical information, health insurance numbers, or biometric information. Additionally, login information for email addresses is PI, including security questions. As well, any financial data permitting access to digital assets is PI. PI doesn't include information made lawfully available to the general public at local, federal, or state levels; or as distributed widely by the media.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

An entity must contact parties affected by a PI breach as soon as it's feasibly

possible to once the breach, or reasonable suspicion of the breach, is determined. Should a good-faith, swift investigation determined no harm from the breach which could result in PI exploitation, notification isn't required.

The AG must be notified should 500 or more residents of Colorado be affected. This notice must be provided no more than 30 days from the time a breach has been determined. This window is in consistence to measures taken to ascertain the scope of a breach or restore system functionality of affected computer networks. Also, all consumer reporting agencies who keep records on consumers nationally are to be notified should more than 1,000 residents be affected. If the entity manages data for a third party which it does not own, and which includes PI, corresponding notice of a breach must be provided to that third party as soon as reasonably possible.

Means of notification include written notice at supplied postal addresses within entity reach, telephone notice, or electronic notice--provided said electronic notice is in compliance with the E-Sign Act (15 U.S.C. § 7001). If the email address of an affected party is compromised, that email can't be used for notice. Electronic notice in this instance must consist of notifying the affected party on an IP address or other trusted online location said affected party customarily frequents. The notice must have several elements. It must include the date or estimated time of breach, what sort of PI was affected, info affected parties can use to contact breached Entities, toll-free phone numbers, addresses, and websites of major credit reporting agencies as well as the FTC (Federal Trade Commission), and a statement which informs residents they can get information from the FTC and credit reporting agencies pertaining to fraud alerts or security freezes. When online credentials are breached, in addition to this information, entities must give affected parties notice that login information must be changed, and appropriate protection steps must be taken to counteract online areas where PI was compromised.

If the entity can demonstrate notification costs will be more than $250,000, or more than 250,000 residents of Colorado have been affected, or there isn't enough contact information available for contact, there are additional substitute notification requirements. All of these must be used: email notice if applicable, conspicuous posts on entity-maintained websites, and statewide media notification.

Associated Penalties

The AG can seek both injunctive relief and direct damages from the entity to affected parties according to the situation.

Exceptions/Exemptions

Notification of consumer reporting agencies at a threshold of 1,000 affected parties isn't required, but only if breached entities conform to Title V of the Gramm-Leach-Bliley Act. Third-party notification does not require the entity to disclose any trade secrets or other confidential information.

Should internal practices include protocols which enforce security policies that agree with this statute, including associated timeframes, entities will be deemed in compliance.

Delay in notification is allowed should law enforcement determine notification may impact criminal investigation, or investigators tell an entity not to notify anyone.

CONNECTICUT

Statute Codes

Breach notification law in Connecticut is gathered under the Banking Law of Connecticut, Connecticut Gen. Stat § 36a-701b, which includes several different aspects. S.B. 650 became law on June 8, 2005 under public Act 05-148 and became effective January 1, 2006. Six years later, H.B. 6001 became law as of June 15, 2012, under Public Act 12-1, and went into effect October 1, 2012. Lastly, S.B. 949 was signed into law June 11, 2015, and became binding on October 1, 2015.

Legal Requirements and Purpose

Connecticut breach notification law applies to entities defined as individuals, agencies, or businesses that regularly maintain, license, or own any PI data. Additionally, entities exterior to Connecticut which contain PI on citizens of Connecticut are included under this statute.

A security breach is defined as access to anything containing PI in an unauthorized way. Should access to such data happen in good faith, it isn't defined as a breach if such data is additionally used in good faith. If a breach occurs but investigation determines it wasn't harmful, breach notification isn't necessary. In Connecticut, you must consult with any relevant local, federal, or state agencies who enforce such laws before making such a determination. If it should develop that notification is necessary, the AG must be notified no later than affected parties are--sooner is better. If third parties are involved--meaning they've got PI, you manage as an entity which may be compromised--then they must be notified as well should this be determined necessary. The faster you can notify them, the better; but there are reasonable delays as scope is being determined, and system's functionality is being brought back online.

PI is defined by Connecticut as the first name and last name, or the first initial and last name, of a citizen combined with additional data such as SSNs, driver's licenses, state IDs, or any information associated with finances. Credit card numbers, debit card numbers, bank accounts, or access information to bank accounts, is considered PI. Information that's already been made legally available to the public through government records at local, state, or federal levels is not PI. Media that has been widely distributed is also not PI.

A special note for Connecticut pertains to Bulletin IC-25, put into place on August 18, 2010. Any licenses or registrants involved in the Connecticut Insurance Department must notify said department pertaining to data security which affects residents of Connecticut when applicable incidents are identified. This can be done no later than 5 calendar days from when identification of the incident happens.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification must be made without unreasonable delay. Re-establishing normal operations and investigating what initiated the breach are considered reasonable. Also, an investigation into
responsible parties is permissible, should it take no longer than 90 days. 90 days is the upper limit after a breach has been discovered, unless there are federal laws in application which require less time. In that case, the federal laws will take precedence.

Notice must be given either in written, telephonic, or electronic form, provided electronic means of notification conform to the E-SIGN Act (15 U.S.C. § 7001). In Connecticut, if the SSN is compromised by a PI breach, the law requires that the party who was responsible to prevent the breach provide services in identity theft protection. Additionally, associated mitigation may be necessary. No cost is allowed for these services for at least a year. All info for enrollment must be provided to all affected citizens, including how a credit freeze on a resident's file can be put into effect.

Should an affected entity be able to demonstrate the cost of giving notice to affected persons would be $250,000 or more, or that more than 500,000 people were affected, or there isn't proper contact information available, there are three steps that must be taken. Email of the notice must be sent out to all affected parties when such contact information becomes available. Second, on the website of affected entities (if such a site is maintained), it's necessary to make a conspicuous notification regarding the data breach that's visible to any visitors. Lastly, newspapers, television, radio, or any other applicable statewide media must be notified.

Associated Penalties

Breach notification in Connecticut is enforced by the AG, who is authorized to seek both injunctive relief and direct damages as applicable.

Exceptions/Exemptions

Entities who operate under their own notification policy can provide breach notification in accordance with such internal PI protocols. This is only allowed provided such entities comply with existing Connecticut laws, and notification of affected persons follows associated timeframes.

Any breach notification which is pursuant to guidelines, laws, regulations, guidance, or rules as put into place by state regulators in effective operation is permissible. Also, should law enforcement delay notification under concern that it could impede an ongoing criminal investigation, this is permissible, provided notification takes place immediately the entity has been given authorization to notify affected persons.

DELAWARE

Statute Codes

Breach notification in Delaware is covered under a section of state law called Computer Security Breaches. The official designation is Del. Code Ann. tit. 6 § 12B-101 et seq. It includes H.B. 116, which became law June 28, 2005, and was rendered effective June 28, 2005. H.B. 247 is also included, and was made law June 10, 2010, and signed in the same day. Also, Delaware's Computer Security Breaches law includes House Substitute 1 for HB 180, which was signed in August 17, 2017, and made effective April 14, 2018.

Legal Requirements and Purpose

Laws pertaining to breach notification in Delaware apply to entities. Entities include individuals, partnerships, corporations, business trusts, LLCs, associations, governments, joint ventures, subdivisions of government, government agency or instrumentality, corporation of a public kind, or basically any operation or individual defined as an entity in the legal or commercial sense. Delaware law additionally applies to entities exterior to the state who may manage PI of state residents. If you've got any PI on Delaware residents, breach notification laws apply to you.

Delaware describes a security breach as unauthorized access of computerized PI; specifically: data which involves integrity, security, or confidentiality of that PI. If PI is encrypted, and it is accessed in an unauthorized way, this isn't a breach unless those who have obtained such encrypted data can decrypt it. If there's a reason to believe someone can decrypt the encrypted data, breach notification is also required. If you suspect there's a decryption key out there, you'd better notify the proper parties. However, good faith acquisition of PI isn't a breach, provided it's also used in good faith.

PI in Delaware is a person's first name or initial, last name, and information coupled to that. Information included with a person's name can include SSNs, driver's licenses or any sort of ID, account numbers or any financial information, passport numbers, email address/username combinations including security questions, medical records of any kind, health insurance policy numbers, biometric data, or tax ID numbers.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

It's required in Delaware that breach notification take place should PI of any Delaware resident be compromised, or if entities can reasonably believe such data may have been compromised. If, after investigation appropriately conducted, it is determined breached data won't threaten affected parties, notification isn't required.

If there are more than 500 residents affected, the entity must contact the AG. This contact must happen no later than the notification of affected residents, and ideally sooner. Credit monitoring services must also be provided should a DE resident's SSN be compromised. You must, under the law, provide credit monitoring services for a year, for free, if an SSN has been compromised or is believed to have been compromised. Also, Delaware law requires entities to give affected individuals all the information they need to enroll in such credit monitoring services and help them understand how to place a credit freeze on their file. Again, if investigation shows harm won't come to affected individuals, notification isn't necessary.

Pertaining to third parties, if an entity who has PI for them when a breach happens must let them know as soon as reasonably possible. If it's feasible, this notification should be sent out immediately once a breach has been identified. This notification should include cooperation with third parties and sharing of licensee information if such sharing becomes necessary. Such notification can't be made later than 60 days in Delaware. If there's a shorter federal law, then that takes precedence. If it can't be determined within 60 days that PI was compromised in a breach, then the entity must, as soon as it is feasible to provide notice to affected residents. This is unless substitute notice, which will subsequently be defined, has already been given.

Notice can be provided through written, telephonic, and electronic notice provided it's in agreement with the E-SIGN Act (15 U.S.C. § 7001). If login data like emails and password combinations are breached, as an entity you can't email the compromised address. Other permitted methods must be used, which may include a conspicuous notice of a breach given to the affected party on the web when it can be determined they're online; or the notice being sent to a trusted IP where it's known such a person accesses their account.

Should it be determined that the cost of providing notice exceeds $75,000, or more than 100,000 residents, or there's no contact information of affected parties, then three substitute notice efforts are required. Email must be sent out, if you manage a web page you've got to make a conspicuous post on your site, and any major statewide networks must additionally be contacted. This includes social media platforms, radio, television, newspapers, or anything else which applies at the time of the breach.

Associated Penalties

The AG can bring action in address of any violations pertaining to this law. The AG may additionally seek other relief if it is determined this is necessary to either facilitate compliance, or secure economic damage recovery for parties affected by the breach.

Exceptions/Exemptions

Breach notification may be provided in conformity to internal notification policies already in adherence to existing laws as regards time and contact requirements.

Additionally, there's the Gramm Leach Bliley Act, as amended (15 U.S.C. § 6801 et seq.), and HIPAA; or the Health Insurance Portability and Accountability Act. HIPAA came about in 1996, and as amended can be referenced under P. L. 104-191. If the entity complies with the rules by primary and functional federal or state regulators, and the entity notifies residents in accordance with such procedures, this is permissible.

Should law enforcement be conducting a criminal investigation and determine that delay of notification is necessary, this is also permissible. However, as soon as their investigation is complete, notification must be made. This notification must come as swift as can reasonably be expected. Such regulations also apply if there is one specific person in which law enforcement is interested who has had PI compromised, and regarding whom law enforcement determines a delay is appropriate.

FLORIDA

Statute Codes

Breach notification laws in Florida are contained under the Florida Information Protection Act of 2014, Fla. Stat. § 501.171, which includes S.B. 1524 and S.B. 1526. S.B. 1524 was signed into law June 20, 2014 and made effective July 1, 2014. S.B. 1526 was signed into law June 20, 2014 and made effective July 1, 2014.

Legal Requirements and Purpose

That which defines breach notification in Florida pertains to entities, defined locally as proprietorships, corporations, cooperatives, associations, estates, or any other such commercial entity which regularly handles PI. Additionally, any entity contracted under such groups for storage or management of PI on behalf or that entity is included. This contracted party is referred to as a "third-party agent".

A security breach in Florida is when PI of an electronically stored kind is accessed without authorization. Good-faith data acquisition is not a breach, provided it's used right.
Florida defines personal information as the first name and last name, or first initial and last name, of a citizen that is combined with any other sensitive data. Specific Florida PI categories include SSNs, driver's license, passport information, military identification info, or any government document used for identity purposes. Financial information like credit or debit card numbers and bank accounts are included, as is medical information, health insurance information, email addresses, passwords, and security questions related to email addresses. Information that's publicly available at local, federal, and state levels is not defined as PI. Encrypted PI is also not included, provided there is no known or expected means of decryption. Also, encryption which has been heavily redacted--which removes personally identifying details of individuals--is not included as PI.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification must take place if PI has been compromised, or it is believed PI may have been compromised. Should investigation reveal a data breach will not cause harm or identity theft, and that investigation complies to laws pertaining to such investigations, then notification is not necessary. However, the breach must still be documented in writing, and that documentation maintained for at least five years. Additionally, the Department of Legal Affairs (heretofore referred to as "the Department") must be notified in writing within 30 days once a determination has been made. The AG presides over this department and should more than 500 individuals in Florida be affected, they must be notified.

Consumer reporting agencies must be notified if more than 1,000 people are affected. When it comes to third party agents, they must let entities know about a breach as soon as possible, but no later than ten days after determination of a breach has happened. If an entity finds out a third party has been breached, the Department will be notified of individuals who've been affected. Third parties are required to give all necessary information pertaining to the breach to the entity. While third parties can notify the Department to save entities trouble, if a third party doesn't let an entity know, that's a violation against said entity.

The Department must be notified no later than 30 days after it's been determined a breach happened, or there's reason to believe a breach has happened. Affected individuals must be notified as fast as possible. Reasonable delays involve law enforcement restriction, re-establishment of data system functionality, and breach scope determination. However, it's not reasonable to delay breach notification of individuals beyond 30 days. Entities are given 15 extra days if good cause is given in writing by the entity to the Department inside 30 days from when a breach has been determined.

Giving the Department notice can be done through written notice that includes a synopsis of the event, how many people were involved, services entities offer affected individuals in compensation, a copy of the notice that will be sent to affected parties, and contact information from the entity providing notice. This contact information must include name, address, phone number, and email address of the affected parties that can used to reach the entity. If the Department asks, entities must also provide a police or incident report, a copy of breach policies in place, and what steps have been taken to fix the problem. Supplemental information from the entity to the Department may be provided any time.

Notice to individuals must at minimum contain when, or when it's estimated that a breach occurred, what kind of PI was affected, and how affected individuals can contact the entity for questions about the breach and associated PI. Written notice to mailing addresses or email notice to verified email addresses can be used to notify affected individuals.

Substitute notice options are available if notification costs exceed $250,000, more than 500,000 people have been affected, or necessary contact information isn't available. Substitute notification must include both conspicuous posting of the breach on the breached entity's website, if there is one, and notification via broadcast media,

print, or whatever urban/rural notification media is available to affected residences of individuals.

Associated Penalties

If breach notification is determined not to conform to the law, administrative fines apply. Improper notification is regarded as deceptive or unfair trade practice by the state of Florida. It can result in civil penalties up to, but not exceeding, $500,000. Penalties can be up to $1,000 for each undisclosed breach up to 30 days, and $50,000 for each 30-day period where breaches go unreported, up to 180 days, or $500,000. Civil penalties described apply per breach, rather than individual affected per breach.

Exceptions/Exemptions

Breach notification in compliance with other laws, rules, guidance, guidelines, or regulations as established by functioning state registration agencies is excepted. If law enforcement says breach notification will impede an investigation, and so orders an entity to delay, this is permissible, provided notification to affected parties takes place with no unreasonable delay after the fact. Any information the Department receives in compliance with notification regulation requirements is deemed confidential and exempt from Public Records requirements. This is covered under the State Constitution and statutes.

GEORGIA

Statute Codes

Breach notification laws in Georgia are covered under the Georgia Personal Identity Protection act, Ga. Code § 10-1-910 et seq. This includes S.B. 230, and 236. S.B. 230 was signed into law May 5, 2005 and became effective May 5, 2005. S.B. 236 was signed into law May 24, 2007 and became effective May 24, 2007.

Legal Requirements and Purpose

The “entity” covered under Georgia breach notification law is rather extensive. It includes individuals who in whole or in part assemble, collect, compile, evaluate, transmit, transfer, report, or communicate PI of individuals for either monetary fees or dues. Entities who do this for non-affiliated third parties, or for any legal agency be it state, local, or federal, are included. This covers bureaus, public educational institutions, and legal institutions. The statute doesn’t affect government agencies maintaining records primarily as a means of keeping traffic safety. The same is true of law enforcement, or licensing for public access court records to property information either real or personal. The legal definition of “entity” in Georgia applies to non-local parties who manage PI of state residents.

A security breach is when PI is accessed without authorization. Good faith data utility isn't a breach, unless the data is misused, or made subject to any subsequent disclosure of an unauthorized kind.

PI in Georgia is defined as a person's first and last name, or first initial and last name, in combination with data elements such as: SSNs, driver's licenses or other identification numbers, any financial information, any passwords or PIN-numbers/ access codes, or any information sufficient to steal identity of compromised parties. PI doesn't apply to publicly available information made lawfully available at local, federal, or state levels.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

An entity is obligated to provide breach notification in Georgia after a breach is discovered, and to whoever's information was accessed by unauthorized parties. Consumer reporting agencies must be notified should 10,000 or more residents in Georgia be compromised at once. This must additionally be done without unreasonable delay. Should an entity keep computerized data for a third party, they must be notified within 24 hours of breach discovery--provided PI was, or is reasonably expected to have been, acquired by an unauthorized person(s).

Notification must be made as quick as possible and without delay. Determining the scope of a breach, and re-establishing a data system's operational integrity, are determined to be reasonable delays. Means by which affected parties can be notified include either written notice, or electronic notice conforming to the E-SIGN Act (15 U.S.C. § 7001). Substitute notification methods become available should more than $50,000 be required to notify affected individuals, should more than 100,000 parties be affected, or if there isn't available contact information. Substitute notice must include all three of the following methods: email notice if/when an address is acquired, a conspicuous post made to the breached entity's website that's clearly visible (should the entity maintain any sort of site), and notification provided to major statewide media outlets.

Associated Penalties

Private lawsuits are not allowed for PI compromise in Georgia. If PI was encrypted, associated notification laws do not apply.

Exceptions/Exemptions

Breach notification exceptions for Georgia include delays for law enforcement should such an agency determine that notifying affected parties would impede an investigation. As soon as law enforcement allows notification, it must be made.

Additionally, if an entity keeps notification procedures in consistence with timing and notification requirements of existing Georgia statutes, this is permissible--provided notification of affected parties according to such procedures is followed.

HAWAII

Statute Codes

Breach notification law for Hawaii is covered under H.R.S. § 487N-1 et seq., which includes S.B. 2290, and S.B. 2402. S.B. 2290, Act 135, was put into law May 25, 2006. It became effective January 1, 2007. S.B. 2402, Act 19, was put into law April 17, 2008. It became effective April 17, 2008.

Legal Requirements and Purpose

In Hawaii, breach notification pertains to entities owning or licensing computerized PI, paper PI, or any other PI management. Entities are defined as corporations, proprietorships, partnerships, associations, or any variety of group operating at a profit. Financial institutions licensed in Hawaii or the U.S., or other countries, and institutions acting as parent businesses for such groups, as well as government agencies, are also included under Hawaii's definition of entity. Additionally, should an entity not be local to Hawaii, if they have PI on the state's residents, they are included under these statutes' authority.

Security breaches happen when unauthorized persons access PI that's not encrypted or redacted. If a breach is likely to have occurred (or has occurred) and there's risk of harm to a Hawaii citizen, then it is considered a PI data breach. Good faith data acquisition isn't a breach if the PI isn't used improperly.

PI in Hawaii is the first name and last name, or first initial and last name, of a citizen combined with other relevant information; SSNs, driver's licenses, identification card numbers, account numbers, credit card numbers, financial information, or similar items. PI doesn't include information or government records legally available to the public at local, federal, or state levels.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification becomes obligatory if a breach is discovered, or an entity is notified of a breach. Should 1,000 or more persons be affected, the AG must be notified. Also, the Office of Consumer Protection in Hawaii must be notified pertaining to content, timing, and distribution of the breach. An entity must additionally notify consumer reporting agencies pertaining to timing, distribution, and affected content. This must be done in writing and without any kind of unexcused delay.

For government agencies, a report must be given to local legislature within 20 days of a breach discovery. This report must show what happened, how many were affected, include a copy of the breach notification sent to affected parties, note whether law enforcement delayed reporting, and detail what preventative measures have been taken in response. If law enforcement restricts notification owing to investigation the 20-day period comes into effect from the time the investigation ends. If an entity

has data on Hawaii's residents that isn't owned or licensed, whoever owns that information must be notified pertaining to PI breach immediately upon its discovery. Timing in all categories here must not incorporate unreasonable delay. Acceptable delay is time to collect contact information, determine how big the breach was, and restore affected systems to integrity.

Permissible means of notifying affected persons involve written notice to their most recent address, telephone where actual contact is made, email notice, and electronic notice in compliance with the E-SIGN Act (15 U.S.C. § 7001). Notice must be clear and straightforward. It must include a description of the incident generally, what PI was affected, what the entity has done to fix the problem, telephone contact information to affected persons from the entity for additional help, and advice pertaining to future action in the wake of the breach; such as reviewing financial statements or credit reports.

Should the entity be able to show notification costs are more than $100,000, more than 200,000 persons were affected, or proper contact info for affected parties isn't available, or if some affected parties can't be identified, substitute contact methods are permitted. Substitute contact methods are permissible for specific persons who aren't normally accessible, too; but only those which can't be notified as per regular methods. Substitute methods must include email notice when available, conspicuously posting about the event on any entity-run websites and notifying of well-known statewide media outlets.

Associated Penalties

Breach notification laws are enforced by Hawaii's AG. Violations of these laws are subject to as much as $2,500 per violation.

Exceptions/Exemptions

Breach notification exceptions for Hawaii include groups complying to the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer notice. This notice came about on March 7, 2005. Additionally, HIPAA-governed entities are accepted provided they remain in compliance to HIPAA.

Delays in notification are allowed for law enforcement agencies conducting criminal investigations. However, request for notification delay must be made in writing. Otherwise, the entity must document such requests, including which law enforcement personnel were involved, and their associated law enforcement agency. This notice must be made as swiftly as reasonably possible after notification delay is commanded by law enforcement.

Waivers are not permitted.

IDAHO

Statute Codes

Breach notification in Idaho is covered under Idaho Code § 28-51-104 et seq. This includes Chapter 258 of S.B. 1374, put into law March 30, 2006, and made effective July 1, 2006. It also includes H.B. 566, made law March 31, 2010, and rendered effective July 1, 2010.

Legal Requirements and Purpose

In Idaho, breach notification pertains to any entity licensing or owning computerized PI on state residents. Entities are defined as individuals or commercial groups. Out-of-state entities are included if they license information on Idaho residents, whether or not they do business in Idaho.

A security breach is when acquisition of PI happens illegally, and in such a way as to compromise integrity, security, or confidentiality of the individual it pertains to. This information must be unencrypted, and good-faith acquisition isn't a data breach--provided data is also used in good faith.

PI is the first name or initial and last name of an Idaho resident combined with other identifying information. This includes SSNs, driver's license or other ID numbers, and financial information like account numbers or credit/debit card numbers. Also included are financial account passwords and security questions. PI doesn't include information available to the public legally, or government records that can be legally accessed at state, federal, or local levels.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Idaho entities are obliged to provide breach notification as swift as possible to affected Idaho residents. If a swift investigation determines no harm or potential harm from compromised resident PI, notification isn't required. Awareness of a breach predicates notifying the AG's office within 24 hours. Additionally, IT Resource Management Council policies require a certain state agency report security breaches to the office of the CIO within the administration department.

If an entity keeps computerized PI it doesn't license or own and is compromised, then the entity must cooperate with its licensee/owner, giving swift notice immediately after breach discovery, or the suspicion of possible PI compromise. Sharing relevant information is included under the definition of cooperation.

Notice can be given through written method to recent addresses of affected persons, telephonic notice, or electronic notice complying to the E-SIGN act (U.S.C. § 7001). If cost of notification is greater than $25,000, more than 50,000 Idaho residents have been affected, or requisite contactinformation isn't available, substitute notice

must include three primary notification methods: email notice to available email addresses of affected parties, a conspicuous post on the Entity's website (if they have one), and notice to statewide media outlets that are well known.

Associated Penalties

Failure to exercise proper breach notification protocols in accordance with Idaho laws can result in a fine no greater than $25,000 per breach. The wording of the law defines failure to provide notification as an "intentional" choice. Also, if it can be proved a government employee intentionally disclosed PI illegally, that employee is subject to a fine no greater than $2,000, a one-year county jail sentence, or both.
Primary state regulators are authorized to enjoin the breached Entity from further action and bring a civil action against entities believed to have violated statutes through notification compliance failure.

Exceptions/Exemptions

Breach notification compliance to state regulators is permissible. Also, an Entity that has its own internal security policies for PI consistent with the timing of state law and which properly notifies affected residents in the event of a breach, will be held in compliance.

Law enforcement delay is permissible if authorities determine notification may impede investigation, provided notification takes place as soon as its reasonably possible to expect once the investigation has ended.

ILLINOIS

Statute Codes

Illinois breach notification codes are lengthy and covered under the Personal Information Protection Act, 815 Ill. Comp. Stat. 530/5, 530/10, 530/12, 530/15, 530/20, 530/25. This includes H.B. 1633, Public Act 94-36, made law June 16, 2005, and made effective June 27, 2006. It includes H.B. 3025, Act 97-483, made law August 22, 2011, and made effective Jan 1, 2012. Lastly, it includes H.B. 1260, made law May 6, 2016, and made effective January 1, 2017.

Legal Requirements and Purpose

Breach notification in Illinois covers entities dealing with nonpublic PI they own or license pertaining to Illinois residents. Data collectors, government agencies, private/public corporations, public/private universities, retailers, financial groups, or anyone else dealing with such information is an "Entity" under Illinois statute codes. Entities out of state managing PI of Illinois residents are included in this law.

A security breach is unauthorized or illegal acquisition of computerized data that could compromise confidentiality, integrity, or security of Entity-maintained PI. PI obtained and used in good faith is not considered a breach.

PI is defined as a person's first name and initial with their last name in combination with other key pieces of data, specifically when this information isn't encrypted, redacted, or made available through digital keys sidestepping varying protective measures. Data in combination with names that is constituted by Illinois as PI includes SSNs, driver's licenses or state IDs, any financial banking information such as credit/debit card numbers or account numbers, medical information or history, health insurance information, or biometric information. Additionally, a username and email address or security question that isn't encrypted/redacted is constituted as PI. Publicly available info made lawfully available, or public government records at state, local, or federal levels, aren't considered PI.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification becomes necessary at no charge upon breach discovery. Illinois may report unauthorized acquisition of PI or its use through a third party necessitates notification, even if the entity doesn't have ownership or materiality in reference to that data. State agencies with PI who've been breached, even if it's written PI, must submit a report within five days of breach discovery. This notification goes to the General Assembly, lists the breach(es), and summarizes preventative measures taken against any future compromises. Agencies submitting reports complying to this statute must additionally annually report all breaches and associated preventative correction tactics.

Pertaining to third parties, entities maintaining or storing such PI data that isn't owned or licensed by them must notify owners immediately after breach discovery. Entities must cooperate with such PI owners by giving notice including approximation of breach date, what the breach was, and what steps information owners should take as a result.

Expedient notification disclosure is mandated, barring reasonable delay such as scope determination, restoration of systems integrity/security, or systems confidentiality restoration. Means of notice include written notice, and electronic notification conforming to the E-SIGN Act (15 U.S.C. § 7001). When email, security questions, or passwords are affected PI, notification in "electronic or other form" is permitted. When PI breach involves email login info, other electronic notice to such residents is allowed, including advice to promptly change such login information and protect potentially affected online accounts. Notice beyond security questions, passwords, and email addresses must include several things. Toll-free phone numbers and addresses of proper reporting agencies, the website, toll-free number, and address of the Federal Trade Commission (FTC), and a statement informing affected persons they can get information regarding security freezes and fraud alerts from such sources. The number of parties affected by the breach will not be included in the notification.

Substitute notice options are available should notification expenses be demonstrable by the entity to cost $250,000 or more, 500,000 or more residents be affected, or contact information for affected parties not be available. Substitute notice must include all three of the following tactics: email notice where applicable, a conspicuous posting about the breach on entity-maintained websites, and major statewide media notification. If geographic areas are affected, notice can be given to prominent media outlets in that area, should this be reasonable.

Associated Penalties

Waivers for breach notification are not permitted in Illinois. Violating this statute is illegal under the Consumer Fraud and Deceptive Business Practices Act of Illinois and will be prosecuted accordingly.

Exceptions/Exemptions

Breach notification exceptions for Illinois exist when an entity has their own internal PI breach policy which already conforms to existing laws in terms of timeframes and affected party notification. Additional exemptions include HIPAA-compliant entities. Also, the Health Information Technology for Economic and Clinical Health Act (HITECH) includes notification provisions that are permissible, but only if the entity gives breach notification to the Secretary of Health and Human Services and AG within five days of notifying the Secretary.

If law enforcement mandates delay for investigation purposes, this is permitted as a reasonable notification delay provided the entity being investigated notifies affected parties immediately upon the investigation's resolution. Also, a written request of delay must be made.

INDIANA

Statute Codes

For Indiana, breach notification is covered under Ind. Code § 4-1-11 et seq.; § 24-4.9-1 et seq., which includes S.B. 503 Act 503, H.E.A. No. 1197 and H.E.B. 1121. S.B. 503 became law April 26, 2005 and was made effective July 1, 2006. H.E.A. 1197 was signed in March 24, 2008, and H.E.B. 1121 was made law May 12, 2009. Both were made effective July 1, 2009.

Legal Requirements and Purpose

Indiana breach notification law applies to entities managing or interacting with computerized PI who have been victims of a data breach. Entities are defined as cooperatives, individuals, business trusts, estates, corporations, general trusts, partnerships, associations, nonprofit corporations, state agencies, organizations

which may or may not be non-profit, or anyone else with such computerized PI. Out of state entities are included under the statute's applicability if they deal with Indiana resident PI.

A security breach is when unauthorized computerized PI is accessed in a way compromising security, confidentiality, or integrity of that information. This includes data transferred to additional media including microfilm, paper, or other transferable data repositories that aren't computerized. Unauthorized device acquisition involving PI is a data breach if the PI isn't encrypted/redacted, or there's some sort of revelatory digital key. Additionally, if that information isn't disclosed, or doesn't remain in the unauthorized person's possession, it's not a breach. Good-faith PI acquisition and use is also not a breach, provided it isn't additionally disclosed.

PI is defined in Indiana as a non-encrypted or non-redacted SSN. Also, a person's first name or initial and last name combined with other defining information is PI. Defining information coupled to an Indiana resident's name includes driver's licenses, state IDs, credit card numbers, financial account information, or security codes and passwords associated with sensitive data. PI doesn't include publicly and lawfully available information or government records at the state, local, or federal level.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification is required after entities discover a breach. Affected Indiana residents must be notified if it's suspected identity deception as defined in Indiana Code § 35-53-5-3.5, fraud, or identity theft. Should an entity make disclosure of this kind, the AG must also be notified of the breach.

Consumer reporting agencies are to be notified by the entity if 1,000 or more consumers are affected. This includes PI of Indiana residents that are affected by a security system breach. Third parties who maintain computerized data for said entity and don't own or license must also be notified. The timing of notification must happen without unreasonable delay. Allowable delays include determination of breach scope, and system's integrity restoration.

Means of notification include mail, telephone, fax, or email if it's available. State agencies have slightly modified notification mandates. Should cost of disclosure be demonstrable by the entity to be greater than $250,000, or more than 500,000 persons be affected, multiple substitute notification methods must be made. These must include conspicuously posting breach notification on entity websites, if there are any, and providing notice to major news reporting agencies that are geographic to where breaches took place.

Associated Penalties

The AG enforces breach notification laws in Indiana. Failure to comply with such obligations is seen as an act of deception. Only state AG action can take place, and can include penalties of injunctive relief, civil penalties, and a fine no higher than $150,0000 per violation, as well as reasonable associated costs.

Exceptions/Exemptions

If an entity has an internal breach notification policy pertaining to PI that is consistent with these statutes, separate notification isn't necessary. Additional exceptions include compliance to the Gramm-Leach-Bliley Act, HIPAA compliance, The USA Patriot Act (P.L. 107-56), Executive Order 13224, The Fair Credit Reporting Act (15 U.S.C § 1681 et seq.), or The Driver Privacy Protection Act (18 U.S.C. § 2781 et seq.). Also, if an internal PI security plan designed by the entity to protect Indiana resident PI is designed and adhered to, including expedient breach notification when applicable, this can be permissible.

IOWA

Statute Codes

For Iowa, breach notification laws are covered under Iowa Code § 715C.1-2. This includes 2007 S.F. 2308, made law May 9, 2008, and made effective July 1, 2008. It also includes 2014 S.F. 2259, made law April 3, 2014, rendered effective July 1, 2014, and 2018 S.F. 2177, which was made law April 10, 2018, and made effective July 1, 2018.

Legal Requirements and Purpose

Breach notification in Iowa must happen when entities managing computerized PI experience a data breach. Iowa entities are defined as owners or licenser's of PI who are public corporations, a government agency, instrumentality, or subdivision, joint ventures, LLCs, associations, partnerships, estates, trusts, business trusts, individuals, or private corporations.

A security breach happens when unauthorized acquisition of computerized PI takes place which may compromise confidentiality, security, or integrity of that data. Any media where such information is stored, including paper, can be considered PI breach if the wrong people acquire it. Good faith PI acquisition and utility isn't a breach. Indiana defines PI as the first name or initial and last name of an individual coupled with other sensitive information. This information can be neither encrypted nor redacted to be a breach. If it is encrypted and there's no decryption key or other revelatory digital agent, no breach has occurred. If PI isn't encrypted or redacted and it's made available, breach has occurred. Information that is PI when combined with other identifying data includes SSNs, driver'slicenses and state IDs managed by government groups, financial information of any kind including debit/credit card numbers, passwords, PINs, account numbers, electronic identification information like bank routing codes or passwords, unique biometric information like fingerprints, retina scans, and anything else relevant. PI doesn't include information that's legally available to the public, or government records accessible at local, state, or federal levels.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

It becomes necessary to provide breach notification after breach discovery or suspicion a breach has transpired. Notification must be made to all affected Iowa residents. Should appropriate investigation determine no harm will come of a breach, notification may not be required; provided, however, documentation in writing concerning the incident and those affected is made and maintained for at least five years.

Notification of third parties maintaining PI, but which entities don't own or license, must take place immediately following breach discovery. Expeditious notification is mandated, but reasonable delays include finding contact information for affected parties, figuring out how big the breach was and restoring data system integrity/ confidentiality. At minimum, the notice must include the following items: description of the breach, when it happened, what PI was obtained, applicable contact information for relevant consumer reporting agencies, and requisite consumer advice regarding incident reports pertaining to identity theft. Such reporting should be made to local legal authorities and Iowa's AG. Notification may be made either by written notice to the latest available address of affected persons, or electronic notice in compliance with the E-SIGN Act (15. U.S.C. § 7001).

If breach notification costs exceed $250,000, more than 350,000 persons in Iowa are affected, or necessary contact information for affected persons isn't available to the breached entity, substitute notice must contain all three of the following methods: Entities must issue email notice when addresses are available, conspicuous posting about the breach must be made on websites if the entity maintains any, and notification of applicable statewide media outlets that are considered major must take place.

Associated Penalties

The AG enforces breach notification law in Iowa and will penalize non-compliance. Under the Consumer Fraud Statute of Iowa, violations are deemed to be an unlawful practice, and can include consequences pertaining to damages of affected parties, and associated injury. Fines can be as high as $40,000 for each violation if found to be appropriate under the Consumer Protection Act. A course of conduct is not considered to be separate and different violations owing to repetition with more than one consumer. The AG can order an entity to pay damages on behalf of those affected by the breach or violation.

Exceptions/Exemptions

If an entity has an internal breach notification procedure that complies with state laws and timeframes, separate disclosure under state statutes isn't required. Also, compliance with other laws will not mandate repeat notification. Federal regulator compliance applies here, more protectiveentity procedures of PI do as well, as does the Gramm-Leach-Bliley Act under Title V, HIPAA compliance, and HITECH compliance (provided the entity follows regulations under Title II, Subtitle F of HIPAA, and Title XIII, Subtitle D of HITECH).

Delay in notification for law enforcement agencies conducting an investigation is permissible, provided breached entities notify affected Iowa persons as soon as law enforcement agencies allow them to, without unreasonable delay. Breached entities are required to give notice of law enforcement notification delay in writing.

KANSAS

Statute Codes

Kansas breach notification is fairly straightforward and can be found under Kan. Stat. § 50-7a01 et seq, which includes S.B. 196, made law April 19, 2006, and made effective January 1, 2007.

Legal Requirements and Purpose

Entities in Kansas are required to provide breach notification should PI of citizens be compromised. Entities are defined as individuals, trusts, partnerships, corporations, associations, cooperatives, government subdivisions or agencies, and anyone else who conducts business that includes the licensing or ownership of computerized PI in Kansas.

A security breach takes place when PI is compromised in terms of confidentiality, integrity, or security through unauthorized access to the data. PI given out in good faith and used in good faith doesn't constitute a breach.

PI is the first name or initial and last name of a Kansas resident combined with other sensitive data like SSNs, driver's licenses, state ID numbers, and financial information like account numbers or credit/debit card numbers. Passwords, security questions, and PIN codes are also PI. Information in state, local, or federal government records, or otherwise lawfully available to the general public, isn't PI.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

It is required for entities to pursue breach notification as soon as reasonably possible after a breach is detected. Should good-faith investigation promptly reveal PI compromised won't result in harm or misuse, notification isn't necessary.

Should more than 1,000 persons be affected by a breach, consumer reporting agencies are to be notified. If an entity manages data owned or licensed by a third party, that third party must also be swiftly notified in the event of a breach. Such notification must transpire as swiftly as possible, allowing for reasonable delays like determination of breach scope, and restoration of data system recovery.

Notice can be provided through written or electronic means, provided electronic outreach conforms to the E-Sign Act (1 U.S.C. § 7001). Substitute options are available should notification cost be greater than $100,000, more than 5,000 people be affected, or contact information not be available. All three of the following must be done in substitution: emails must be sent as applicable, a conspicuous post noting the breach must be made on the entity's site should a website be maintained, and major media with statewide reach must be notified.

Associated Penalties

In Kansas, breach notification is enforced by the AG. An insurance commissioner can also enforce if a breach has happened at an insurance company. Otherwise, the AG can bring actions of law or equity as a means of enforcing compliance. Additionally, future violations can be enjoined.

Insurance companies licensed for Kansas business will be at the sole discretion and authority of the state's insurance commissioner in terms of enforcement should violations take place.

Otherwise, the AG will bring an action in terms of either equity or law as a means of addressing violations and providing appropriate relief. Set determination of fines is not available at this time, but penalties under the Consumer Protection Act may be applied, and these can be as high as $10,000.

Exceptions/Exemptions

Exemptions for breach notification include internal procedures already conforming to existing breach notification law, including associated timing. Multiple notifications aren't necessary if an internal procedure already exists. Additionally, compliance with state or federal regulators is permissible.

Should law enforcement determine notification will impact an investigation, delay is also allowed. Notice must be made expediently after law enforcement determines notification will no longer impede investigation.

KENTUCKY

Statute Codes

Breach notification laws in Kentucky are under KY Rev. Stat. §365.732, including H.B. 232, which became law April 10, 2014, and was rendered effective July 15, 2014. Additionally, H.B. 5 was made law April 10, 2014, and made effective January 1, 2015.

Legal Requirements and Purpose

An entity experiencing breaches negatively affecting PI of Kentucky residents must render breach notification. An entity in Kentucky is defined as an “information holder”. This is any individual or group conducting business throughout the state. NTPs (Non-affiliated Third Parties) are included; this includes public education groups, state or municipal agencies operating for the government, or anyone else that acquires and keeps PI pursuant to a contract.

A security breach is when someone who isn’t authorized accesses PI in a way compromising integrity, security, or confidentiality of data. PI acquired and used through good faith doesn’t constitute a breach.

PI refers to the first name or first initial and last name of a person combined with additionally sensitive data such as SSNs, driver’s licenses, financial account numbers, or credit/debit card numbers and their security questions, PINS, and passwords. For NTPs, personal marks, and biometric data are considered PI in addition to a person’s name when combined with financial information, SSNs, tax IDs, driver’s licenses or state IDs, passport numbers, and health information which individually identifies persons. This information is only PI if it is neither redacted nor encrypted, or no keys to encrypted data have been additionally breached.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification must take place upon breach discovery, as reasonably fast as possible. All affected Kentucky residents must be notified. NTPs breached must contact the AG within 72 hours of breach discovery. Entities who are private have no state regulatory authority notification obligation.

Consumer reporting agencies must be notified when 1,000 or more Kentucky residents are affected, as defined by 15 U.S.C. § 1681a. Timing, how the breach was distributed, and content affected must be included in notification.

If an entity keeps information owned or licensed by a third party, that third party must be notified when a breach happens as quick as possible, within reason. NTPs are required to do the same, but within 72 hours of breach determination. NTPs in federal regulation compliance can do this by giving reports required for such compliance to the proper institutions. The third party--or contracting agency--from there has notification responsibility for those affected.

Reasonable delays include determination of scope pertaining to a breach, and resolution of data system integrity. NTPs are required to notify relevant parties within 72 hours.

Means of notification include electronic notice compliant with the E-Sign Act, 15. U.S.C. § 7001, or written notice. If more than 500,000 Kentucky residents are affected, or the cost of notifying them can be demonstrated to be more than $250,000, three substitute notification methods must be pursued. Any available email addresses of affected parties must be used, a conspicuous post on any websites the breached entity maintains must be made, and statewide media that’s well-known must also be notified.

Associated Penalties

Breach notification enforcement in Kentucky may be subject to specific cases. Two hospitals in Kentucky experienced substantial breaches recently; one where 24,600 patients were exposed at a hospital in Louisville specializing in psychiatry, another at a medical office in Bowling Green, where 5,000 individuals were affected by a missing hard drive's data.

Applebee's had a breach in 2018 which could have exposed financial information (credit/debit card numbers) at its 167 locations nationwide. Fourteen were specifically impacted in Kentucky.

A willful violation could be determined by the court under the Consumer Protection Act in the amount of $2,000 per individual.

Exceptions/Exemptions

Exceptions for breach notification include law enforcement commanding a delay on notification, provided notification transpires immediately when law enforcement officials allow without unreasonable delay. NTPs can only delay 72-hour notification if law enforcement compels them.

Compliance to the Gramm-Leach-Bliley Act, HIPAA, Kentucky Agency, and local regulatory agencies is permissible. Notification requirements pertaining to NTPs as covered in KRS Chapter 61 don't apply to entities in compliance with existing law.

The Kentucky Board of Education can promulgate regulations of an administrative kind, provided they are in accordance with KRS Chapter 13A.

LOUISIANA

Statute Codes

Louisiana Database Security Breach Notification Law is covered under La. Rev. Stat § 51:3071 et seq., which includes several sections. La. Admin. Code tit. 16, Pt. III § 701, S.B. 205 as signed into law July 12, 2005 under Act 499, and made effective January 1, 2006, and S.B. 361, which was put into law May 16, 2018 under Act 382, and made effective August 1, 2018.

Legal Requirements and Purpose

Entities must provide breach notification when necessary. Entities in Louisiana are individuals, partnerships, corporations, sole proprietorships, joint ventures and stock companies, as well as any entity of a legal kind owning computerized PI and doing business in Louisiana. Out-of-state entities maintaining information on Louisiana residents are bound by this law.

A security breach happens should PI be compromised in terms of integrity, security, or confidentiality by unauthorized users. PI given out and used in good faith isn't a breach.

PI is the first initial or first name in combination with a resident's last name and other sensitive data. This other data can include SSNs, driver's license numbers, state ID numbers, account numbers of a financial kind, credit/debit cards, passwords and security questions, passport numbers, or biometric data (fingerprints, retina scans, voiceprints, or anything uniquely biological). PI doesn't include legally available information through government or media distribution.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

A breach notification must happen as soon as reasonably possible once breach has been discovered. All affected residents are to be notified. If reasonable investigation determines affected data won't harm affected parties, no notification is necessary--provided the investigation is both swift and properly extensive. A written copy of such a determination, a 5-year documentation, as well as a copy provided of this investigation to the AG must be made.

The AG must be notified in writing describing the breach when necessary. Notification should go to the Consumer Protection Section of the AG's premises. Notice must include who was affected and sent out within 10 days of Louisiana resident notification. Each day the notice isn't received by the AG will be considered a violation separate from the others.

Third parties who own or license information that an entity manages must be notified as soon as possible, baring reasonable delay. In terms of timing, notification cannot exceed 60 days from breach discovery. Scope, data system's restoration, and measures to prevent additional breach are excusable delays, but not after 60 days. If law enforcement freezes notification for an investigation, written notice inside the 60-day span must be rendered to the AG.

Means of notification include electronic outreach compliant with the E-Sign Act (15 U.S.C. § 7001), and written notification. Substitute methods are available if notification cost is greater than $100,000, or more than 100,000 residents were affected. All the following methods must be used if substitute notice becomes necessary: email to affected parties if email addresses are available, posting of the breach conspicuously on any websites maintained by the entity, and statewide major media notification.

Associated Penalties

Breach notification penalties include civil actions for damage recovery from failure to disclose breach in a timely manner and a fine of no greater than $5,000 per violation. Each subsequent day without AG notification after the 10-day window is another fine as potentially high as $5,000.

Exceptions/Exemptions

Exceptions to breach notification laws include interior PI notification policies which already agree in terms of timing and enforcement--no separate notice from internal procedures is necessary. Additionally, Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, as issued March 7, 2005, allows exceptions to compliant financial institutions.

As earlier noted, law enforcement notification delay is allowed, provided the AG is notified in writing within 60 days pertaining to notification delay, and residents affected are notified immediately upon law enforcement authorization.

MAINE

Statute Codes

Breach notification law in Maine is covered under the Notice of Risk to Personal Data Act, 10 Me. Rev. Stat. § 1346 et seq. This includes L.D. 1671, which became law under Chapter 379 on June 10, 2005, and was rendered effective January 31, 2006, as well as H.P. 672, which was made law May 19, 2009, under Chapter 161, and became effective as of May 19, 2009.

Legal Requirements and Purpose

Entities who experience data compromise must provide breach notification to affected individuals. Entities are defined extensively in Maine, including partnerships, individuals, corporations, LLCs, estates, cooperatives, trusts, associations, government agencies, education systems, the Maine Maritime Academy, private educational institutions, information brokers, or any other group that has business involving PI. Any group keeping info on Maine residents, whether in-state or not, is included under the reach of this legislation.

A security breach is when computerized PI is compromised in terms of integrity, confidentiality, or security by unauthorized users. Good faith PI acquisition and use isn't a breach, provided it isn't given to unauthorized parties.

PI is a first name or initial, last name, and other sensitive data that isn't either redacted or encrypted or acquired with a decryption key. Subsequent sensitive data included here are SSNs, driver's licenses and state ID cards, account numbers, credit/debit card numbers, passwords, PINs, security questions, access codes, or any other information that could be used to fraudulently assume identity. PI doesn't include third-party database information maintained by casualty and property insurers, or information legally available through government records at state, local, or federal levels. Widely distributed media also isn't PI.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification becomes obligatory when entities become aware of a breach. Notification must be made to each affected party without unreasonable delay. If good-faith investigation reveals no harm or expectation thereof, notification isn't necessary. Consumer reporting agencies must be notified if 1,000 or more Maine residents are affected. This notification needs to specify the breach date, how many people were affected (if that information is known), and anticipated date breached parties will be affected. Third parties who own or license data that the entity manages must also be notified as soon as reasonably possible following a breach of computerized PI.

Reasonable delays include law enforcement delaying notification for investigation, restoration of breached system integrity, and determination of breach scope. After a law enforcement agency determines notification is allowable, this must take place no later than 7 business days after authorization.

Electronic notice consistent with the E-SIGN Act (15 U.S.C. § 7001) and written notice are permissible means of notification. Substitute options are allowed if cost of notification can be demonstrated by the entity to exceed $5,000, more than 1,000 individuals have been affected, or contact information for affected parties isn't sufficient. Substitute notification must include email notice, if possible, a conspicuous post on any websites the entity maintains, and the alerting of statewide major media.

Associated Penalties

In Maine, breach notification penalties can include civil penalties as high as $5,000 per violation and as high as $2,500 per day. Also, equitable relief and enjoinment stemming from future violations may be applicable. The AG enforces these laws, and when applicable, so does the Department of Professional and Financial Regulation, as well as the Office of Consumer Credit Regulation.

Exceptions/Exemptions

Breach notification can be delayed for law enforcement should notification transpire within 7 days after law enforcement rescinds any restrictions.

MARYLAND

Statute Codes

Breach notification requirements for Maryland are under Md. Code Com. Law § 14-3501 et seq. They include two specific wings of legislation: H.B. 208, which became law April 3, 2007, and began to apply January 1, 2008, and H.B. 974, which became law May 4, 2017, and began to apply January 1, 2018.

Legal Requirements and Purpose

Entities who have experienced breach notification must alert affected parties. Entities are in Maryland sole proprietorships, corporations, partnerships, associations, or any other group operating at a profit--including financial institutions of all kinds--which maintain computerized PI on citizens. Any group local to Maryland, or foreign to America, is included under these laws if they manage PI on Maryland residents.

A security breach transpires when PI is accessed by unauthorized parties such that integrity, security, or confidentiality of PI is impacted. Good-faith PI acquisition and use isn't a breach, provided PI isn't made further available to unauthorized parties.

PI in Maryland is defined as a first name or initial, last name, and other distinguishing information neither encrypted nor redacted. This can include SSNs, driver's licenses, state ID numbers, financial information like account numbers, credit/debit card numbers, security codes, PINs, passwords,

security questions, health information, health insurance policy numbers or related information, biometric data (fingerprint, voice print, DNA, retinal/iris scans), or login data like usernames and passwords combined with security questions for email addresses. PI doesn't include data legally available to the general public through media or federal, state, and local government records. PI also doesn't include information individuals have consented to have publicly shared, or information either listed or spread compliant to HIPAA.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification is necessary upon discovery without unreasonable delay. Should a comprehensive, swift, good-faith investigation determine no PI harm, notification isn't required provided records are maintained reflecting this determination at least three years after said determination has been made. Should investigation conclude potential harm, affected parties are to be notified. Notification must happen as swift as reasonably possible, and no later than 45 days from the time an investigation has been concluded. Scope of breach, individuals affected, and system integrity restoration, must take place within this time.

AG notification must be made if a PI breach is verified. However, notification must be given to the State Office of the Attorney General before it is given to affected parties. Additionally, if 1,000 individuals or more have been affected by a PI breach, consumer reporting agencies must be notified. Third parties who own or license information entities manage, but don't themselves own or license, must also be contacted as swift as possible. Third-party notification must happen before 45 days have gone by from breach discovery. The third party will pursue breach notification of owners or licensees of associated PI.

Notice may be provided in writing to the most recent applicable addresses of affected individuals by telephone to the most recent phone number(s), or by email to the most recent email address; provided affected parties have expressly consented to

such notification. Unless breaches have compromised email accounts, several things must be included in notification. How extensive a breach is must be communicated and contact information for the entity who was breached must be provided (including addresses and toll-free telephone numbers; or regular phone numbers if there are no toll-free ones). Additionally, toll-free phone numbers, addresses, and web addresses of the FTC (Federal Trade Commission), as well as the AG must be provided. They must come with a statement detailing how affected parties can get info from such resources pertaining to proper actions that can be taken.

When data breaches have compromised email access of affected individuals, electronic notice can be provided which tells these individuals to change their passwords and security questions as applicable, as well as take other email account protection measures. This must be done in a conspicuous, clear way through trusted IPs at times conforming to greatest likelihood of affected individuals using the internet.

Substitute notification methods are allowable should breach notification costs exceed $100,000, more than 175,000 persons be affected, or contact information not be available. Substitute notification must include email notice as applicable, conspicuous posting pertaining to the breach on any websites the entity maintains, and statewide media notification.

Associated Penalties

Breach notification in Maryland is enforced by the AG. Affected citizens may pursue actions as outlined in Title 13 of the Maryland Code, the “Unfair and Deceptive Trade Practices Act”.
Waivers are not permitted in Maryland.

Exceptions/Exemptions

Exceptions to these breach notification laws include delay for law enforcement, if such legal agencies tell an entity to do so. Once notification authorization is again allowed, notification must take place within thirty days.

If an entity is already complying to notification law existing under primary regulator laws from federal or state legislation, they will be held in compliance. Also, entities complying to the Gramm-Leach-Bliley Act are held in compliance of Maryland law. This extends to compliance to federal Interagency Guidelines Establishing Information Security Standards and Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice laws; including any ongoing revisions therein. HIPAA compliance is also accepted here.

MASSACHUSETTS

Statute Codes

In Massachusetts, breach notification law can be found under Mass. Gen. Laws 93H § 1 et seq. This law includes 201 C.M.R. 17.00. Additionally, H.B. 4144 was signed into law August 3, 2007 and made legal October 31, 2007, while H.B. 4806 was made into law January 10, 2019, and made effective April 11, 2019.

Legal Requirements and Purpose

Entities experiencing breach notification must swiftly notify affected parties. Massachusetts defines entities as natural persons, corporations, associations, legal entities, partnerships, executive offices, boards, commissions, bureaus, or any other Massachusetts authority or political subdivision owning, licensing, or maintaining PI on Massachusetts residents. Groups exterior to Massachusetts maintaining PI on Massachusetts residents are also included under these statutes.

A security breach is when PI is compromised in terms of confidentiality, security, or integrity by an unauthorized party. The PI must be neither redacted nor encrypted, nor accessible through encryption key. Identity theft risk exposure is the threat being protected against. Accordingly, good-faith acquisition of PI (though perhaps unauthorized), which is also used in good faith, is not a breach--provided further unauthorized disclosure doesn't take place.

PI is the first name or initial and last name of a citizen coupled with other sensitive data, including SSNs, driver's licenses or state ID numbers, and financial account information including credit/debit cards, PIN numbers, passwords, or any combination thereof permitting unauthorized access. PI does not include government records at local, state, or federal levels or lawfully obtained information otherwise available to the public at large.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification becomes necessary as soon as possible from the time an applicable PI breach is observed. Massachusetts is inclined to regard unauthorized third-party use as a notification obligation trigger, even if ownership and materiality seem to indicate otherwise.

The Director of Consumer Affairs and Business Regulation, as well as the AG, must be provided notice as well. Such notice must include, but may not necessarily be limited to, what sort of breach transpired, how many Massachusetts residents were affected, persons or agencies responsible for reporting the security breach (and their relationship to those who've had PI affected), what sort of agency or individual is reporting the breach, who is responsible (should this be known), what sort of PI was impacted, if reporting parties keep any information security programs, and steps

taken to defer further breach of this kind. Those who've been breached must file a report with the AG as well as the Director of Consumer Affairs and Business Regulation demonstrating compliance to credit monitoring regulation should citizens have SSNs affected. Presently the AG and Director of Consumer Affairs are both groups with online forms for such reports.

When the Director of Consumer Affairs receives such information, the Director will make a public incident report on appropriate websites, additionally providing electronic copies as a sample of the notice affected parties will receive. The Director will also identify relevant consumer reporting or state agencies, forwarding such information to breached entities. The entity must then notify consumer reporting and state agencies the Director identifies, doing so without any unreasonable delay.

Agencies inside The Executive Department must provide a written notification characterizing the breach to The Technology Division and the Division of Public Records as expeditiously as possible, excepting any reasonable delay, once breach is discovered. Compliance with such procedures and policies as adopted by such divisions must take place.

Third party entities who manage PI must provide breach notification as swiftly as possible, without unreasonable delay. The entity must then comply with those who either license or own such PI by informing them of the breach, when it happened (approximated if necessary), and forward preventative steps. Cooperation need not require confidential disclosure of trade secrets or anything of proprietary nature. Additionally, non-affected residents need not be informed of breaches.

Breach notification must take place as soon as possible, and scope determination is not a valid reason for delay. Systems recovery or law enforcement notification freeze are reasonable. When breach notification is provided, the nature of the breach may not be required, however what is required is key information. This includes affected parties' right to obtain police reports, how a security freeze can be requested along with necessary information for such a request, clear communication that no charge will be required for a security freeze, and relevant mitigation solutions available in accordance with the law. Should affected parties be subservient to persons or corporations experiencing breach, consumer notice must include the name of whichever person or corporation was breached.

Means of notifying affected parties can include electronic notice complying to the E-SIGN Act (15 U.S.C. § 7001) or written notice. Should notification costs be demonstrated by the entity to exceed $250,000, affect more than 500,000 persons, or sufficient contact information for affected parties isn't available, three substitute notification methods must be pursued. Email must be sent to affected residents, entities with a website need to make clearly conspicuous notification on their homepage of the event, and a broadcast or publication given through major media outlet which reaches all of Massachusetts must be made.

Associated Penalties

In Massachusetts, the AG enforces breach notification legislation. Civil penalties, injunctive relief, and damages may apply to entities found out of compliance. Enforcement comes through the AG, who may take relief action or level appropriate fines against entities found in violation. There are no specific pre-existing dollar amounts to such breaches and fines or damages are determined at the discretion of the AG.

Should the AG use the Consumer Protection Act to interpret a penalty, $5,000 per incident may be leveled at those found out of compliance.

Exceptions/Exemptions

Compliance with other laws that match these guidelines is permissible. Also, if law enforcement enforces a notification delay, this is additionally permissible. However, as soon as the delay is lifted, swift notification must take place. Entities must also cooperate with law enforcement during investigation. This includes information-sharing relevant to breach incidents. Confidential information, or trade secrets, are not included in compelled information-sharing.

MICHIGAN

Statute Codes

In Michigan, breach notification laws are collected under the Identity Theft Protection Act, Mich. Comp. Laws § 445.63, 72 et seq. This includes two specific measures, S.B. 309, which was signed into law December 30, 2006, under Act 566, and made effective July 2, 2007, and S.B. No. 223, signed into law December 21, 2010, and made law April 1, 2011.

Legal Requirements and Purpose

Michigan breach notification must take place for entities who have had a security breach. In Michigan, entities are any unit of state government, offices, agencies, authorities, departments, boards, commissions, associations, legal entities, LLCs, corporations, individuals, or partnerships. Any operation like this owning or licensing PI data on Michigan residents is covered under this law. Additionally, out-of-state entities who have such information are covered under these laws.

A security breach is when PI is compromised in terms of security or confidentiality by unauthorized access or acquisition. Good-faith PI access isn't a breach if the data is also used in good-faith and isn't distributed to further unauthorized parties. Good-faith determinations require careful consideration.

Michigan defines PI as the first name or initial and last name of a person coupled with other sensitive data like SSNs, driver's licenses and state ID numbers, demand deposits, financial account numbers, security codes, access codes, or passwords allowing access to financial accounts.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification becomes necessary if unencrypted or un-redacted PI has undergone unauthorized access. If PI is encrypted, but unauthorized persons get a decryption key, this also predicates breach notification. Should a security breach be determined not to have harmful potential on one or more persons by the entity, notification isn't necessary. This section isn't applicable to persons in federal, state, or local government agencies lawfully acquiring documents made available to the public at large.

Consumer reporting agencies must be notified if 1,000 or more residents are affected by a breach and after those affected by the breach have been themselves notified. The number of affected parties and time of breach must be included in this notification. Persons or agencies under Title V of the Gramm-Leach-Bliley Act aren't included under this section.

If an entity doesn't own or license information, but manages it on behalf of a third party, that third party is to be notified as swift as possible unless it's determined no harm will come to those who have been breached. Unreasonable delay isn't allowed in notification timing. Scope of breach and system integrity restoration constitute reasonable delay.

Notice may be provided in writing to the most recent available addresses of affected parties, or by telephone. Telephone notification must make actual contact; no recorded messages. Also, this option is only viable if recipients express consent. If a live conversation on a phone to a consenting individual doesn't take place, and is unachievable within three business days of initial attempts, additional methods must be pursued, such as an electronic notice. Recipients must express consent, and an existing business relationship must exist between the entity and recipient which includes regular email interaction. This option is also viable if primary contact is through the internet.

Breach notification shall be clear and conspicuous, communicating the breach in general terms, what PI was affected, subsequent data protection measures, inclusion of telephone numbers where additional help and information can be acquired, and a reminder to maintain vigilant against future fraud or identity theft.

Substitute breach notification options are allowed should more than 500,000 Michigan residents be affected or if cost of notification can be demonstrated by the entity to exceed $250,000. Substitute notice must include three separate notification methods: email if possible, conspicuously posting about the breach on entity-maintained websites (if there are any), and notification of statewide media well-known in Michigan, and including both telephone numbers or web addresses for additional information or assistance.

Should a company providing public utility and sending out monthly billing statements to clientele experience a breach, notice may be given through such means in compliance with this statute, and through the provision of four specific tactics. Email notice according to this statute must be made if possible, media reaching affected clientele must be notified, a conspicuous post pertaining to the breach must be put on the utility provider's site, and written notice must be sent to affected parties at the postal address contained in that utility company's records.

Associated Penalties

AG enforcement defines Michigan breach notification law. Criminal penalties exist where fraudulent notice is given. This is a misdemeanor offense which can be punished with either 30 days' imprisonment, $250 per violation, or both. Secondary and tertiary violations render the same penalties, but fines double and triple (to $500, then $750) with subsequent violations. Misrepresentation of security breaches to affected parties can result in 93 days of jail time and $1,000 per violation, or both. Second and third violations result in fines of $2,000 and $3,000, respectively. Failure to provide notice can result in civil fines up to $250 per incident, with a $750,000 security breach cap. Such penalties have no effect on civil remedy availability under federal or state law.

Exceptions/Exemptions

Exceptions to breach notification laws for Michigan include financial institutions already complying to the Federal Interagency Guidance Response Programs for Unauthorized Access To Consumer Information and Customer Notice, as issued March 7, 2005. Additionally, HIPAA-covered entities in compliance are exempted.
Delaying breach notification for law enforcement is allowed if law enforcement initiates such delay. When delay is lifted, notification must happen as soon as it's possible to notify affected parties--within reason.

Entities may give notice in compliance to agreements with other entities, provided said agreements don't conflict with existing Michigan laws.

MINNESOTA

Statute Codes

Breach notification law in Minnesota is covered under Minn. Stat. § 325E.61, which includes H.F. 2121, a measure made law June 2, 2005, under Chapter 167, and made effective January 1, 2006.

Legal Requirements And Purpose

An entity must render breach notification if they own or license data including PI. Entities in Minnesota are any business or person conducting business in the state. Out-of-state entities with such PI on state residents are also covered under Minnesota law.

A security breach is defined as unauthorized PI acquisition which compromises confidentiality, security, or integrity of that data. PI given in good-faith and used accordingly is not a breach, provided further unauthorized access doesn't take place.

Minnesota defines PI as a first name or initial with a person's last name in an unencrypted/un-redacted presentation where no decryption option is available. This name must be coupled with additional information such as SSNs, driver's licenses or ID numbers, financial information like account numbers, credit/debit card numbers, passwords, access codes, PINs, or anything permitting access to an account. PI doesn't include information publicly and lawfully available through state, federal, or local records.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification must take place immediately upon discovery of a breach to affected parties, and without unreasonable delay. If more than 500 individuals are compromised at once, the entity must additionally notify relevant consumer reporting agencies within 48 hours. If an entity manages information it neither licenses nor owns for a third party, notification of a breach must take place immediately upon discovery--provided, of course, the breach is determined to have harmful potential. Disclosure requires all expedience; however, scope determination, identification of affected parties, and data system integrity are allowable breach notification delays.

Notice can be provided by writing or electronic notice complying to the E-SIGN Act (U.S.C. § 7001). Should 500,000 or more residents be affected, or cost of notice exceeds $250,000, substitute options must include three specific outreach efforts. Email must be sent if email addresses are available. If an entity has a website, they must design a conspicuous post pertaining to the breach, and any major statewide media must be notified.

Associated Penalties

Breach notification in Minnesota is enforced by the AG. Private Right of Action is allowed, and waivers are not permitted. The AG can take action and seek a penalty of no more than $25,000 for the state.

AG enforcement is for entities found out of compliance. The AG may seek civil penalties or injunctive relief no higher than $25,000.

Exceptions/Exemptions

Breach notification in compliance to existing internal policies which agree with Minnesota law is allowable, and separate notice from internal procedures isn't necessary. HIPAA-compliant entities are also exempted.

If law enforcement stops notification for criminal investigation, this is allowable provided notification takes place when this delay is lifted by law enforcement officials. In Minnesota, 15 U.S.C. § 6809(d) has a "financial institution" definition which this law does not apply to.

MISSISSIPPI

Statute Codes

In Mississippi, breach notification is under Miss. Code § 75-2429, including H.B. 582, which became law April 7, 2010, and was rendered effective July 1, 2011.

Legal Requirements and Purpose

It becomes necessary to provide breach notification if an entity experiences PI security breach. An entity in Mississippi is a person or business conducting operations which owns, maintains, or licenses PI.

A security breach is when unauthorized access to computerized PI of Mississippi residents takes place, and that PI isn't encrypted, redacted, or otherwise secured such as to be unreadable/unusable to unauthorized parties.

PI is defined in Mississippi as the first name or initial and last name of a citizen combined with other sensitive data, including SSNs, driver's licenses or state ID numbers, financial information like account numbers, credit/debit card numbers, passwords, security codes, PINs, or anything else providing access to private financial accounts. PI doesn't include federal, state, or local government records made lawfully available to the general public.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification must take place if after appropriate, good-faith investigation, an entity concludes a breach could cause harm to affected parties. If an entity manages PI it neither owns nor licenses for a third party, that third party must be notified as soon as reasonably possible pertaining to breaches. After investigation completion, notice must be provided without unreasonable delay. Allowable delays include incident scope determination, affected individual identification, and restoration of data system integrity.

Notice may be given via writing, telephone, or electronic outreach conforming to the E-SIGN Act, 15 U.S.C. § 7001. If more than 5,000 residents are affected, or cost of notification exceeds, $5,000, substitute notice must include three specific outreach attempts. Email notice to available email addresses must be sent out, a conspicuous post on any websites maintained by the entity must be made, and major statewide media must be appropriately notified.

Associated Penalties

Mississippi breach notification laws are enforced by the AG. Compliance failure is considered unfair trade practice.

AG enforcement determines penalties for entities out of compliance, under the Consumer Protection Act, should knowing and willful violation be clearly established, fines could be as high as $10,000 per violation.

Exceptions/Exemptions

Exemptions to breach notification include internal policies of an entity which already agree with Mississippi law, provided internal practices agree to Mississippi law in terms of timeframe and implementation. Basically, you don't have to send out multiple notices if you already follow satisfactory internal practices. Similarly, compliance with existing federal regulations is permissible.

If law enforcement predicates breach notification delay, this is allowed provided notification transpires as expediently as possible once this law enforcement delay is lifted.

MISSOURI

Statute Codes

Missouri breach notification is covered under Mo. Rev. Stat. § 407.1500, H.B. 62, which was made effective August 28, 2009.

Legal Requirements and Purpose

Application of breach notification law applies to entities who own or license PI on Missouri residents. Entities are defined as legal commercial entities, public corporations, any government agency, subdivision, or instrumentality, joint ventures, associations, LLCs, partnerships, trusts, business trusts, estates, corporations, or individuals.

Accessing PI without authorization in a way that compromises the confidentiality, security, or integrity of PI is considered a breach. Good-faith PI acquisition isn't a breach if the PI is used properly.

PI is defined as Missouri citizens' first name or initial conjoined with their last name and other sensitive data. This additional data includes SSNs, driver's license numbers or other unique ID numbers created or collected via government, financial information like account numbers, credit/debit card numbers, PINs, pass codes, or anything else allowing identity theft and unauthorized account access. Unique routing codes or other financial account access information is included, as is any medical information or health insurance information like policy numbers or subscriber identification numbers. PI is not defined by legally obtained information from local, federal, or state government records, or otherwise available to the general public.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification must take place if an applicable breach is discovered. It must take place as expediently as possible. Should appropriate investigation demonstrate identity theft or fraud risk isn't an issue, after consulting with relevant legal authorities, notification isn't required. However, the incident must be documented in writing, and said documentation must be maintained no less than five years. If more than 1,000 persons are affected by a breached entity, consumer reporting agencies must also be notified. Also, the AG must be notified when 1,000 or more parties are affected by a breach. The AG's office must be notified pertaining to timing, distribution, and content affected in such notification. Entities who manage information they don't own or license for third parties must contact those third parties as swiftly as possible after a breach is discovered.

Unreasonable delay is not allowed in breach notification. Reasonable delay includes breach scope determination, or system restoration after technological intrusion. Also, time necessary to determine contact information of affected parties is allowable. Means of notification include written or telephonic notice, provided actual contact is made via telephone. Electronic notice is also available should it conform to the E-SIGN Act (15. U.S.C. § 7001). Such notice must include a general description of what happened, what PI was affected, phone numbers affected parties can call for assistance and information (if there are any such numbers), contact information for consumer reporting groups, and any other pertinent advice relating to how affected parties should act going forward, including maintaining vigilance through account review and credit report monitoring.

Substitute notice is allowed if 150,000 or more people are affected, and notification cost exceeds $100,000. Also, if there's no available contact information, substitute notice can be used. The same is true should affected parties be unidentifiable. This substitute notice must include three outreach methods. Email notice should be given, if the entity maintains a website a conspicuous post must be put there, and major statewide media must also be notified.

Associated Penalties

The AG enforces breach notification laws and exercises exclusive authority to bring action pertaining to actual damages of what may be characterized by Missouri law as willing, knowing violation. Penalties sought must not exceed $150,000 per breach as discovered through a single investigation.

Exceptions/Exemptions

Exceptions to such breach notification law include internal policies of an entity which match existing law in terms of timing and policy. They additionally include entities regulated by state or federal law who properly maintain these guidelines. Also, a financial institution complying to the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued March 7, 2005, shall be held in compliance. Additionally, entities meeting the requirements of the National Credit Union Administration regulations located in 12

CFR Part 78 are in compliance, as are those complying to Title V under the Gramm-Leach-Bliley Act.

If law enforcement delays notification for criminal investigation, this is allowed, provided affected entities document such delay requests in writing as they happen, including the name(s) of law enforcement officer(s) making such request, and the agency they work for. Once the delay is lifted, notice must be given as swiftly as possible.

MONTANA

Statute Codes

Montana breach notification is covered under Mont. Code § 30-14-1701 et seq., including two considerable sections; H.B. 732, which became law April 28, 2005, under Chapter 518, and was made effective March 1, 2006, and H.B. 74, which was made law February 27, 2015, and made effective October 1, 2015.

Legal Requirements and Purpose

Breach notification is necessary should PI managed by an entity be compromised. An entity is a person or a business conducting operations in Montana which include ownership or licensing of computerized data including PI. Non-local entities maintaining PI on Montana residents are also under these laws.

A security breach occurs when PI is accessed by unauthorized parties in a way materially compromising confidentiality, security, or PI integrity. PI acquired in good-faith, and used accordingly, doesn't constitute a breach--so long as further disclosure of an unauthorized kind doesn't take place.

Montana defines PI as the first name or initial and last name of an individual in conjunction with additional data such as SSNs, driver's license numbers, state IDs, tribal IDs, bank account numbers, credit/debit card numbers, security codes, access codes, or passwords permitting financial account access. Medical record info as lined out in 33-19-104 (PI relating to physical or mental conditions, medical history, medical claims, or medical treatment, and obtained from a medical professional or institution, the individual in question, or their spouse, parent, or legal guardian) is also included, as are Tax IDs, and a PIN for identity protection as provided by the U.S. IRS. PI doesn't include public data made lawfully available from federal, state, or government records.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification must take place when a PI-compromising breach is detected--

provided there's reason to believe that PI may be compromised, and it's unencrypted. Should breach notification suggest or imply affected parties can get a credit report, coordination with a credit reporting agency pertaining to timing, distribution, and the content of the notice given to affected individuals must take place; but such coordination cannot delay breach disclosure.

When breach notification is necessary, an electronic copy of such a notification statement which includes the date and distribution method must be sent to the Consumer Protection Office of the AG, provided information identifying individuals being notified is excluded. When notifications concern more than one person, single copies must be submitted indicating how many individuals in Montana received notification. For breached insurance support organizations and like entities, this information must be submitted to the Montana Insurance Commissioner, Mont. Code § 33-19-321.

Third-party notification must take place if PI an entity neither owns nor operates but manages it and is affected by a breach. This notification must happen as immediately as possible following breach, or a believed breach. The timing of all breaches must happen so quickly, without unreasonable delay. Some reasonable delays include the determination of a breach, and system's integrity restoration. Notice must be given either by written or telephone outreach. Electronic notice is allowed provided it complies with the E-SIGN Act (15 U.S.C. § 7001).

Substitute notification is allowable should 500,000 or more Montana citizens be affected, cost of notification be expected to exceed $250,000, or contact information of affected parties be unavailable. When email addresses are available, substitute notice will be sent by this method. When they're not available, entities with a website must make a conspicuous post about the breach and let statewide or local media know of the breach.

Associated Penalties

Breach notification penalties are pursuant to applicable law in Montana.

In Montana, up to $10,000 in fines may be required of entities out of compliance. Short-term injunctions, permanent injunctions, or restraining orders may be applied.

Exceptions/Exemptions

Breach notification exception is available for entities maintaining internal notification security procedures pertaining to PI, provided those procedures don't unreasonably delay breach notification when it is required.

If law enforcement delays notification for an investigation, this is allowable provided notification takes place with no unreasonable delay after the restriction has been lifted.

NEBRASKA

Statute Codes

Breach notification in Nebraska is covered under the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. § 87-801 et seq. This includes L.B. 876, which became law April 10, 2006, and was made effective July 14, 2006, and L.B. 835, which became law April 13, 2016, and became effective July 20, 2016.

Legal Requirements and Purpose

Breach notification is necessary for Nebraska entities owning or licensing computerized data including PI. Entities are government agencies, corporations, business trusts, individuals, general trusts, estates, partnerships, limited partnerships, limited liability partnerships, LLCs, associations, joint ventures, organizations, a government group, subdivision, agency, or instrumentality, or any other legal entity operating for profit or not and conducting business in Nebraska. Entities located outside Nebraska owning/licensing PI on Nebraska residents are included under this definition.

A security breach is when unauthorized access to unencrypted computerized PI, in a way compromising security, integrity, or confidentiality of that data, takes place. Good-faith PI acquisition is not a breach, provided the data is also used in good faith and not further disclosed. PI acquired through search warrant, subpoena, or other legal order of a state agency does not constitute a security breach.

PI in Nebraska is defined as the first name or initial and last name of a Nebraska resident combined with additional data elements that aren't encrypted, redacted, or otherwise rendered unreadable to unauthorized parties. Additional data elements include SSNs, driver's license numbers or state ID numbers, account numbers, credit/debit card numbers combined with security codes, access codes, or passwords permitting financial access, unique electronic ID routing codes or numbers combined with security information, or unique biometric data like a fingerprint, voice print, retinal scan, or other unique biological identifier. A username and email address combined with a password or security question permitting online access is PI. A decryption key or other access method that will render encrypted data unencrypted is PI in the eyes of Nebraska law. PI doesn't include legally available information the general public can access, or government records of this kind at state, local, or federal levels.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification becomes necessary when a harmful breach is determined by the entity. If good-faith, prompt, reasonable investigation determines PI compromise won't cause harm, notification isn't necessary. Should notice be required, no later than the time notice is given to affected residents, entities must additionally notify the AG. Entities with computerized PI data they don't own or license must give notice

to the third parties they're managing that data on behalf of. This notice must be given as soon as possible and cooperatively. Cooperation is defined as sharing with owners/licensees of such breached PI relevant data pertaining to the breach, so long as such information isn't proprietary to the breached entity.

Expedient notification is necessary. Reasonable delay includes breach scope determination, and restoration of systems integrity. Means by which notice may be given include written or telephone notice. Electronic notice is allowed provided it conforms to the E-SIGN Act (15 U.S.C. § 7001).

If 100,000 or more residents are affected, or notification expense exceeds $75,000, three substitute measures are available, but all three must be pursued. They include: email notice when email addresses are available, conspicuously posting on an entity's website, if they have one, and major statewide media notification.

Associated Penalties

In terms of breach notification law in Nebraska, waivers are not permitted, and the AG enforces this statute. The AG may issue subpoenas, as well as seek recovery of direct economic damages pertaining to each NE resident affected by statute violation.

AG enforcement applies to those found out of compliance in Nebraska. Subpoenas may be issued, financial damages for recuperation may be sought for individually affected residents. Under the Consumer Protection Act, this could mean fines up to $2,000 per violation.

Exceptions/Exemptions

Should an entity have ten or fewer employees, and demonstrate cost of notice exceeds $10,000, breach notification exceptions allow substitute notice; but that must include all of the following measures: email notice when emails are available, paid advertisement notification pursued through local news outlets such as newspapers in the geographic area of the entity (such newspaper notification must cover at least a quarter page in the newspaper in question, and be published at least once a week for three weeks), conspicuous posting on entity websites if there are any, and major media outlet notification in the geographic area where the entity is.

An additional exception is available for businesses who have internal PI procedures that agree with existing statutes in terms of notifying affected residents, and timely notification. Also, if state or federal law mandates breach notification procedures, compliance to those laws is considered compliance with this statute; provided the AG is notified conforming to necessary breach notification procedures, and affected persons are also notified.

Should law enforcement delay notification for criminal investigation, this is permissible provided good-faith notification is made without unreasonable delay once the restriction has been removed.

NEVADA

Statute Codes

S.B. No. 186 was signed into law June 15, 2011, and became effective October 1, 2011. S.B. 347 was signed into law June 17, 2005. On October 1, 2005, forgery crimes against the elderly, state actor requirements, and credit card issuer requirements were put into effect. As of January 1, 2006, credit card issuer requirements, data destruction requirements, reasonable protection requirements, and security breach notification provisions were put into effect. Encryption provisions became necessary January 1, 2008. A.B. 179 was signed into law May 13, 2015, and became effective July 1, 2015.

Legal Requirements and Purpose

Breach notification is required by an entity in the wake of unauthorized PI access. In Nevada, an "Entity" is any type of business entity or association, including retailers, financial institutions, higher education groups, corporations, or government agencies, who either own or license computerized data including PI.

A security breach is when acquisition of PI happens in a way that's not authorized, and which may be seen to compromise confidentiality, integrity, or security of PI. Good-faith PI acquisition isn't a breach, if the data isn't used improperly and additional disclosure doesn't happen.

PI is defined by Nevada as a person's first name or initial with their last name, and additional PI such as SSNs, driver's licenses or state ID numbers, bank account numbers, credit/debit card numbers, and associated financial security codes, PINs, or security questions. Medical ID numbers or health insurance identification numbers are also PI. Usernames or other unique identification information pertaining to email addresses, such as passwords, access codes, or security questions, are considered PI. Nevada doesn't consider the last four digits of an SSN to be PI, nor do they consider the last four digits of a driver authorization card, identification card, or data publicly and lawfully available at federal, state, or local levels to the general public to be PI.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification applies when a harmful security breach is discovered where unencrypted PI is (or is believed to have been) compromised by unauthorized parties. Should more than 1,000 persons be affected, consumer reporting agencies must be notified without unreasonable delay. Such agencies must be appraised as to notification time and included content.

Entities who maintain information they don't own must contact third parties owning or licensing such information. This must be done as soon as possible in the wake of a breach believed to be harmful. Notification must be made as fast as possible,

barring reasonable delays for scope determination and restoration of IT system integrity. Means by which notification may occur include written notice, or electronic notice compliant to the E-SIGN Act (15 U.S.C. § 7001).

Substitute notification is available if 500,000 or more parties are compromised by a breach, notification costs can be demonstrated by the breached entity to potentially exceed $250,000, or sufficient contact information isn't available. Three substitute methods must be used: email outreach if addresses are available, conspicuous posting to any websites run by the entity, and statewide major media notification.

Associated Penalties

Waivers for breach notification are not permitted in Nevada. Should the AG or a relevant District Attorney (DA) determine an entity is violating, or intends to violate, provisions of this statute, the AG or DA may bring an action against such an individual for acquisition of permanent or temporary injunction against the violation.

Exceptions/Exemptions

Breach notification need not be doubled. If in-house PI management protocols predicate expedient breach notification to affected parties in conformity to existing laws, additional notification isn't necessary. Also, compliance with other laws like the Gramm-Leach-Bliley act is deemed compliance with this statute.

Should law enforcement delay notification for an investigation, this is permissible, provided notification takes place as soon as reasonably possible after restriction has ended. Action on behalf of data collectors may be commenced against persons who unlawfully obtain or benefit from PI. Additionally, see Nev. Rev. Stat § 242.181, and the special rules which apply to health records under Nev. Rev. Stat §§ 439, 603A.100.

NEW HAMPSHIRE

Statute Codes

New Hampshire breach notification includes N.H. Rev. Stat § 359-C:19 et seq., and H.B. 1660; which became law June 2, 2006, and was made effective January 1, 2007.

Legal Requirements and Purpose

Breach notification is required from entities managing computerized data including PI. Entities are defined as corporations, individuals, trusts, partnerships, associations either incorporated or unincorporated, LLCs, or any agency, board, authority, court, division, commission, bureau, department, institution, or state entity at the government level--including political state subdivisions. All PI-maintaining entities, local to New Hampshire or not, are included under this definition.

Security breaches are unauthorized computerized PI acquisition compromising integrity, security, or confidentiality of PI maintained by entities doing business in New Hampshire. Acquisition of PI in good-faith is authorized, provided the PI is used in good-faith, and further disclosure doesn't happen.

New Hampshire defines PI as the first name or initial and last name of an individual in combination with other sensitive data. This additional data can include SSNs, driver's license numbers, government identification numbers, account numbers, credit/debit card numbers combined with security codes, passwords, or anything else used to access a personal financial account. Data isn't considered encrypted if required keys, access codes, or security codes for decryption are available in compromised data sets. PI doesn't apply to lawfully available data, including federal, state, or government records the general public can access.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification must happen when a security breach is noticed, or there's suspicion of breach. If affected information can't be misused or is unlikely to cause harm, notification isn't necessary.

Should more than 1,000 consumers require notification, the entity must without reasonable delay provide notification to consumer reporting agencies that apply. This notification must include the approximate date of breach, the number of people affected, and the information in sent notice. Such obligation doesn't apply to entities operating under the Gramm-Leach-Bliley Act, Title V.

Entities doing business subject to N.H. Rev. Stat. § 358-A:3(I) must additionally notify primary regulators presiding over trade or commerce. All other entities must notify the AG in the event of a breach. Such notice must include when it's anticipated that affected individuals will be notified, and an approximation of affected individuals that will be notified.

Notification to individuals affected by a breach must happen as expediently as possible. At minimum, such notice must include a general description of what happened, an approximation of when the breach occurred, what PI was affected, and telephone contact information for the breached entity. Means of notification include written or telephone notice, as well as electronic notice should this be the primary means affected individuals communicate with the breached entity. Additionally, notice which matches internal entity procedures conforming to internal security policies pertaining to PI can be used.

Substitute notification is allowable if 1,000 or more persons are affected, cost of notification exceeds $5,000, sufficient contact information can't be acquired, or notification consent to other notification methods hasn't been given by affected parties. Substitute notification must include the following methods: email notice as it's available, conspicuously posting about the event on any websites as maintained by the breached entity, and statewide major media notification.

Associated Penalties

The New Hampshire AG exercises breach notification enforcement. Additionally, private right of action stipulates individuals injured by breach notification violation may pursue civil action. If the court finds in their favor, actual damages will be charged to the entity. If the court finds knowing willful PI compromise, no less than twice such an amount, but as much as three times such an amount will be awarded to the plaintiff. Suit and attorney costs will also be awarded to them. Finally, injunctive relief will become available to such individuals without bond at the court's discretion.

Exceptions/Exemptions

Exceptions to New Hampshire breach notification law include compliance to primary regulation agencies in terms of expedient notification.

Lastly, it is allowed if law enforcement deliberately delays notification for an investigation.

NEW JERSEY

Statute Codes

Breach notification laws for New Jersey are gathered under the Identity Theft Prevention Act. Specific codes are: N.J. Stat. § 56:8-163, and A. 4001; which was signed into law September 22, 2005 and made effective January 1, 2006. In an additional note, except for police reports, all provisions became legal on the later date, whereas police reports became effective on September 22, 2005.

Legal Requirements and Purpose

Breach notification is required in New Jersey for any municipality, county, district, public authority, agency, or political subdivision of any public body in New Jersey. Additionally, sole proprietorships, partnerships, associations, corporations, or any other entity is covered here, regardless of associated business profit. Financial institutions are included. Any group like this licensing or authorizing a certificate under the law of New Jersey, or the United States, or from any other country, or any subsidiary/parent company of a financial group is included if they conduct business in New Jersey and maintain computerized data which includes PI. The term "Entity" applies to such groups or individuals and includes those operating outside of New Jersey who keep PI on residents of the state.

A security breach is unauthorized PI access which may compromise integrity, security, or confidentiality of such data. This data can't be encrypted or "knowable"; otherwise it's not PI. Good-faith PI acquisition and use isn't a breach if it isn't further disclosed.

PI in New Jersey is defined as SSNs, driver's license numbers or state ID cards, financial account numbers, credit/debit card numbers, PINs, access codes, security questions, or anything else usable to access financial accounts. Data that isn't associated but that a link could associate is considered PI should means of linking such data become accessed without authorization.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification becomes necessary upon discovery and to affected parties. If reasonable belief of breach takes place, notification is also necessary. If the entity establishes no PI misuse is possible in all reasonability, no notification is necessary, but documentation in writing must be maintained for at least five years.

If 1,000 or more persons are affected by a breach, consumer reporting agencies must additionally be notified without unreasonable delay. Also, before disclosing a breach to affected parties, an entity must report the breach to the Division of State Police in the Department of Law and Public Safety for handling and investigation. This could require information be disseminated or referred to other law enforcement agencies more appropriate to the task.

Entities managing data they don't own or license on behalf of a third party must additionally notify that third party when a breach or suspected breach of computerized PI is evident.

Notification must happen as soon as possible, reasonable delays being breach scope determination and data system integrity restoration. Notices may be provided either in written form, or electronic form complying to the E-SIGN Act (15. U.S.C. § 7001). Substitute notification options are allowable if more than 500,000 persons are affected, notification expense exceeds $250,000, or necessary contact information for affected parties isn't available. Such notification must include these measures: email outreach where applicable, conspicuous posting on any entity-maintained websites, and major statewide media notification.

Associated Penalties

Breach notification penalties depend on how varying cases are litigated in New Jersey.

Civil action, substantial fines payable to the state, data destruction requirements, and corrective cyber-security reform strategies may constitute New Jersey penalties for non-compliance. The Consumer Protection Act may initiate penalties of $10,000 for a first offense, and as much as $20,000 for a second.

Exceptions/Exemptions

Breach notification exceptions in New Jersey include internal PI management practices which are already in agreement with existing statutes (including timing and specific notification to affected parties) and notification delays law enforcement imposes to conduct investigation.

NEW MEXICO

Statute Codes

Breach notification law in New Mexico is covered under H.B. 15, which became law April 6, 2017 and became effective June 16, 2017.

Legal Requirements and Purpose

Breach notification law in New Mexico applies to anyone licensing data elements including PI of New Mexico residents, legally termed the “Entity”. Entities out-of-state who own PI on New Mexico residents must answer to this law.

A security breach is when unauthorized PI acquisition takes place, and that PI isn’t encrypted; or, if it is encrypted, an access key is also acquired. This unauthorized access must compromise integrity, security, or confidentiality of associated PI. Good-faith PI legitimately acquired and used isn’t a data breach so long as it isn’t improperly disclosed.

PI is defined in New Mexico as the first name or initial and last name of a person in conjunction with additional data elements such as SSNs, driver’s license numbers, government-issued ID numbers, biometric data, or any financial information, such as account numbers, codes, passwords, debit/credit card numbers, passwords, or anything else that could be used to fraudulently access a person’s financial account. The PI definition doesn’t apply to lawfully obtained information available to the general public at local, state, or federal levels through government records.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

When a security breach occurs, or is reasonably believed to have occurred, breach notification becomes necessary. However, if investigation shows associated PI won’t cause harm to affected individuals, notification isn’t necessary.

Should 1,000 or more New Mexico residents be affected, consumer reporting agencies must also be notified as swiftly as possible; no later than 45 calendar days after a breach is noticed--unless law enforcement delays notification for investigation purposes.

The AG must be notified also if more than 1,000 residents are affected from one breach. The AG’s office must be notified pertaining to how many New Mexico residents are believed to be affected, and provided a copy of the notification such affected residents received. This must also be done within 45 calendar days after a security breach is discovered.

Entities managing data for third parties, but not owning/licensing it, must contact those third parties as swiftly as possible, but no later than 45 days after incident discovery. If sufficient investigation determines no threat to PI of affected individuals, third-party notification isn't necessary.

The maximum amount of days a notification should be sent out is 45 calendar day after a breach has been discovered. Reasonable breach notification delays include scope determination and restoration of data system integrity. When notice must be given it has to include the name and contact information of the person giving notification, what sort of PI was affected, when (approximately or exactly) breach occurred, a general description of what occurred, toll-free phone numbers and addresses of major consumer reporting agencies, advice directing recipients to review potentially affected accounts including what to look for, and advice informing notification recipients of their rights as sanctioned under the Fair Credit Reporting Act. Means of notification provision include United States mail, and electronic notification pursuant to the E-SIGN Act (15 U.S.C. § 7001).

Substitute notification options are available should affected individuals be greater than 50,000, notification costs exceed $100,000, or contact information not be sufficient. In such scenarios, substitute notice must include the three following methods: email where addresses are available, conspicuous posting pertaining to the breach on any entity-maintained websites, and a written notification sent to the AG, as well as any major media outlets of New Mexico.

Associated Penalties

Breach notification enforcement in New Mexico comes through the office of the AG, who may bring damages and action for an injunction. Under AG enforcement, a court action may be filed wherein civil penalties as high as $25,000 may be applied. Failed notification may be $10.00 per violation to a maximum of $150,000. Willful violation constitutes a penalty up to $5,000 under the Consumer Protection Act

Exceptions/Exemptions

Breach notification exceptions are available if internal PI management policies which agree with legal statutes pertaining to time and notification of affected policies are in place. This statute doesn't apply to entities operating in compliance to HIPAA or the Gramm-Leach Bliley Act.

Law enforcement delays for criminal investigation are permissible.

NEW YORK

Statute Codes

New York General Business Law § 899-AA, and N.Y. State Tech Law 208. Additionally, A.B. 4254 was signed into law as of August 10, 2005. Tech Law 208 became effective as of December 7, 2005. Lastly, S. 2605-D became effective as of March 28, 2013. The application of these laws basically includes any individual, business, or state entity in New York that owns or licenses computerized information which may include Private Information (PI). The purpose is to protect personal privacy.

Legal Requirements, Purpose, and Involved Timeframes

When it comes to a business' obligation to notify affected parties, the entity must disclose any breach information after a breach is discovered. Should such a breach occur, it is the responsibility of the entity to inform those whose PI has been compromised. Should more than 5,000 N.Y. residents be affected, consumer agencies must be notified with the following information: timing, what/who was affected, how PI was distributed, and an approximation of affected parties.

Breaches are defined by these laws as the acquisition of computerized PI that isn't authorized, and which may compromise confidentiality, security, and integrity of a business. Good faith data acquisition not strictly authorized isn't considered a breach, if the data isn't used to illegally disclose anything.

Should such notification become necessary, the Attorney General, consumer protection board, state police, and New York's Office of Information Technology must be notified of when the breach occurred, what/who was affected, and how notifications to affected parties were distributed. The Attorney General's website has a form to facilitate this process.

The Attorney General will also have to be notified when residents are notified of a breach. The Office of Information Technology Services, Consumer Protection Board, and Division of State Police are required to be notified of the breach as well.

PI can be personal or private. Personal PI identifies individuals, private PI is non-encrypted information that isn't personal but may be proprietary, or otherwise confidential. Private PI may include SSNs, driver licenses or other ID info, banking information such as credit card numbers or routing numbers, security access codes, passwords, or anything similar. PI doesn't include publicly available data legally available to people at the city, state, or federal levels.

Penalties and Exceptions

Exceptions include cities, counties, villages, towns, municipalities, or other local agencies which may have information that is used in non-traditional ways--the information of a convicted felon may be an example of "publicly" available "private" data, depending. Some personal information can become public. Application of these

laws persists regardless of tech profitability. Basically, even if you don't own private information, it falls under these laws. If you conduct business out of state, should the data be centered in the state, these laws apply. PI a business doesn't own requires notification of that information's owner. All these notifications are to be done swiftly as possible, avoiding delays deemed unreasonable in a legal sense, and considering the scope of a given breach, as well as restoration of operational integrity.

AG enforcement defines New York, court action may include injunctions, violation restraints, relief pertaining to article 63 of the Civil Practice Law and Rules, fines and damages as the court deems fit, and up to $5,000 per instance under the Consumer Protection Act according to court determination.

Penalties and Exceptions

Notices of a data breach should be provided via written, telephone, or electronic method. If the expense of notification is greater than $250k, more than 500k people are affected, or there isn't available contact info for affected parties, substitute notice options include emails, posting conspicuously on affected persons' websites, or giving information to major statewide media for distribution. Should a law enforcement agency determine notification should be delayed because it may impede the investigation, then notification can be delayed. Improper notification will lead to prosecution and associated verdicts. This could include anything from fines to an entity being entirely dissolved; it depends on the AG.

NORTH CAROLINA

Statute Codes

North Carolina breach notification is covered under N.C. Gen. Stat. §§ 75-61, 75-65, which includes S.B. 1048 as signed into law September 21, 2005, and amendment S.B. 1017, which was signed into law July 27, 2009.

Legal Requirements and Purpose

Breach notification must be made by entities owning, licensing, or maintaining PI and conducting business when a breach is noticed or suspected. Entities in North Carolina are defined as government or government subdivisions and agencies, financial institutions or their subsidiaries/parent organizations, financial institutions holding licenses (or authorization or certificates under the laws of any country or state), sole proprietorships, corporations, partnerships, associations, or other relevant groups.

A security breach is defined as unauthorized access to unencrypted or un-redacted data containing PI in ways which may be considered to harm affected parties. If data is encrypted/redacted, but there's a security key to reveal hidden data, this is a security breach. Good-faith PI acquisition and use is not labeled as a data breach if it's not further disclosed.

PI is defined by North Carolina as the first name or initial and last name of a person combined with additional sensitive data. Additional data includes SSNs, tax ID numbers, driver's licenses or state ID numbers, checking, savings, and credit/debit card numbers, PINs, digital signatures, biometric data such as fingerprints, and any other numbers/data usable to access financial resources. Also, should electronic ID numbers, email addresses or names, internet account numbers, internet ID names, parents' legal surname before marriage, or other passwords get out, they're considered PI if they could be used to acquire access into a person's resources or financial account(s). PI does not include legally available public information in directories of government records at federal, state, or local levels, or anything else widely disseminated to the general public (including addresses, names, or telephone numbers), provided such information has been voluntarily provided with consent of the individual in question.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification must take place as soon as possible when breaches are noticed or suspected. Consumer reporting agencies must be notified if 1,000 or more individuals are affected and without unreasonable delay. The Consumer Protection Division of North Carolina's AG office must be informed of the nature of the breach should any breach notification take place. The AG's office must be appraised of how many people were affected, what steps were taken in terms of investigation, preventative measures, when the breach took place, how widely it was distributed, and what information was contained in the notice affected individuals received. North Carolina's AG has a website with a form to help breached entities properly provide such information.

Entities managing North Carolina resident PI they don't own or license for third parties must notify those parties of a breach as soon as possible once it has been noticed. In terms of timing, unreasonable delay must not impede notification. Reasonable delay involves breach scope determination, restoration of integrity, confidentiality, and security to affected data systems.

Breach notification to affected parties must be clear and conspicuous, including seven specific pieces of data. A general description of the incident must be included, what type of PI was affected must be noted, acts taken to prevent further unauthorized access must be noted, telephone numbers of businesses or persons providing further information or assistance must be provided (should there be such telephone numbers), advice pertaining to account review vigilance and monitoring of free credit reports must be given, toll-free numbers/addresses of major consumer reporting agencies must be rendered, and toll free numbers, addresses, and websites for the FTC (Federal Trade Commission), and North Carolina AG office--as well as a statement individuals can obtain from such sources regarding identity theft prevention--must also be provided.

Means of providing breach notification include written notice, telephone notice where direct contact is made, and electronic notice in accordance with the E-SIGN Act (15 U.S.C. § 7001). Should contact information be unavailable, 500,000 or more

individuals be affected by the breach, or cost of breach notification exceed $250,000, three substitute notification methods must be used. They include an email should email addresses be available, conspicuous posting on any entity-maintained websites pertaining to the breach, and major statewide media notification.

Associated Penalties

Breach notification waivers are not permitted in North Carolina. The AG enforces this statute, and both criminal and civil penalties exist. Individuals injured from violation of this statue could institute civil action. AG enforcement applies in North Carolina, remedies may be sought under North Carolina State Chapter 51-15. These are non-exclusive remedies, additional penalties could apply. Knowing violation may be as high as $5,000 under the Consumer Protection Act.

Exceptions/Exemptions

Breach notification exceptions include financial institutions with internal PI management protocols consistent with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued March 7, 2005, and any revisions/additions/or substitutions associated with this notice.

Also, if law enforcement delays breach notification for criminal investigation, this is allowable provided such a request is put in writing, and includes the name of the law enforcement officer making the request, as well as that person's law enforcement agency. When delay is lifted by law enforcement, breach notification must subsequently take place without unreasonable delay.

NORTH DAKOTA

Statute Codes

Breach notification in North Dakota is covered under N.D. Cent. Code § 51-30-01 et seq. This includes S.B. 2251, which became law April 22, 2005, and became legal June 1, 2005, H.B. 1435, which became law April 18, 2013, and S.B. 2214, which was made law April 13, 2015, and became effective August 1, 2015.

Legal Requirements and Purpose

Breach notification is required of any entity who either licenses or owns computerized data which includes PI and conducts business in North Dakota. Out-of-state entities are likewise culpable under the law should they maintain PI on North Dakota residents.

A security breach is when acquisition of PI at the hands of unauthorized parties takes place in such a way as to compromise that data in terms of integrity, security, or confidentiality. PI acquired and used in good-faith, and not further disclosed, isn't a breach.

North Dakota defines PI as the first name or initial and last name of a person combined with additional sensitive data. Such additional data includes SSNs, operator license numbers as assigned by the Department of Transportation (DOT), non-driver color photo identification card numbers assigned by the DOT, account numbers, credit/debit card numbers, security codes, access codes, passwords, or any other financial account access information, date of birth, the mother's maiden name of an individual, medical information, health insurance data, any ID number given by an employer in combination with any sort of security code, or a digitized electronic signature. PI doesn't include lawfully available information the general public can access, or federal, state, and local government records.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification must take place if a security breach or suspected security breach impacting North Dakota resident PI negatively takes place. The AG is to be notified by mail or email pertaining to any security breach of this kind involving more than 150 persons. Entities managing third-party information they don't own or license must contact that third party as soon as possible after a discovery of PI security breach.

Breach notification must happen as expediently as possible accepting reasonable delay such as breach scope determination or data system integrity restoration. The format of a notice that may be provided includes written outreach and electronic notice in compliance with the E-SIGN Act (15 U.S.C. § 7001). If contact information isn't available, more than 500,000 residents are affected, or cost of outreach can be demonstrated by the breached entity to exceed $250,000, substitute notification options must include three specific outreach items: email outreach if addresses are available, conspicuous posting of breach notification on any websites run by the entity, and statewide major media notification.

Associated Penalties

Breach notification is enforced by the AG, and as such will include appropriate penalties if compliance isn't observed.

Under the Consumer Protection Act, penalties up to $5,000 may be applied. The AG may enforce penalties in accordance with North Dakota State Chapter 51-15.

Exceptions/Exemptions

Breach notification exemptions for North Dakota include financial groups complying to the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer notice, and any entity in compliance to title 45 of the Code of Federal Regulations, part 164, subpart D. If law enforcement determines delay is necessary for criminal investigation, this is also permissible.

OHIO

Statute Codes

Breach notification in Ohio is covered under Ohio Rev. Code § 1349.19. This includes H.B. 104, which was signed into law November 17, 2005, and amended by S.B. 126; which was itself signed into law December 29, 2006 and made effective February 17, 2006. An amendment for exclusion of HIPAA-covered entities went into effect March 30, 2007.

Legal Requirements and Purpose

Breach notification for PI compromise must be made by any entity owning or licensing such computerized data in Ohio. Individuals, corporations, estates, business trusts, partnerships, or associations are included under the term “Entity”.

A security breach is defined as someone obtaining unauthorized access to computerized data including PI in such a way as to facilitate a risk for identity theft or other fraud to an Ohio resident, or their property.

Ohio defines PI as a person’s first name or initial and last name combined with sensitive data which is neither encrypted nor redacted, or otherwise altered as to be unreadable. This additional data includes SSNs, driver’s license or state ID numbers, account numbers, credit/debit card numbers, security codes, access codes, passwords, security questions, or anything usable to access a financial account. PI doesn’t include lawful information available to the general public from state, federal, or local government records. Additionally, PI does not include news of an editorial or advertisement kind published in vetted media outlets, gatherings/furnishings of information by such outlets, or publications designed and distributed to vetted, bona fide associations or charitable groups; or any similar organization.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification obligation develops when an entity discovers or suspects a breach by unauthorized parties which could bring harm to individuals whose PI has been affected. Should 1,000 or more residents of Ohio be affected in one breach, the breached entity must notify applicable consumer reporting agencies. “Covered entities” under HIPAA aren’t bound by this requirement.

Should the entity manage information they don’t own or license for a third party, or act as a custodian for such computerized data, any involved third party (government or otherwise) must be notified of a potentially harmful breach as expeditiously as possible. Disclosure must be made no later than 45 days from an incident’s discovery, allowable delays including breach scope determination, determination of whose PI was affected, accessed, or acquired, and restoration of data system integrity.

Such notice must be given in written, telephone, or electronic form (if that's the entity's primary means of communication with affected Ohio residents). Substitute notice options are available should more than 500,000 persons be affected, cost of notification be demonstrated by breached entities to exceed $250,000, or sufficient contact information not be available. In such instances, three specific substitute notification methods must be used: email notice as applicable, conspicuous posting pertaining to the breach on any websites run by the affected entity, and major media outlet notification. Major media notification must be pursued until approximately 75% of Ohio's population can be reasonably expected to be reached.

Associated Penalties

The AG of Ohio enforces penalties, and may conduct investigation or bring a civil action should an entity fail to provide breach notification complying to this statute.
Ohio breach penalties are enforced by the AG, who may pursue a civil action for compliance failure. Penalties include temporary restraining orders, injunctions both permanent and temporary, fines up to $1,000 a day during initial sixty days of noncompliance, a fine raise of $5,000 after that time, and a raise of $10,000 per day after ninety days. Under the Consumer Protection Act, $25,000 per violation may be leveled if the court rules.

Exceptions/Exemptions

Breach notification substitute exceptions exist for businesses with 10 or fewer employees who demonstrate they'll have to pay $10,000 or more in breach notification costs. For them, substitute notification can consist of paid advertisement in local newspapers once a week for three weeks, and in an ad that's a quarter of a page in size. Additionally, conspicuous posting on any websites they maintain must be made, as well as major media outlet notification pertaining to the affected geographic area.

Financial groups, trusts, credit unions, financial institution affiliates, or other similar institutions who are already required to inform individuals who have had PI breached will be held in compliance provided they adhere to those laws and do so in the right time frame.

If an entity has gone into a contract with another entity prior the breach, the disclosure may be made in conjunction with that contract, provided said contract doesn't conflict with or invalidate any of the provisions in this statute.

Law enforcement delay is allowable if law enforcement decides notification would impede a criminal investigation. However, after notification is allowed again, the entity must swiftly disclose the breach to affected parties.

OKLAHOMA

Statute Codes

Oklahoma breach notification is covered under 24 Okla. Stat. § 161 et seq., which includes H.B. 2245, a measure signed into law April 28, 2008, and made effective November 1, 2008.

Legal Requirements and Purpose

Breach notification becomes necessary when an entity experiences security breach. An "entity" in Oklahoma is constituted as a business trust, estate, LLC, limited partnership, general partnership, organization, association, government, government subdivision, instrumentality, or agency, joint venture, or any other "entity" of a legal kind which either licenses or owns data of a computerized kind including PI.

A security breach is when PI is acquired without authorization such that affected individuals are compromised in terms of confidentiality or vulnerability to fraud like identity theft. PI acquired in good-faith and used accordingly does not constitute a security breach, provided further unauthorized disclosure doesn't take place.

PI in Oklahoma is defined as the first name or first initial and last name of a person in combination with other sensitive data. This additional data includes SSNs, driver's licenses and state ID numbers, or financial data such as account numbers, credit/debit card numbers, PIN-codes, passcodes, passwords, or anything else potentially providing fraudulent access to financial accounts.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification must take place upon breach discovery or reasonable suspicion PI neither encrypted nor redacted has been impacted in a way which may invite fraudulent activity. If it's suspected decryption keys have been acquired by unauthorized parties, this counts as a security breach requiring notification. Oklahoma entities must disclose whether unencrypted/un-redacted PI has been affected, or if keys to encryption have been obtained.

Should an entity manage data it neither owns nor licenses, said entity must contact the responsible third party pertaining to any compromising breach after it's been discovered. Such disclosure to affected entities and third parties must take place without unreasonable delay. Reasonable delay includes breach scope determination, and data system integrity restoration.

Means of notification include written notice to most recent available addresses of persons whose data has been breached, telephone notice, or electronic notice. Should 100,000 or more persons be impacted, breach notification costs exceed $50,000, or sufficient contact information not be available, substitute notification options must

include two of three options. There's email notice, if that's available, conspicuously posting information pertaining to the breach on any websites maintained by the breached entity, and major statewide media notification.

Associated Penalties

The AG enforces breach notification statutes in Oklahoma with exclusive authority. The AG can bring an action to obtain civil penalties no greater than $150,000 per breach (or a series of similar breaches discovered in one investigation), or actual damages stemming from a violation.

Exceptions/Exemptions

Exceptions to Oklahoma breach notification law include interagency guidance and primary regulator provisions. An entity compliant to procedures of the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is in compliance with Oklahoma breach notification laws. Additionally, any other primary federal regulations the entity already complies to are permissible. It is not necessary to send out two groups of notifications to maintain dual compliance

Breach notification delay is allowed should law enforcement determine notification would hamper criminal investigation. Once authorization for notification is made, said notification must take place as soon as reasonably possible.

OREGON

Statute Codes

Oregon breach notification is covered under the Oregon Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, 646A.602, 646A.604, 646A.624, 646A.626. This includes: S.B. 583, which was made law July 12, 2007 and made effective October 1, 2007, S.B. 574, made law June 13, 2013, and made effective September 12, 2013, S.B. 601, made law June 10, 2015, and made effective January 1, 2016, and S.B. 1551, made law March 16, 2018, and made effective June 2, 2018.

Legal Requirements and Purpose

Breach notification law applies to entities who've experienced a security breach, and who license, own, or otherwise possess PI used in business, occupation, vocation, or volunteer capacity. Entities in Oregon are individuals, partnerships, cooperatives, organizations, public or private corporations, LLCs, estates, or any other entity, whether it operates as for profit, or it exists as a public body (further defined in Rev. Stat. § 174.109).

A security breach is unauthorized acquisition of computerized data maintained by an entity which includes PI that may be materially compromised in confidentiality, security, or integrity by such unauthorized acquisition. Inadvertent PI acquisition not used in violation of law or in a way harming security, integrity, or confidentiality of PI is not a security breach.

Oregon defines PI as the first name or initial and last name of a person combined with any of the following information: SSNs, driver's license numbers, state ID numbers issued by the DOT (Department Of Transportation), passport or other U.S. identity numbers, financial information like account numbers, debit/credit card numbers, PINs, passwords, access codes, security questions, or any other information that could provide unauthorized parties access to a financial account, biometric data (fingerprints, physical characteristics, retina/iris scans, etc.), health insurance policy numbers, or any medical history information. Data without the first or last name of an individual is also PI should it be usable to commit identity theft. Publicly available data, except for SSNs, that's lawfully available at state, local or government levels to the general public is not PI.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification becomes necessary following discovery or receipt of notification and must be given to anyone whose PI has been affected. Should consultation with state, local, federal, or other relevant agencies, or investigation, reveal no harm from a breach, no notification is necessary; but documentation must be maintained in writing a minimum of 5 years.

Breaches affecting 1,000 or more parties require breach notification be given to all relevant consumer reporting agencies without unreasonable delay. If a police report number is available, this must be included in such notification.

If 250 or more Oregon residents are affected by a breach, the AG must be notified in writing or electronically. The AG shall be informed in the same way as persons with breached PI. Federally exempt parties must additionally provide the AG at least one sample of a notice affected persons or primary regulators receive in a reasonable time. Entities maintaining information they neither own nor license must contact owners/licensors of that information as soon as it's reasonably possible to do so following discovery of PI breach. All such instances of disclosure must take place no longer than 45 days from incident discovery, and as soon as possible within that time frame. Reasonable delays after discovery include determination of breach scope, acquisition of necessary contact information, and restoration of IT system's integrity.

Included in breach notification should be a general description of the incident and its date (or approximate date), what PI was affected, contact information from the person providing notice for the entity, national consumer reporting agency contact information, and advice directing affected individuals regarding potential identity theft, and how to report to applicable law enforcement, the Federal Trade Commission (FTC), and the AG. Means of notification include writing, telephone (provided direct contact is made), and electronic outreach complying to the E-SIGN Act (15 U.S.C. § 7001).

Should identity theft prevention options or credit monitoring solutions be offered without charge from the entity, no credit/debit card numbers can be required of affected parties. Separate, clear, conspicuous and distinct disclosure of free protection measures to affected parties must be rendered by the entity. Any company offering services on behalf of the entity must be required by the entity to conform to such terms.

Should 350,000 or more persons be affected, costs of notification exceed $250,000, or sufficient contact information not be available, substitute notice consists of conspicuously posting about the event on any websites maintained by the entity, or major newspaper and television statewide media notification.

Associated Penalties

Failure to provide proper breach notification is considered unlawful practice; a violation of the statute under ORS 646.607, Unlawful Trade Practice.

Personal violation, aiding, or abetting could result in fines up to $1,000 per violation paid to the State Treasury, in addition to other legal penalties under law enforcement. All breaches are separate offenses in Oregon. Penalties are not to exceed $500,000. All penalties are cumulative. Under the Consumer Protection Act, fines may be as high as $25,000.

Exceptions/Exemptions

Breach notification exceptions in Oregon include compliance with separate laws, such as primary regulator laws, Title V of the Gramm-Leach-Bliley Act, HIPAA compliance, or compliance to state/federal law which is more restrictive. This is provided other laws equally require thorough disclosure in a timely manner as outlined in Oregon breach notification law.

Law enforcement notification delay is allowed should law enforcement request as much to protect a criminal investigation. Full written request by such an agency is necessary, and notification must take place as soon as reasonably possible after conclusion of investigation restrictions, as reflected by law enforcement notifying the entity in writing.

PENNSYLVANIA

Statute Codes

Breach notification regulations in Pennsylvania are covered under the Breach of Personal Information Notification Act, 73 Pa. Stat. § 2301 et seq. This includes S.B. 712, which was signed into law under Act No. 94 as of December 22, 2005 and made effective June 20, 2006.

Legal Requirements and Purpose

Breach notification in Pennsylvania becomes necessary for any entity (state agency, political subdivision, business, or individual) doing business and either storing or managing computerized data which includes Pennsylvania resident PI. Organizations not local to Pennsylvania who additionally maintain resident PA are included under this legislation.

A security breach takes place when unauthorized access of data which could materially compromise confidentiality or security of Pennsylvania resident PI as maintained by an entity happens. If there is reasonable belief injury or loss could affect a Pennsylvania resident, that's a breach. However, good-faith PI acquisition where PI isn't used improperly, and further disclosure doesn't take place, is not a security breach.

PI in Pennsylvania is defined as the first name or initial combined with a resident's last name, and other sensitive information. This additional information includes SSNs, driver's license or state ID numbers, bank account numbers, credit/debit card numbers, passwords, security codes, access questions, or anything else which may enable unauthorized users financial account access. PI doesn't apply to state, local, or federal government records, or other information lawfully available to the general public.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification becomes necessary as soon as reasonably possible following breach discovery, where PI is or is reasonably expected to have been accessed by unauthorized parties. Notice is required if encrypted information is accessed while unencrypted, if encryption security is breached, or if a person that's not authorized manages to access encryption protocols.

Should 1,000 or more individuals be affected by a breach, notification of relevant consumer reporting agencies is necessary without any unreasonable delay. Entities managing information on behalf of third parties must also notify them as expediently as possible following breach discovery. All such notification must be done as expediently as possible, excepting time necessary to determine scope of breach and restore IT system's integrity.

Means of notification include written notice, and clear telephone notice if expectation of contact is reasonable. Clearly and conspicuously, the entity must provide a description of the incident generally, and verify PI affected without requiring affected parties to furnish PI. Also, affected persons must be given a phone number they can call, or an applicable website where they can find further help. Email notice is allowed should there exist a prior business relationship, and a valid email address to an affected person. Substitute notification options can be pursued should 175,000 or more residents of Pennsylvania be affected, cost of notification be demonstrated to exceed $100,000, or sufficient contact information not be available. In such instances, all these measures must be taken email must be sent if email addresses are available,

entities who maintain websites must conspicuously post pertaining to the breach, and major statewide media must be notified.

Associated Penalties

The AG in Pennsylvania issues enforcement on breach notification, and with exclusive authority can bring actions under the Unfair Trade Practices and Consumer Protection Law for statute violation.

Exceptions/Exemptions

Exceptions for breach notification include compliance with primary federal regulators (provided such compliance reflects notification and timing guidelines in the Pennsylvania code), compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer notice act, and compliance to internal PI management protocols (consistent with Pennsylvania code) which outline timely notification in the event of an applicable breach.

Delay for law enforcement investigation of the incident is allowed, provided the entity is advised in writing which specifically references the statute. Breach notification must be made after criminal investigation compromise has been determined moot.

RHODE ISLAND

Statute Codes

Breach notification in Rhode Island is covered under the Rhode Island Identity Theft Protection Act of 2005, R.I. Gen. Laws § 11-49.2-1 et seq. This includes H.B. 6191 which became law without Governor's signature July 10, 2005, under Chapter 225, and became effective March 1, 2006.

Legal Requirements and Purpose

Breach notification is required of any entity (municipal agency, individual, sole proprietorship, state agency, partnership, corporation, association, business or legal entity, trust, joint venture, estate, commercial entity, or cooperative) that either licenses, uses, maintains, acquires, processes, owns, stores, or collects data including PI.

A security breach in Rhode Island happens when computerized data including PI for which an entity is responsible becomes subject to unauthorized acquisition or access such that security, confidentiality, or integrity of such data is compromised. PI acquired and used in good faith, without further disclosure, is not a security breach.

PI is defined in Rhode Island as the first name or first initial and last name of a resident combined with one or more pieces of sensitive information. This includes: SSNs, driver's licenses, state IDs, tribal identification numbers, account numbers, credit/debit card numbers combined with security codes, access codes, passwords,

PINs or security questions which may permit unauthorized financial account access, medical information, health insurance information, or an email address including codes, passwords, or security questions facilitating access. Rhode Island defines encryption as data transformed via algorithmic processes operating at 128 bits or higher. The purpose of such encryption is to occlude data for any but those with access credentials or decryption keys. Encrypted data acquired with a key or access password is considered unencrypted. PI doesn't include lawful information made available to the general public, or acquired through local, state, or federal government records.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification must happen immediately upon discovery of security breaches identified to pose significant risk of identity theft to affected Rhode Island residents. This is necessary even if no direct discovery has happened, but there's reasonable suspicion of a breach.

Should 500 or more Rhode Island residents be affected, the breached entity must additionally notify the AG and any applicable major credit reporting agencies pertaining to what content and distribution characterize breach notices to affected parties and the approximate time of the breach. This must be done without delaying notice to Rhode Island residents who've been affected. The timing of such notification requires notice be sent within 45 calendar days from breach confirmation. Reasonable delay includes authorization necessary to fulfill notification requirements in accordance with law enforcement.

Means of breach notification include written notice and electronic notice, provided said electronic notice complies with the E-SIGN Act (15 U.S.C. § 7001). Such notification must include, to the extent which this information is known, a general but brief description of what took place and how, as well as affected individuals. Additionally, PI affected by the breach must be included in notification, as well as the date of said breach, or an estimation thereof. Also, when the breach was discovered there must be included clear, concise information pertaining to services of remediation for affected individuals. Such remedial information may include websites or toll-free phone numbers, as well as relevant credit reporting agencies, remediation service providers, and contact information for the office of the AG. Lastly, breach notification must clearly and concisely describe how affected consumers can either obtain or file police reports, request security freezes (or get other information needed for requesting such a freeze), as well as information pertaining to possible associated fees required in dealing with consumer reporting agencies.

Substitute notice options are available when more than 50,000 Rhode Island residents are affected by a breach, it can be demonstrated cost of notification will exceed $25,000, or necessary contact information isn't available. Such substitute notice must include these three outreach methods: email notice when addresses are available, conspicuous posting on entity-maintained websites, if there are any, and major statewide media notification.

Associated Penalties

Rhode Island breach notification penalties include a fine of not more than $100 per record of that which is determined to be “reckless violation”. This is constituted as a civil violation. Should knowing and willful violation be determined, a penalty of no more than $200 per record could be leveled against a defendant. Basically, if the AG thinks a violation has occurred, and it’s in the public interest to bring an action against an entity seen in violation of breach notification law, the AG may do so.

Exceptions/Exemptions

Breach notification exceptions in Rhode Island include compliance to other laws, internal PI management, and notification policies. Should an entity keep security breach procedures internally which agree with Rhode Island law in terms of timely notification, this is permissible. Primary federal regulator compliance also constitutes breach notification fulfillment. A financial group, trust, credit union, or associated affiliates subject to the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be held in compliance. HIPAA-covered entities are likewise compliant.

Delay in notification may happen should law enforcement determine notification will impede a criminal investigation. Law enforcement agencies requesting notification delay must notify the entity when such delay no longer applies, and the entity must then immediately commence to regular notification procedures. Entities must cooperate with law enforcement investigation, sharing all relevant information pertaining to the incident except that which is a trade secret or otherwise confidential.

Waivers are not permitted in Rhode Island.

SOUTH CAROLINA

Statute Codes

Breach notification law in South Carolina is covered under the Financial Identity Fraud and Identity Theft Protection Act, S.C. Code § 39-1-90. This includes S.B. 453, which became law April 2, 2008, and was made effective July 1, 2009, and H.B. 3248, which became law April 23, 2013, and became effective the same day.

Legal Requirements and Purpose

An entity conducting business in South Carolina, and either licensing or owning computerized data including PI, must provide breach notification to affected parties when breaches occur. South Carolina defines an entity as a natural person, individual, government or governmental subdivision or agency, corporation, partnership, estate, trust, association, or cooperative.

A security breach is when unauthorized acquisition or access to non-encrypted or redacted PI happens in a way compromising integrity, confidentiality, or security of

said data. A breach is when this is known to have occurred, or it's reasonably likely to have occurred. PI acquired and used in good faith without being further distributed is not a security breach.

PI is defined as the first name or initial and last name of a South Carolina resident combined with other sensitive data. This additional sensitive data includes: SSNs, driver's licenses or state ID numbers, financial information of any kind allowing unauthorized access (credit/debit card numbers, passwords, security codes, banking account numbers, or security questions), or any other information usable to access financial information or any other information issued by government or regulatory agency which could uniquely identify the affected individual. PI doesn't include information legally available to the general public, or government records likewise legally available at local, state, or federal levels.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification becomes obligatory as soon as it's either noticed or reasonably suspected PI that is either unencrypted or redacted (or keys/access credentials to encrypted information) has been compromised in a way which could harm affected parties.

If 1,000 or more persons are affected by a breach, the entity must additionally notify the Consumer Protection Division of the Department of Consumer Affairs, as well as any relevant consumer reporting agencies. The Consumer Protection Division must be supplied with details pertaining to timing, content, and distribution of breach notification. If the entity maintains PI it doesn't own or license for a third party, that third party must be contacted immediately following breach discovery. The timing of such notification must be done without any unreasonable delay. Reasonable delays include breach scope determination and data system integrity restoration.

Means of providing notice include written and telephone outreach, as well as electronic notice provided it conforms to the E-SIGN Act (15 U.S.C. § 7001). Substitute notification is allowed should more than 500,000 South Carolina residents be affected, it be demonstrable that notification costs would exceed $250,000, or sufficient contact information not be available. Such substitute notification methods include email notice when applicable, conspicuous posting pertaining to the breach on entity-maintained websites, and major statewide media notification.

Associated Penalties

Breach notification penalties include civil actions brought by injured South Carolina residents for recovery of damages when it can be demonstrated breach notification constitutes a knowing violation. Actual damages from violation can be sought, as well as an injunction enforcing compliance, and recovery of court costs and attorney fees. According to South Carolina law, knowingly or willfully violating breach notification laws makes the perpetrator subject to an administrative fine as high as $1,000 for each resident whose PI was affected by a breach. The Department of Consumer Affairs will determine amounts here.

Exceptions/Exemptions

Internal protocols managing PI and providing timely notification in compliance with South Carolina breach notification law shall be deemed in compliance. Additionally, compliance to the Gramm-Leach-Bliley Act is allowed. Financial institutions subject to the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice of March 7, 2005, will be held in compliance as well.

Law enforcement delay is permissible if it's found notification could impede criminal investigation. Once law enforcement delay on notification is lifted, notification must commence as immediately as possible.

SOUTH DAKOTA

Statute Codes

South Dakota breach notification is covered under South Dakota S.B. 62, which became law March 21, 2018, and became effective July 1, 2018.

Legal Requirements and Purpose

Breach notification must take place should computerized PI managed by an "Information Holder" experience data breach. An Information Holder is any operation or person conducting business in South Dakota.

A security breach in South Dakota is when unauthorized acquisition of PI that isn't encrypted, or which includes measures to bypass encryption such as a key, is accessed in a way that may materially compromise integrity, confidentiality, or security of that data. Good-faith acquisition of PI isn't a breach, provided the PI isn't misused, or further disclosed to unauthorized parties.

PI has two categories in South Dakota: "Personal" and "Protected". PI of a personal nature pertains to the first name or initial and last name of a South Dakota resident combined with SSNs, driver's license number or any unique ID number as designed or managed by a government group, a financial account number, debit/credit card numbers, security codes, access codes, PINs, routing numbers, or anything that could facilitate unauthorized access to a financial account. Additionally, health information as HIPAA defines it in 45 CFR 160.103 is personal PI, as is any employer ID in combination with access codes or other authentication credentials. Lawfully available information the general public has access to at state, local, and federal levels isn't personal PI.

Meanwhile, protected PI includes email addresses and usernames, as well as associated security questions and passwords. Also, bank account numbers, credit/

debit card numbers, or their security access information (passcodes and security questions) are protected PI. (There is a crossover between personal and protected PI.)

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification must happen upon discovery of a security system breach affecting the PI of Information Holders. Notice isn't required should appropriate investigation and AG notification confirm affected individuals won't experience harm. The Information Holder must document such incidents in writing, however, and maintain such documentation no less than three years.

The AG must be notified should 250 or more residents be impacted by an Information Holder data breach. Without unreasonable delay, relevant consumer reporting agencies must be notified, as well as any other relevant agency or bureau, in the event of a security breach. Such notification must be given within sixty days of breach discovery. Means of notification include written notice and electronic notice in compliance with the E-SIGN Act (15 U.S.C. § 7001). Should 500,000 or more South Dakota residents be affected, it be demonstrable by the Information Holder that breach notification costs will exceed $250,000, or requisite contact information of affected residents not be available, three secondary notification methods must be used. Email, as available, conspicuous posts on any websites Information Holders maintain, and statewide media notification.

Associated Penalties

South Dakota breach notification is enforced by the AG, who under the Act has authority to bring an action for civil penalties.

Under the Consumer Protection Act, intentional violation could result in fines up to $2,000 per violation. The AG may prosecute on a business or individual basis. Civil action no greater than $10,000 per day per violation may apply. The AG could also recover costs or fees associated with breach action. Gramm-Leach-Bliley Act adherents and HIPAA adherents are exempt.

Exceptions/Exemptions

Breach notification exceptions include compliance with other laws. For example, federal compliance to GLBA and HIPAA is permitted, and will not require additional notification. Also, internal PI management and notification laws are compliant, provided they conform to breach notification timeframes.

Law enforcement delays for investigations are permissible, provided the Information Holder notifies affected parties within 30 days from the time notification becomes allowed again by investigators.

TENNESSEE

Statute Codes

Breach notification law for Tennessee is collected under the Tennessee Identity Theft Deterrence Act of 1999, Tenn. Code § 47-18-2017. This includes H.B. 2170, made law under Chapter 473 on June 8, 2005, and made effective July 1, 2005, S.B. 2005, which became law March 24, 2016, and was rendered effective July 1, 2016, and S.B. 547, which was signed into law April 4, 2017, and became effective the same day.

Legal Requirements And Purpose

Entities experiencing a security breach must provide breach notification to affected parties. Entities are referred to those conducting business as an individual, profitable business ventures, or agencies (including any political subdivisions) who either license or own computerized data including PI. Entities not local to Tennessee are still covered under this law if they own or license computerized data including PI pertaining to Tennessee residents.

A security breach is either acquisition of unencrypted computerized data including PI, or unauthorized access to encrypted computerized PI data including a decryption key. This access must compromise confidentiality, security, or integrity of PI. To be considered encrypted in Tennessee, data must be encrypted in accordance with the Federal Information Processing Standard, FIPS, 140-2. Acquisition of PI in good-faith isn't a security breach if the data isn't used improperly, and no further unauthorized access happens.

Tennessee defines PI as the first name or initial and last name of a resident in combination with their SSN, driver's license number, or any financial information which could lead to unauthorized financial account access. PI doesn't include information available to the general public legally, or as collected by government records at local, state, and federal levels. PI is also not redacted or otherwise unusable.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification obligation comes into effect upon security breach. Immediate notification is necessary without unreasonable delay should a breach happen, or there be a good reason to believe Tennessee resident PI may be visible to unauthorized parties toward unlawful ends.

Should 1,000 or more residents have PI compromised, relevant consumer reporting agencies must additionally be notified without any unreasonable delay pertaining to when the breach happened, how extensive the breach was, and what is included in breach notification. Should the entity maintain PI it neither owns nor licenses for third parties, those parties must additionally be notified immediately upon security breach discovery, barring reasonable delay. Such disclosure must take place within 45 days unless law enforcement delays notification legitimately.

Notice may be provided by written or electronic means, provided electronic outreach is in compliance with the E-SIGN Act (15 U.S.C. § 7001). If 500,000 or more residents are affected by security breach, potential breach notification costs can be demonstrated by the breached entity as exceeding $250,000, or requisite contact information for affected Tennessee residents isn't available, three substitute measures of notification must be taken: email notice when there are available addresses, conspicuous posts to any entity-maintained websites, and major statewide media notification.

Associated Penalties

Breach notification penalties in Tennessee are related to rulings which result from Private Right of Action laws.

Under the Consumer Protection Act, fees of $1,000 per violation may be required. Private lawsuits and civil actions may be pursued by individuals or groups for damage recovery. Attorney fees and costs may be required from those found out of compliance.

Exceptions/Exemptions

Breach notification exception exists for entities with internal PI management and notification laws which provide information pertaining to applicable security breaches in agreement with time limitations as outlined by state law. Also, compliance with other laws is recognized by Tennessee; including compliance to Title V of the Gramm-Leach-Bliley Act, and compliance to HIPAA (42 U.S.C. § 1320d).

Should law enforcement require delay for criminal investigation, this is permissible provided breach notification takes place within 45 days of law enforcement removing notification restrictions.

TEXAS

Statute Codes

Breach notification laws in Texas are covered under Tex. Bus. & Com. Code §§ 521.002, 521.053. This covers Acts 2007, 80th Leg., ch. 885, § 2.01., which was Amended by Acts 2009, 81st Leg., ch. 419, § 3, and made effective April 1, 2009. Acts 2011, 82nd Leg., ch. 1126, § 14, H.B. No. 300, was made effective September 1, 2012. Lastly, S.B. 1610 was signed into law June 14, 2013, and became effective the same day.

Legal Requirements And Purpose

Breach notification is required of entities managing computerized data including PI in an ownership or licensing capacity. Entities in Texas are businesses or persons conducting business in the state. Entities out of state managing PI of Texas residents are included under this legislation.

A security breach transpires when unauthorized parties gain acquisition of computerized data including PI in ways which compromise security, integrity, or confidentiality of that data. This includes encrypted PI, should the breach provide unauthorized parties with a decryption key. Good-faith PI acquisition isn't a security breach if the information is used properly, and isn't further disseminated.

PI in Texas is defined as the first name or initial and last name of a Texas resident combined with other sensitive information like driver's licenses, SSNs, government ID numbers, financial account numbers and credit/debit card numbers, and passwords, security questions, or other information which could be used to unlawfully permit access to a financial account. Texas also makes delineation between PI and sensitive PI. In Texas, Sensitive PI is information related to the physical/mental health of an individual, healthcare aspects of that individual, or payment/provision for such an individual's healthcare. Sensitive PI doesn't relate to publicly available information lawfully visible to the general public from federal, state, or local government records.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligation of breach notification develops should any security breach take place where sensitive PI is, or is believed to have been, acquired by unauthorized parties in a way which may lead to harm. This disclosure must transpire as immediately as reasonably possible. Should 10,000 or more persons be affected by security breach, relevant consumer reporting agencies must additionally be notified pertinent to distribution, timing, and content of applicable notices.

Entities maintaining data for third parties, but not owning or licensing that data, must provide disclosure to third parties pertaining to sensitive PI breach as soon as reasonably possible upon breach discovery. Allowable delays include breach scope determination, data system integrity restoration, and law enforcement rulings regarding whether notification will affect any criminal investigation.

Means of notification include written notice to the most recent known address of affected Texas residents, or electronic notice in compliance with the E-SIGN Act (15 U.S.C. § 7001). Should affected persons be residents of states with their own breach notification laws, entities may provide notice under that state's law, or the law of Texas. Substitute notification options are available should 500,000 or more residents be affected, whether it be demonstrable by the entity that breach notification would exceed $250,000 in cost, or sufficient contact information not exist for affected parties. Substitute notification options include email when applicable, conspicuously posting information pertaining to security breach on any entity-maintained websites, and broadcasting the security breach on any applicable major statewide media.

Associated Penalties

Breach notification penalties in Texas include civil penalties of $2,000 to $50,000 for each violation and potential injunctive relief. Should compliance failure be demonstrated, fines of $100 per affected person per day may be due, but cannot exceed $250,000 per breach.

Exceptions/Exemptions

Exceptions to breach notification law include internal policies entities may have pertaining to PI breach notification consistent with Texas law in terms of outreach and timing, as well as delays for law enforcement. Should law enforcement agencies determine breach notification may impede an investigation, delay is allowed provided notification take place as soon as feasibly possible once notification restrictions be removed.

UTAH

Statute Codes

Breach notification laws in Utah are included under the Protection of Personal Information Act, Utah Code §§ 13-44-101, 13-44-202, 13-44-301. This includes S.B. 69, which became law March 20, 2006, under Session Law Chapter 343, and became effective January 1, 2007. It also includes S.B. 208, which became law March 30, 2009, and became effective May 1, 2009.

Legal Requirements And Purpose

Breach notification in Utah is required of entities experiencing security breach of computerized PI they're responsible for. An entity is any person or group owning or licensing computerized PI of a Utah resident.

A security breach in Utah is defined as unauthorized acquisition of computerized PI such that confidentiality, security, or integrity may be compromised. Employees or agencies with PI who aren't authorized won't be considered breaching security provided PI isn't used inappropriately, or further disseminated.

Utah defines PI as the first name or initial of an individual combined with their last name, and other sensitive information such as SSNs, driver's license or state ID numbers, or any financial information which could lead to unlawful access of a person's financial account; including credit card numbers, account numbers, debit card numbers, passwords, security questions, PINs, or anything else relevant. PI doesn't include legally available information at state, local, or federal levels through government records, or other widely distributed media that the general public may access.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification becomes obligatory should investigation reveal PI misuse, theft, fraud, or reasonable suspicion of such compromising factors. If good-faith, prompt investigation of suspected breach reveals no potential harm or misuse to resident PI, no notification is necessary.

Should an entity manage information on behalf of a third party, that third party must be notified immediately following a breach, or suspected breach, as soon as reasonably feasible. The timing of any notification must represent utmost expediency, delays allowed being breach scope determination and data system integrity restoration.

Means of providing notification include writing via first-class mail to most recent addresses on file, telephone outreach including automatic dialing tech not restricted legally, electronic outreach in compliance to the E-SIGN Act (15 U.S.C. § 7001), or publication of breach information in a generally circulated newspaper in compliance to Utah Code § 45-1-101. There are no substitute notice options in Utah.

Associated Penalties

Breach notification waivers are not permitted in Utah, and penalties are presided over by the AG. Financial penalties for those found out of compliance could be civil fines no more than $2,500 either for one or a series of violations pertaining to a specific consumer, but will not reach greater than an aggregate of $100,000 for total violations to more than a single consumer.

Exceptions/Exemptions

Breach notification exceptions include internal PI management policies in compliance with time and notification policies of Utah code, and compliance with other federal or state laws that are likewise in agreement. Being compliant to such laws, and notifying residents accordingly, will not incur repeat notification necessity.

Law enforcement delays for criminal investigation are allowed, provided good-faith breach notification takes place without unreasonable delay once disclosure restrictions are removed by the authorities.

VERMONT

Statute Codes

Breach notification statute codes in Vermont are covered under 9 V.S.A §§ 2430, 2435. This includes S. 284, which was signed into law May 18, 2006 under Act 162, but Amended by H. 254; which was signed into law under Act 109 on May 8, 2012, and became effective the same day. Also, H. 513 was signed into law May 13, 2013, and became effective the same day.

Legal Requirements And Purpose

Breach notification is necessary for entities in Vermont experiencing PI security breach. An entity is a data collector who may be defined as the state, state agencies, public and private universities, political subdivisions of the state, LLCs, Financial institutions, corporations whether private or public, retailers, or any other person or

group who handles, collects, deals with, disseminates, or otherwise manages PI of a non-public kind. Automatic data collection is included under this definition, as is licensing or ownership of any PI concerning Vermont individuals.

A security breach is defined as acquisition of electronic information in an unauthorized way that may compromise integrity, security, or confidentiality of that data. An entity has not experienced security breach if PI is acquired in good-faith, though unauthorized, conditions (provided that PI is not improperly used or disclosed in an unauthorized way). Factors to determine if PI is acquired in an unauthorized way or not include indicators that PI may have been in the physical possession of an unauthorized party (a stolen computer or device), indications information may have been copied or downloaded, fraud or identity theft indicators, or non-public PI becoming public.

PI is defined in Vermont as an individual's first name or initial and last name combined with other sensitive information that isn't encrypted; or which was accessed with a decryption key. This additional information includes SSNs, motor vehicle operator's license numbers or IDs for non-drivers, and financial information allowing unauthorized account access (such as account numbers, credit/debit card numbers, PINs, passwords, or security questions). PI doesn't refer to information the public can access generally, or that is contained in federal, local, or state government records of a public nature.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification becomes necessary as soon as possible from discovery or reasonable suspicion of a security breach. Should an established notification produce no harm to individuals affected or their PI, breach notification is not necessary--as long as the Vermont AG is provided with a detailed explanation of the incident. Entities registered with The Department of Banking, Insurance, Securities, and Health Care Administration must provide said Department appropriate explanation.

Relevant consumer reporting agencies must be notified should 1,000 or more Vermont residents be affected at one time. This notification must be delivered as soon as reasonably possible. Persons licensed under Title 8 by the Department of Banking, Insurance, Securities, and Health Care Administration are not bound by this subsection.

The AG or Department of Financial Regulation must be notified of a breach within 14 business days of breach discovery, or within 14 days of the entity's consumer notifications; whichever happens sooner. If an entity has sworn in writing under AG oversight to maintain PI management policies conforming to state law, that entity must disclose to the AG prior reaching out to affected Vermont residents. Notice must include when the breach happened and a description of what happened. Should no date be known, notice must be sent when one does become known. Copies of consumer notices must be provided to the AG. Entities may also send samples of public disclosure notifications provided information pertaining to specific consumers and their PI is redacted from the public announcement.

Should entities maintain or have computerized PI data it neither owns nor licenses for third parties, those associated third parties must be notified concerning breach as soon as reasonably possible following breach discovery, in consistence with law enforcement requirements. Such notification must be done within 45 days of breach discovery, reasonable delays within this time including determination of breach scope, as well as the re-establishment of IT system security, integrity, and confidentiality.

Means of notification must be conspicuous and clear, including (when known), several specific items. The notification must say what happened generally, what PI was affected, what the entity did after the breach was discovered, available toll-free numbers affected parties can call for additional help or information, advice pertaining to vigilance in account review (and credit report monitoring for signs of identity theft or fraudulent activity), and the approximate date of breach. All these items must be provided either in written notice to residents' addresses on file, telephone notice provided actual contact is made (no prerecorded messages), or electronic notice to valid email addresses should neither telephone nor mailing information be available, and no request for additional PI including hyperlinks is included in the email. Generally, ensure electronic notification conforms to the E-SIGN Act (15 U.S.C. § 7001).

Substitute notification options are available should it be demonstrable by the entity that cost of notification may exceed $5,000, more than 5,000 people are affected, or sufficient contact information not be available. Substitute notice must consist of conspicuous posts to entity-maintained websites, and major regional and statewide media notification.

Associated Penalties

Breach notification in Vermont is enforced by the AG, and waivers are not permitted. The Data Breach Notification Act is co-equal to the Consumer Protection Act in Vermont. AG enforcement through subpoena may be pursued. Civil penalty up to $10,000 per violation could be leveled at those out of compliance. Injunctive relief may be sought.

Exceptions/Exemptions

Breach notification exceptions include financial institutions already operating in compliance to The Federal Interagency Guidance Response Programs for Unauthorized Access To Consumer Information and Customer Notice, issued March 7, 2005. Additional exemption includes compliance to the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice as issued April 14, 2005.

Should law enforcement delay notification for investigation, this is permissible. Written request from law enforcement agency is advised. Should no written request be made, the entity must document the request contemporaneously, in writing, being sure to include the names of officers of the law requesting delay, as well as their associated agency. When notification restrictions are lifted, breach notification without unreasonable delay must immediately be provided. This is to commence when legal authorities provide written communication which the entity may demonstrate via receipt. Such media may include electronic communication or facsimile.

VIRGINIA

Statute Codes

Breach notification is covered in Virginia under Va. Code § 18-2-186.6, which was made effective on July 1, 2008, and amended to § 18-2-186.6; HB 2113. This became effective July 1, 2017. Additionally, § 32.1-127.1:05 became effective January 1, 2011.

Legal Requirements And Purpose

Breach notification in Virginia is necessary if computerized PI as managed by an entity is compromised under security breach. An entity is defined by Virginia as individuals, business trusts, corporations, partnerships, LLCs, Limited Liability Partnerships, associations, organizations, government agency, subdivision, or instrumentality, joint ventures, legal entities, or any other group who, for profit or not, either owns or licenses computerized data which includes PI.

Government entities have an additional provision. Specifically, health information collected by authorities, boards, bureaus, commissions, districts, or agencies of the Commonwealth, or which represent any Commonwealth subdivision. This also includes towns, counties, cities, governing bodies of counties, municipal counties, planning commissions, school boards, and boards of visitors to public institutions of higher education. Finally, other corporations, organizations, or agencies of Virginia which in whole or principally are supported by public funds are defined under these Government Entity provisions.

A security breach is defined as access or acquisition of PI in an unauthorized way, provided that data is neither encrypted nor redacted, and no encryption key exists to decrypt such PI. Should an entity have reasonable reason to believe such access may initiate identity theft or other fraud, a data breach has happened. Good-faith PI acquisition where data is properly used and not further disclosed is not defined as a security breach.

PI in Virginia is defined as the first initial or name and last name of a Virginia resident combined with additional unencrypted or un-redacted data such as SSNs, driver's license or other state ID numbers, or any financial account information which allows for unauthorized access. Account numbers, credit/debit card numbers, security access codes, PINs, passwords, or security questions are included here. Health information is a citizen's first and last name (or first initial and last name) combined with any medical or health history, including mental or physical conditions, diagnoses, or treatment programs. Additionally, health insurance policy or subscriber numbers, as well as any other associated identifying numbers, are PI under this definition. PI doesn't include lawfully available information the general public can access, or lawfully available government records at federal, state, or local levels.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification must take place should breach be discovered, or breach be reasonably expected to have transpired--provided the breach may be expected to result in identity theft, fraud, or other applicable harm to Virginia residents. Breach notification must take place if encrypted information is accessed when it isn't in an encrypted form, or if a key to encryption has been accessed by unauthorized parties. When health information is compromised, individuals involved with the subject of the medical information, or who the information directly concerns, must be individually contacted should there be more than one person affected.

Relevant consumer reporting agencies must be contacted should more than 1,000 persons be affected by a breach. They must be notified without any unreasonable delay. The AG must be notified as well should 1,000 or more persons be affected and without unreasonable delay. The AG must be told when the breach occurred, how it was distributed, and what content is included in notifications. Health-related breaches require an entity to contact the Commissioner of Health. Payroll service providers or employers licensing or owning PI data pertaining to withheld income tax must contact the AG, providing them federal employer identification numbers without any unreasonable delay should a breach be discovered. From there, the AG must notify the Department of Taxation pertaining to the breach.

Should an entity own or license third-party information, that third party must be notified as immediately as possible without unreasonable delay pertaining to a breach, as soon as a breach is discovered. Reasonable delays for notification include breach scope determination and data system integrity restoration.

Breach notification must include several distinct pieces of information. The incident must be generally described, what PI was compromised must be communicated, acts taken in response must be outlined, telephone numbers affected parties can call for help or more information must be provided, and advice must be given pertaining to affected parties maintaining vigilance in account statement review and credit report monitoring. Means of providing such notice may include sending written notification to recently available mailing addresses, telephone notice, or electronic notice. Substitute notice options are available should the affected Entity be able to demonstrate breach notification costs will exceed $50,000, more than 100,000 Virginia residents be affected, or contact information be unavailable. In such circumstances, all the following tactics must be used: email outreach where possible, conspicuous posts pertaining to the breach on entity-maintained websites, and major statewide media notification.

Associated Penalties

Breach notification penalties are enforced by the AG in Virginia. AG-imposed civil penalties are not allowed to exceed $150,000 per system security reach, or a similar series of breaches discovered through a single investigation. (This provision has no application regarding breaches of health information.)

Exceptions/Exemptions

Breach notification exceptions include internal policies pertaining to PI management and breach notification which agree with Virginia law. Entities following Title V of the Gramm-Leach-Bliley Act will be held in compliance, as will those who comply to primary state or federal regulators. “Covered Entities” or “Business Associates” under HIPAA will be held in compliance subject to breach requirements pertaining to health information protected under 42 U.S.C § 17932 et seq., or involving a non-HIPAA “entity subject” under the Health Breach Notification Rule as promulgated by the FTC (Federal Trade Commission) pursuant to 42 U.S.C. § 17937 et seq.

Should law enforcement delay breach notification, this is allowed, provided breach notification takes place without reasonable delay once disclosure limitations are lifted.

WASHINGTON

Statute Codes

Breach notification in Washington is covered under Wash. Rev. Code § 19.255.010 et seq., § 42.56.590. This includes S.B. 6043, which became law under Chapter 368 on May 10, 2005, and became effective July 25, 2005. H.B. 1149 is additionally included, and requires payment processor, business, vendor, and financial institution reimbursement for expenses related to credit or debit card replacement after a breach. This was signed into law March 22, 2010, and became effective July 1, 2010. Lastly, Washington breach notification law includes H.B. 1078, which was signed into law April 23, 2015, and became law July 24, 2015.

Legal Requirements And Purpose

Breach notification is necessary for any entity experiencing PI data breach concerning data it owns or licenses on behalf of Washington residents. An “entity” in Washington is any local agency, person, or business conducting business in the state.

A security breach is when data compromising security, integrity, or confidentiality of entity-maintained PI is either accessed or acquired by unauthorized persons. PI acquired through good-faith isn’t a breach if it’s not misused or otherwise disclosed.

Washington defines PI as the first name or initial and last name of a Washington resident combined with SSNs, driver’s licenses or state IDs, or any financial information which may permit illegal access to a resident’s financial account; including credit/debit card numbers, account numbers, passwords, security codes, access codes, PINs, or anything else which could be so-used. PI doesn’t include legally available information from local, state, or federal government agencies, or information generally available to the public at large.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification obligation begins as soon as breach discovery happens. Notification must be sent out as soon as reasonably possible when there's a definite breach, or it's suspected that a breach which could compromise PI has transpired. This is if the PI wasn't "secured", meaning properly encrypted with no decryption key being accessible without authorization. Should it be determined no reasonable harm to affected parties will occur, breach notification is not necessary.

An entity must notify the AG if 500 or more Washington residents are affected by a single breach. This breach must include a single electronic sample copy electronically submitted to the AG, but redacting PI information. The entity must also appraise the AG of how many consumers the breach affected, or estimates if exactitude cannot be determined.

If entities maintain data they neither own nor license for a third party, those third parties must be notified as soon as possible following breach discovery, or reasonable suspicion of PI compromise. The timing of all such notifications must constitute the quickest possible notification delivery without unreasonable delay. The upper limit is 45 calendar days after breach discovery. Reasonable delays include deliberate restriction from law enforcement pertaining to a criminal investigation, breach scope determination, and restoration of system's integrity. Means of notification provision may include written notice, and electronic notification in compliance with the E-SIGN Act (15 U.S.C. § 7001). Included in plain language in such a notification must be names and contact information of reporting individuals or agencies subject to this law, what kind of PI was believed to have been affected, and toll-free phone numbers and available addresses to applicable credit reporting agencies. Substitute notification is available should entities be able to demonstrate notification cost exceeds $250,000, more than 500,000 persons are affected, or sufficient contact information cannot be obtained. In such instances, all of these substitute notification methods must be used: email outreach where possible, conspicuous posts to entity-maintained websites, and major statewide media notification.

Associated Penalties

Breach notification penalty may come from the AG, who can bring an action on behalf of affected residents. A violation of this breach notification statute is considered to be either an unfair method of competition or deceptive act. Consumers injured by breach notification violation are able to recover damages through a civil action.

The attorney general may bring action on behalf of residents to enforce these state statutes regarding noncompliance and failure to take precautions against a breach. Consumer Protection Act fines could be as high as $2,000 per violation.

Exceptions/Exemptions

Breach notification exceptions chiefly concern compliance to other existing laws. Financial institutions under the authority of the comptroller of currency, the federal deposit insurance corporation, credit union administration, or federal reserve system are deemed in compliance under the Interagency Guidelines for Establishing Information Security Standards. The specific laws are 12 C.F.R., Part 30, Appendix B, 12 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, 12 C.F.R. Part 364,

Appendix B, and lastly 12 C.F.R Part 748, Appendices A and B. Compliance is granted given proper notification of affected persons in timeframes as outlined under Washington breach notification law. Entities must comply with AG notification requirements, and also notify applicable primary federal regulators. HIPAA-covered entities are also considered compliant, should they operate in accordance with section 13402 of the Federal Health Information Technology For Economic and Clinical Health Act, Public Law 111-5. The AG must be notified by covered entities conforming to notification guidelines and timeline requirements of section 13402. Finally, entities maintaining interior PI management protocols matching Washington law are deemed in compliance.

Delay for law enforcement investigation is allowed, provided affected parties are notified of a breach as soon as possible after notification restrictions have been lifted.

Should a breach transpire where unencrypted financial information be compromised, or PCI DSS compliance is not in evidence, vendors, businesses, and payment processors can be held liable for the expense of reissuing credit/debit cards should full unencrypted account information pertaining to such identification devices be exposed.

WASHINGTON, D.C.

Statute Codes

Signed into law March 8, 2007, and made effective July 1, 2007, is breach notification legislation under D.C. Code § 28-3851 et seq., Council Bill 16-810.

Legal Requirements And Purpose

In Washington, D.C., breach notification must take place when any entity has computerized PI compromised. Entities include any persons or groups dealing in computerized PI. Entities maintaining PI on D.C. residents from without D.C. limits are also legislated under this statute.

A security breach in D.C. is defined as unauthorized acquisition of PI data which is not used in good faith; that is to say: it compromises integrity, security, or confidentiality of affected parties. Data which has been made secure in a way preventing unauthorized persons from accessing it is not deemed a security breach. Anything given in good faith is not a breach, provided such PI isn't used improperly.

D.C. defines PI as any number, any code, or any combination of this information which provides access to financial accounts. It's also defined as a first name and last name, or a first initial and last name, or any other identifying characteristic, tied to specific information like. D.C.'s laws specifically identify information such as SSNs, driver's licenses, identification cards, credit card numbers or debit card numbers as

PI. PI does not include information that is publicly available, or has been legally made available through state, federal, or local government records.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

For those who it applies to, breach notification becomes obligatory should PI be involved. If more than 1,000 persons are affected, consumer reporting agencies must be notified as swiftly as possible. This does not apply to entities required to notify consumer reporting agencies under Title V of the Gramm-Leach-Bliley Act.

When an entity keeps computerized PI they don't own for a third party, that owner/licensee must be notified as expediently as possible after a breach has been discovered. All notifications must take place as swiftly as possible in consistence with time necessary to determine how big the breach was and restore associated data systems.

Means of notification can include written or electronic notice, provided electronic notice conforms to the E-SIGN Act (15 U.S.S. § 7001). Substitute notice options are permissible if cost of providing notification exceeds $50,000, or more than 100,000 D.C. residents have been affected, or contact information for affected parties is not available. These substitute notification options must include all three of the following actions: email to affected persons when it becomes available, posting of a conspicuous sort on entity website(s) if there are any, and notifying of major local or national media, if national media notification is necessary.

Associated Penalties

Penalties pertaining to breach notification in D.C. are enforced by the AG, who may seek either direct damages or injunctive relief. D.C. residents injured by violation of these breach notification statutes may pursue civil action for recovery of damages in the wake of compromised PI. These damages may include action costs and attorney fees. Dignitary damages such as suffering or pain will not be included.

In D.C., breach violations are enforced through the AG, who may recover civil penalties up to $100 per violation, in addition to lawyers' fees and costs. Under the Consumer Protection Act, $1,000 per violation may be required of those found out of compliance.

Exceptions/Exemptions

Breach notification exemptions include internal laws in compliance to existing statutes in terms of timing, etc. Notification by email is permissible exclusively should this be the primary mode of communication between the entity and affected party.

Delay is permissible should law enforcement determine notification would impede a criminal investigation. However, as soon as the investigation is concluded, or law enforcement lifts the delay, notification must be made.

WEST VIRGINIA

Statute Codes

Breach notification in West Virginia is covered under W. VA. Code § 46A-2A-101 et seq. This includes S.B. 340, which became law March 27, 2008, and became effective June 6 2008.

Legal Requirements And Purpose

Breach notification must be provided if an entity maintaining PI for West Virginia residents is compromised by a security breach. An entity is any legal entity, including agencies, instrumentalities, or subdivisions of the government, government groups, organizations, joint ventures, associations, LLCs, limited liability partnerships, partnerships, limited partnerships, business trusts, estates, individuals, or corporations.

A security breach transpires when unauthorized acquisition or access of computerized PI neither redacted nor encrypted compromises PI confidentiality or security in a way which could result in fraud or identity theft to West Virginia residents. Acquisition of PI in good-faith is no security breach, provided that information isn't improperly used or disclosed.

PI is defined in West Virginia as the first name or initial and last name of a West Virginia resident combined with additional data elements such as SSNs, driver's licenses, state ID numbers, bank account numbers, credit/debit cards, access codes, passwords, security questions, or anything else used to gain unauthorized financial account access. PI doesn't pertain to lawfully available information available to the general public either through media distribution, or government records at state, local, or federal levels.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification becomes obligatory when discovery or reasonable belief of breach which may harm affected individuals develops. Should the breach not acquire encrypted information, but a decryption key, notice is also required.

Relevant consumer reporting agencies must be notified should 1,000 or more persons be affected. Such notification must take place without unreasonable delay. Notification must include what content is included in breach notification messages, when the breach occurred, and how it was distributed. Names or other PI of recipients of breach notification reports are not required in consumer reporting agency disclosure.

Entities who manage computerized PI on behalf of third parties must notify those third parties upon discovery or reasonable belief of security breach. Such disclosure must come as soon as reasonably possible. Notification should include all categories of PI affected, as it's possible to demonstrate them. Also, notices should include

phone numbers and websites usable to contact the entity, as well as what data is maintained by the entity on individual or individuals, and toll-free contact numbers and addresses for applicable major credit reporting agencies. Lastly, it should include advice on how to place a fraud alert or credit freeze. Means of notification include written notice to most recent postal addresses, telephone notice, or electronic notice compliant with the E-SIGN Act (15 U.S.C. § 7001). Should the entity be able to show breach notification cost exceeds $50,000, more than 100,000 persons are affected, or sufficient contact information cannot be acquired, substitute notification options include any two of the following: email outreach where addresses are available, conspicuous posting on entity-maintained websites, and major statewide media notification.

Associated Penalties

Breach notification penalties are enforced by the AG. AG enforcement advances West Virginia penalties. Repeated violation of defendants may initiate a civil action. Max penalties are $150,000 per security breach in cases where the civil action is pursued. Financial institution regulation breach is enforced by such an entity's functional regulator. Under the Consumer Protection Act, repeated, the willful violation may constitute fines of $5,000 per violation.

Exceptions/Exemptions

Breach notification exceptions include Federal Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and Customer Notice compliance, and primary state or federal regulator compliance. Additionally, internal notification policies pertaining to PI breach and in agreement with all West Virginia laws concerning outreach methods, content, and timing will be deemed in compliance. Lastly, entities in compliance to Title V of the Gramm-Leach-Bliley act are exempted.

Should law enforcement require breach notification delay, this is permissible provided the entity notify affected parties as soon as reasonably possible to when law enforcement lifts notification restriction.

WISCONSIN

Statute Codes

Breach notification statute codes for Wisconsin are covered under Wis. Stat. §134.98. This includes S.B. 164, which was made law under Act 138 March 16, 2006, and became effective March 31, 2006.

Legal Requirements And Purpose

Breach notification becomes necessary when computerized data maintained by anentity is compromised. An entity in Wisconsin is defined as any group or person managing, licensing, or owning PI. This includes any state group, department,

independent agency, institution, authority, association, society, or other body of local government either authorized or made through law or constitution. Also included are cities, villages, legislature, courts, towns, counties, and people who aren't defined as individuals, but are defined as conducting and containing Wisconsin business in a way which regularly incorporates PI, licenses PI in Wisconsin, maintains PI for a Wisconsin resident concerning a depository account, or lends money to a Wisconsin resident.

A security breach takes place when unauthorized PI access transpires or is suspected to have transpired. If principle places of business where PI is located aren't in Wisconsin, but contain PI on state residents, this is also defined as a security breach.

PI is the unencrypted and un-redacted first name or initial and last name of a Wisconsin resident in combination with SSNs, driver's licenses or state ID numbers, or any financial information that could be used to fraudulently access a person's account; including credit/debit card numbers, security access codes, passwords, security questions, or other applicable information. Additionally, PI includes DNA profiles and unique biometric data--such as fingerprints, voice prints, retina or iris images, or anything else uniquely physical. Any elements of data publicly available in a legal way through media or government agency at state, local, or federal levels is not considered PI.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Obligatory breach notification applies when breaches are discovered or strongly suspected, and to each afflicted party. If PI acquisition won't harm individuals in terms of fraud or identity theft, breach notification is not required. Good faith PI acquisition isn't a security breach if the data isn't used illegally or further distributed by the associated entity employee.

Should 1,000 or more residents be affected by a security breach, applicable consumer reporting agencies must be notified as quickly as reasonably possible concerning what PI was affected, how the breach was distributed, and what the notices sent to individuals contained.

Entities who maintain data they don't own for third parties must also notify those third parties as soon as reasonably feasible after breach discovery or suspicion. The timing of any notification must be within 45 days of breach discovery. Reasonable delays include determination of breach scope and means of communication an entity has. Such notification must indicate affected Entities are aware of the security breach, and be sent out either by mail, or a means the entity has previously employed for communication with subjects whose PI they manage. Substitute notification options become available if mailing addresses of affected parties can't be ascertained, or previous communication has not taken place between the entity and the person affected by data breach. In such instances, the entity will provide substitute notice by means which is calculated to actually alert the affected party, within reason.

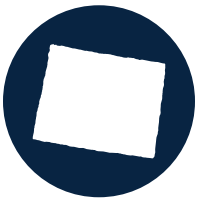
Associated Penalties

Breach notification penalties are determined by relevant Wisconsin authorities.

Knowing breach violation, or assistance in violation risks conviction and associated charges. Under the Consumer Protection Act, minimum fines for each violation are $100, maxing out at $10,000. Civil penalties may also apply, with a range of $50 to $10,000 as dictated by particular violations.

Exceptions/Exemptions

Breach notification exceptions in Wisconsin include compliance to the Gramm-Leach-Bliley Act under Title V, as well as entities in compliance with HIPAA. Additional exceptions include law enforcement delays when a criminal investigation takes place, provided notification takes place as soon as law enforcement allows.



WYOMING

Statute Codes

Breach Notification in Wyoming is contained under Wyo. Stat. § 40-12-501 et seq. This became effective July 1, 2007. Additionally, Senate File Nos. 35 and 36 were signed into law on March 2, 2015, and became effective July 1, 2015.

Legal Requirements And Purpose

Breach notification requirements in Wyoming pertain to entities, which are individual or commercial operations conducting business in Wyoming which own or license computerized information about Wyoming residents containing PI.

A security breach takes place when unauthorized acquisition of PI which may materially compromise integrity, security, or confidentiality of Wyoming Residents in a way that could cause loss or injury happens. Acquisition of PI by employees or agents of entities in good-faith is not a breach, provided PI isn't used improperly or further disclosed.

Wyoming defines PI as the first name or first initial and last name of a Wyoming resident in combination with an SSN, driver's license number, any financial account information which could lead to unauthorized account access, tribal identification card, government or federally-issued ID, shared security tokens or secrets used for authentication, email addresses, usernames or security questions, marriage or birth certificates, medical information including conditions both mental and physical as well as history and treatment or diagnosis through health care professionals, any health insurance information, biometric data (voice print, fingerprint, iris or retina scan, etc.), or taxpayer ID number. PI doesn't include widely-distributed information available to the general public, or government records at state, local, or federal levels; regardless of its source.

Time Frames

Breach Reporting, Regulation Reporting, Client Notification

Breach notification is obligatory immediately upon discovery or reasonable suspicion

of PI compromise. Notification must happen as soon as it's reasonable to provide it. Should good-faith investigation determine no danger from compromised PI, notification isn't obligatory.

Entities who keep information for third parties must notify those third parties as soon as reasonably possible once breach is noticed or is suspected. Entities maintaining information between themselves may come to an agreement pertaining to who provides notification to whom.

Notification timing must be as expedient as possible, reasonable delays being breach scope determination and system integrity restoration. Notice provided must be clear, conspicuous, and include several distinct elements. These elements are a toll-free number affected individuals can use to contact applicable major credit reporting agencies, what sort of PI was affected, a general description of what happened, when approximately the breach occurred (should that be something which can be determined), general description of actions taken in the wake of an event, advice directing affected parties to maintain account review and credit report monitoring vigilance, and whether law enforcement investigation predicated delay. Means of notification include written notice and electronic mail notice. Substitute notification options are available should Wyoming-based entities be able to demonstrate cost of breach notification would exceed $10,000 (or $250,000 for entities not local to the state). Substitute options are additionally available should 10,000 or more individuals be affected (or 500,000 or more be affected out-of-state). In such instances, substitute notice options must include making conspicuous posts on entity-maintained websites or comparable proprietary electronic systems of the common carrier variety, and notification of any available major statewide media. Such notice must include toll-free phone numbers where individuals can determine if their PI was included in a given breach.

Associated Penalties

Breach notification compliance is enforced by the AG, who may bring an action in terms of law or equity as a means of addressing violations. The AG may bring appropriate relief as necessary for damage recovery, or to ensure proper compliance to Wyoming statute codes regarding breach notification.

Under the Consumer Protection Act, up to $10,000 per willful violation of breach law may be leveled against those found guilty. AG enforcement defines penalties in Wyoming and may result in additional relief as deemed appropriate.

Exceptions/Exemptions

Breach notification exceptions include compliance to financial institutions as outlined under 15 U.S.C. § 6809, or federal credit union compliance as defined under 12 U.S.C. § 1752, as well as under 15 U.S.C. § 6801(b)(3) and 12 C.F.R. pt. 364 App. B or pt. 748 App. B. Such compliance is permissible, provided it is in accord with state law pertaining to notification and timing. Also, HIPAA compliance under 45 C.F.R Parts 160 and 164 will be deemed in compliance.

Should law enforcement require delay in notification for criminal investigation, this is permissible provided the enforcement agency makes such a delay determination in writing.

CONCLUSION

Comprehensively Preparing Your Business

Regardless of the state you're in, a business, individual or group who deals with information that may be considered private needs to know what to do should a breach occur.

First, understand what constitutes a security notification. Generally a breach is exposure of PI such that it could result in some form of fraud, most famously, identity theft. From there, know your state's expectation on reporting that breach. Some states have an upper limit, some require the swiftest reporting possible. In almost all cases, there is some room for reasonable delay, but it must be "reasonable" in a sense recognizable during a court hearing. Keep everything in writing, and develop means of reaching residents swiftly when a breach happens. Remember, modern technology climates are fraught with cybercriminal threat, and internal error is equally likely to expose vulnerabilities incidentally.

What may make the most sense is working with a group like SCA to determine security solutions of a comprehensive quality. Such a professional relationship will give you the greatest likelihood of deflecting a data breach.

ABOUT US

For over 13 years our team has established a sterling reputation among 1000's of financial institutions, healthcare organizations, title and settlement companies, Government/Public Sector organizations and other businesses who handle sensitive information. SCA has a long history of success based on its core values which include building lifetime partnerships based on mutual trust and respect, a culture of service and employing dedicated, knowledgeable staff. These values have allowed us to expand, strengthening the depth and breadth of our people and services. Safeguarding critical information, regardless of media, and complying with information security regulations, are the sole focus of SCA.

GET A COMPLIMENTARY BREACH ASSESSMENT CONSULTATION WITH A TECHNOLOGY SPECIALIST TODAY

SCA

SECURITY COMPLIANCE ASSOCIATES

(727) 571-1141

2727 Ulmerton Road, Suite 310
Clearwater, Florida 33762

scasecurity.com