ALABAMA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Ala. Code § 8-38-1 to 12

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	No later than 45 days	Yes, if > 1,000 residents notified

Scope of this Summary:
Notification requirements applicable to individuals or entities that acquire, use, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements.

Risk of Harm Threshold	Notification not required if, after good-faith and prompt investigation, the covered entity determines that the breach is not reasonably likely to cause substantial harm to residents. Determination must be documented in writing and maintained for at least five years.
Breach Defined	The unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach.
Encryption Safe Harbor	Statute does not apply to covered information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable, including encryption of the data, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the personally identifying information readable or useable has been breached together with the information.
Forms of Covered Information	Electronic Only
Covered Information	First name or first initial and last name in combination with one or more of the following: • A non-truncated Social Security number or tax identification number. • A non-truncated driver's license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual. • A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account. • Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional. • An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. • A username or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.
Consumer Notice Timing	If notification required following good-faith and prompt investigation, must be made in the most expedient time possible, but no later than 45 calendar days following notification of breach or determination that breach occurred and is reasonably likely to cause substantial harm to residents.
Consumer Notice Method	By written notice (to address in covered entity's records) or electronic notice (to email address in covered entity's records). Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Notice must contain: • Description of covered info subject to breach; • Date, estimated date, or estimated date range of breach; • General description of actions taken to restore security and confidentiality of covered info; • General description of steps the affected resident can take to protect against identity theft; and • Contact info for covered entity that affected resident can use to inquire about breach.

Delayed Notice	Notification may be delayed if law enforcement determines that notification will impede a criminal investigation or national security, and if the law enforcement agency has submitted a written request for the delay.
Government Notice	If over 1,000 residents notified, must notify AG as expeditiously as possible, but no later than 45 days after notification of breach or close of investigation. Must include synopsis of events surrounding incident; approximate number of affected residents; any services being offered to residents free of charge and how to use them; contact information that AG can use to obtain additional information; supplemental or updated information may be provided at any time.
Consumer Reporting Agency Notice	If over 1,000 residents notified, must notify major Consumer Reporting Agencies without unreasonable delay of timing, distribution, and content of notices.
Exceptions for Other Laws	The statute exempts any entity subject to or regulated by federal or state laws or regulations on data breach notification, provided the entity: Maintains procedures under those laws and regulations. Provides notice to affected individuals according to those laws and regulations. Timely provides a copy of the notice sent to residents to the Attorney General when the entity notifies more than 1,000 individuals.
Third-Party Notice	If you maintain, store, process, or otherwise have access to covered info on behalf of another entity, you must notify it as expeditiously as possible and without unreasonable delay, but no later than 10 days following discovery of a breach or reason to believe breach occurred, and must cooperate by providing information in your possession so covered entity can comply with its notice requirements.
Private Right of Action	The Alabama general breach notification statute does not provide a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

ALASKA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Alaska Stat. § 45.48.010 to .090

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expeditious time possible and without unreasonable delay	No*

Scope of This Summary:

Notification requirements applicable to persons doing business or a person with more than 10 employees that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if, after appropriate investigation and after written notification to the Alaska Attorney General, covered entity determines that there is not a reasonable likelihood that harm to consumer has resulted or will result from the breach.
Breach Defined	Unauthorized acquisition, or reasonable belief of unauthorized acquisition, that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted, so long as the encryption key was not accessed or acquired.
Form of Covered Info	Electronic or Paper
Covered Information	First name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or state identification card number. ○ Account number, credit card number, or debit card number, except if these can only be accessed with a personal code, then the account, credit card, or debit card number in combination with any required security code, access code, personal identification number, or password. ○ Passwords, personal identification numbers, or other access codes for financial accounts.
Consumer Notice Timing	Must be made in the most expeditious time possible and without unreasonable delay, consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
Consumer Notice Method	By written notice or electronic notice (if it is the primary method of communication with resident or is consistent with E-SIGN). Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content of notice undefined.
Delayed Notice	Notification may be delayed if law enforcement determines that notice will interfere with a criminal investigation.
Government Notice	* Written notification to Alaska Attorney General required only if you do not send notice because you have determined harm threshold is not reached.
Consumer Reporting Agency Notice	If more than 1,000 residents notified, must notify all nationwide Consumer Reporting Agencies without unreasonable delay of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	The above-described Consumer Reporting Agency Notice does not apply to an information collector subject to the Gramm-Leach-Bliley Financial Services Modernization Act (GLBA).
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach. Must cooperate by sharing relevant information about breach, except for confidential business info or trade secrets.
Private Right of Action	In Alaska, a violation of the data breach notification statute by a non-governmental agency is a violation of the Alaska Unfair Trade Practices and Consumer Protection Act.

Potential Penalties	An individual who suffers a loss resulting from a violation of the statute may recover actual: Economic damages not to exceed $500; Costs and attorneys' fees.

Last revised on June 15, 2023

ARIZONA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Ariz. Rev. Stat. Ann. § 18-55 1 to 552

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	No later than 45 days	Yes, if > 1,000 residents notified

Scope of This Summary:
Notification requirements applicable to persons or entities that conduct business in the state and own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	N/A
Breach Defined	Unauthorized acquisition and access that materially compromises the security or confidentiality of covered information maintained as part of a database of personal information regarding multiple individuals, and that causes or is reasonably likely to cause substantial economic loss to a resident, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, redacted, or secured by any other means rendering the element unreadable or unusable.
Form of Covered Information	Electronic Only
Covered Information	• Personal information means an individual's first name or first initial and last name in combination with one or more of the following specified data elements: ○ Social Security number. ○ The number on a driver's license issued pursuant to § 28-3166 or number on a non-operating identification license issued pursuant to § 28-3165. ○ A private key that is unique to an individual and that is used to authenticate or sign an electronic record. ○ A financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual's financial account. ○ A health insurance identification number. ○ Information about an individual's medical or mental health treatment or diagnosis by a healthcare professional. ○ Passport number. ○ Taxpayer identification number or an identity protection personal identification number issued by the United States Internal Revenue Service. ○ Unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account. • Personal information also means: ○ An individual's username or email address in combination with a password or security question and answer that allows access to an online account. ○ Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.
Consumer Notice Timing	Notice required within 45 days of determination that a breach has occurred.
Consumer Notice Method	By written notice; email notice if the person has email addresses for the individuals who are subject to the notice; or telephonic notice, if telephonic contact is made directly with the affected individuals and is not through a prerecorded message. Substitute notice is available if certain criteria are satisfied.

Consumer Notice Content	• Notifications to affected individuals must include at least:
	  ○ The approximate date of the breach.
	  ○ A brief description of the personal information included in the breach.
	  ○ The toll-free numbers and addresses for the three largest nationwide Consumer Reporting Agencies.
	  ○ The toll-free number, address, and website address for the Federal Trade Commission or any federal agency that assists consumers with identity theft matters.
	• For a breach of only an individual's username or email address in combination with a password or security question and answer that allows access to an online account, an entity may comply with notification requirements by:
	  ○ Providing the notification in an electronic form that directs the affected individual to promptly change their password and security question or answer as applicable, or to take other steps that are appropriate to protect the online account with the entity and all other online accounts for which the individual uses the same username and email address and password or security question or answer.

Delayed Notice	Notification may be delayed if law enforcement advises that notice will impede a criminal investigation. Notice must be made no later than 45 days after law enforcement informs the covered entity that delay is no longer required.
Government Notice	If notice to more than 1,000 residents is required, the entity shall notify the Attorney General.
Consumer Reporting Agency Notice	If notice to more than 1,000 residents is required, the entity shall notify the three largest nationwide Consumer Reporting Agencies within 45 days.
Exceptions for Other Laws	The statute exempts from compliance the following entities: Any person who is subject to the federal Gramm-Leach-Bliley Act (GLBA); Any person who is subject to the federal Health Insurance Portability and Accountability Act (HIPAA).
Third-Party Notice	If you maintain unencrypted computerized data that includes covered information on behalf of another entity, you must notify it without unreasonable delay following discovery of a breach. Must cooperate by sharing relevant information about breach.
Private Right of Action	The Arizona statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

ARKANSAS

Data Breach Notification Summary

Davis Wright Tremaine LLP

Arkansas Code §§ 4-110-101 —4-110-108

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expedient manner possible without unreasonable delay	Yes – AG notice triggered if more than 1,000 residents notified.

Scope of This Summary:

Notification requirements applicable to persons and businesses that acquire, own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if, after a reasonable investigation, covered entity determines that there is no reasonable likelihood of harm to consumers.
Breach Defined	Unauthorized acquisition of computerized data which, as a result, compromises the security, confidentiality, or integrity of personal information maintained by the covered entity, with the exception of certain good-faith acquisitions.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted.
Form of Covered Info	Electronic Only

Covered Info	• An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements:
	• Social Security number.
	• Driver's license number or Arkansas identification card number.
	• Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
	• Medical information, meaning any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a healthcare professional.
	• Biometric data, meaning data generated by automatic measurements of an individual's biological characteristics, including without limitation:
	  ○ Fingerprints.
	  ○ Faceprint.
	  ○ A retinal or iris scan.
	  ○ Hand geometry.
	  ○ Voice print analysis.
	  ○ Deoxyribonucleic acid (DNA).
	  ○ Any other unique biological characteristics of an individual if the characteristics are used by the owner or licensee to uniquely authenticate the individual's identity when the individual accesses a system or account.

Consumer Notice Timing	Without unreasonable delay and in the most expedient manner possible.
Consumer Notice Method	By written notice or electronic notice if it is consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content of notice undefined.
Delayed Notice	Notification may be delayed if law enforcement determines that notice will impede a criminal investigation.
Government Notice	Must notify the Attorney General if more than 1,000 residents must be notified. Notice must be at the same time as notice to affected residents or within 45 days of determining there is a reasonable likelihood of harm to residents, whichever is first.

Consumer Reporting Agency Notice	N/A
Exceptions for Other Laws	The statute exempts entities subject to Arkansas or federal regulations or rules more protective of personal information, with breach disclosure requirements at least as thorough as the Arkansas requirements.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	The Arkansas general breach notification statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil or criminal penalties. Specifically, covered entities that "knowingly" and "willfully" commit an unlawful practice under this law shall be guilty of a Class A misdemeanor.

Last revised on June 15, 2023

CALIFORNIA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Cal. Civ. Code §§ 1798.82 & 1798.150 (as amended, 2019)

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	Most expedient time possible and without unreasonable delay	Yes, if > 500 residents notified

Scope of This Summary:

Notification requirements applicable to persons or businesses that conduct business in the state and that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	N/A
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, so long as the encryption key was not or is not reasonably believed to have been acquired.
Form of Covered Info	Electronic only.

Covered Info	• An individual's first name or first initial and last name in combination with any one or more of the following data elements:
	  ○ Social Security number.
	  ○ Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
	  ○ Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
	  ○ Medical information, meaning any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional.
	  ○ Health insurance information, meaning an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
	  ○ Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Does not include a physical or digital photograph, unless used or stored for facial recognition purposes.
	  ○ Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.
	  ○ Genetic data, meaning any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.
	
	• Additionally: A username or email address, in combination with a password or security question and answer that would permit access to an online account.

Consumer Notice Timing	Must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

Consumer Notice Method	By written notice, or electronic notice if it is consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied. Alternative methods apply to breaches solely involving usernames or email addresses.
Consumer Notice Content	Notice must be in "plain language," use at least 10-point font, and organized by clearly and conspicuously displayed title ("Notice of Data Breach") and headings ("What Happened", "What Information Was Involved", "What We Are Doing", "What You Can Do", and "For More Information"). Notice must include: name and contact information of covered entity; types of covered info that were or reasonably believed to have been the subject of the breach; the date, estimated date, or date range of the breach; date of the notice; whether notice was delayed due to law enforcement; general description of the breach; and toll-free numbers and addresses of the major Consumer Reporting Agencies if Social Security, driver's license, or state identification card numbers were exposed. If Social Security, driver's license, or state identification card numbers are affected, and if the entity providing notice was the source of the breach, must offer appropriate identity theft prevention and mitigation services, if any, at no cost to resident for not less than 12 months.
Delayed Notice	Notification may be delayed if law enforcement determines that notice will impede a criminal investigation.
Government Notice	If more than 500 state residents are notified as result of a single breach, must also electronically submit a sample copy of the notification to the California Attorney General (excluding personal information).
Consumer Reporting Agency Notice	N/A
Exceptions for Other Laws	The statute deems entities covered by the Health Insurance Portability and Accountability Act (HIPAA) in compliance with the content requirements for individual notices if it has complied with the notice content requirements in the Health Information Technology for Economic and Clinical Health (HITECH) Act (42 U.S.C. 17932).
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	In California, any customer injured by a violation of the general breach notification statute may bring a civil action to recover damages, and any business that violates or proposes to violate the statute may be enjoined.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

COLORADO

Data Breach Notification Summary

Davis Wright Tremaine LLP

Colo. Rev. Stat. § 6-1-716

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	No later than 30 days	Yes, if 500+ residents notified

Scope of This Summary:

Notification requirements applicable to individuals or commercial entities that conduct business in state and own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if, after prompt investigation, the covered entity determines that misuse of resident's covered info has not occurred and is not reasonably likely to occur.
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, redacted, or secured by any other means rendering the name or element unreadable or unusable, so long as the encryption key is not reasonably believed to have also been acquired.
Form of Covered Info	Electronic Only

Covered Info	• First name or first initial and last name in combination with any one or more of the following data elements:
	  ○ Social Security number.
	  ○ Student, military, or passport identification number.
	  ○ Driver's license number or identification card number.
	  ○ Medical information, meaning any information about a consumer's medical or mental health treatment or diagnosis by a healthcare professional.
	  ○ Health insurance identification number.
	  ○ Biometric data, meaning unique biometric data generated from measurements or analysis of human body characteristics for the purposes of authenticating the individual when he or she accesses an online account.
	
	• Personal information also means a Colorado resident's:
	  ○ Username or email address in combination with a password or security question and answer that would permit access to an online account; or
	  ○ Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

Consumer Notice Timing	Must be made no later than 30 days after the date of determination that the breach occurred, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
Consumer Notice Method	By written notice, telephonic notice, or electronic notice (if it is the primary method of communication with the resident or is consistent with E-SIGN). Substitute notice is available if certain criteria are satisfied.

Consumer Notice Content	• Notice must include, but need not be limited to, the following information:
	  ○ The date, estimated date, or estimated date range of the security breach.
	  ○ A description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach.
	  ○ Information that the resident can use to contact the covered entity to inquire about the security breach.
	  ○ The toll-free numbers, addresses, and websites for Consumer Reporting Agencies.
	  ○ The toll-free number, address, and website for the Federal Trade Commission.
	  ○ A statement that the resident can obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

	• If an investigation determines that a resident's online account credentials (username or email address in combination with a password or security question and answer that would permit access to an online account) have been misused or are reasonably likely to be misused, then the covered entity shall additionally direct the person whose personal information has been breached to promptly: ○ Change their password and security question and answer, as applicable, or ○ Take other steps appropriate to protect the online account with the covered entity and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question or answer.
Delayed Notice	Notification may be delayed if law enforcement determines that notice will impede a criminal investigation, and law enforcement notifies the covered entity not to send notice. Notice must be made no later than 30 days after law enforcement informs the covered entity that delay is no longer required.
Government Notice	If covered entity reasonably believes that breach affected 500 or more residents, must also notify the Attorney General no later than 30 days after determination that breach occurred.
Consumer Reporting Agency Notice	If more than 1,000 residents notified, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of anticipated date of notice and approximate number of residents to be notified.
Exceptions for Other Laws	A covered entity is deemed in compliance with the statute if it maintains and complies with breach notification procedures established by the covered entity's state or federal regulator pursuant to applicable federal or state law, if the procedures are consistent with the timing requirements of the statute. *Covered entities deemed in compliance must notify the attorney general if a breach occurs.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it in the most expedient time possible and without unreasonable delay following discovery of a breach, if misuse of the covered info about a resident has occurred or is reasonably likely to occur. Must cooperate by sharing relevant information about breach but not disclosure of confidential business info or trade secrets.
Private Right of Action	The Colorado general breach notification statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

CONNECTICUT

Data Breach Notification Summary

Davis Wright Tremaine LLP

Conn. Gen. Stat. § 36a-701b

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	No later than 60 days	Yes

Scope of This Summary:

Notification requirements applicable to any persons who conduct business in the state and own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if, after appropriate investigation and consultation with relevant federal, state, and local law enforcement, the covered entity reasonably determines the breach will not likely result in harm to affected residents.
Breach Defined	Unauthorized access to or acquisition of covered info.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or secured by other methods that render them unreadable or unusable.
Form of Covered Information	Electronic Only
Covered Information	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Taxpayer identification number. ○ Identity protection personal identification number issued by the United States Internal Revenue Service. ○ Driver's license number, state identification card number, passport number, military identification number or other identification number issued by the government that is commonly used to verify identity. ○ Credit or debit card number. ○ Financial account number in combination with any required security code, access code or password that would permit access to such financial account. ○ Medical information, meaning any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional. ○ Health insurance information, meaning an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual. ○ Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina or iris image. ○ Username or email address in combination with a password or security question and answer that would permit access to an online account. ○ Precise geolocation data (effective Oct. 1, 2023).
Consumer Notice Timing	Must be made without unreasonable delay but no later than 60 days after the discovery of the breach, unless a shorter time is required under federal law, subject to completion of an investigation to determine the nature and scope of the incident, to identify those affected, or to restore the reasonable integrity of the system.
Consumer Notice Method	By written notice, telephone notice, or electronic notice if it is consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	If Social Security numbers are breached or reasonably believed to have been breached, must offer appropriate identity theft prevention and, if applicable, mitigation services at no cost to the resident for not less than 24 months, as well as information on how the resident can place a credit freeze.
Delayed Notice	Notification may be delayed if law enforcement determines that notice will impede a criminal investigation and law enforcement requests notification be delayed.

Government Notice	Covered entity must also provide notice to the Connecticut Attorney General no later than the time notice is provided to the resident.
Consumer Reporting Agency Notice	The Connecticut general breach notification and insurance data security statutes do not require notification to credit reporting agencies.
Exceptions for Other Laws	A covered entity will be deemed compliant with the statute if, in the event of a breach, the covered entity complies with the breach notification requirements of its functional regulator as defined by the Gramm-Leach-Bliley Act at 15 U.S.C. 6809(2) and notifies affected residents of a breach in accordance with those requirements.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of breach.
Private Right of Action	The Connecticut general breach notification statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on November 15, 2023

DELAWARE

Data Breach Notification Summary

Davis Wright Tremaine LLP

6 Del. Code Ann. §§ 12B-101 to -104

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	No later than 60 days	Yes, if >500 residents notified

Scope of This Summary:
Notification requirements applicable to any person who conducts business in state and owns, licenses, or maintains covered info. Some types of businesses may be exempt from some or all of these requirements.

Risk of Harm Threshold	Notification not required if, after an appropriate investigation, the covered entity reasonably determines that breach is unlikely to result in harm to affected individuals.
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted so long as encryption key is not reasonably believed to also have been acquired.
Form of Covered Info	Electronic Only
Covered Information	A Delaware resident's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or state or federal identification card number. ○ Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account. ○ Passport number. ○ A username or email address, in combination with a password or security question and answer that would permit access to an online account. ○ Medical history, mental or physical condition, medical treatment or diagnosis by a healthcare professional, or deoxyribonucleic acid profile. ○ Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person. ○ Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes. ○ An individual taxpayer identification number.
Consumer Notice Timing	Must be made without unreasonable delay but no later than 60 days after determination that breach occurred.
Consumer Notice Method	By written notice, telephonic notice, or electronic notice if it is the primary method of communication with resident or is consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied. Other notice methods may be available if only email account login credentials are compromised in breach.
Consumer Notice Content	If a resident's Social Security number was compromised, covered entity must offer one year of credit monitoring services to the resident free of cost and must also provide all information necessary to enroll in such services and information on how resident can place a credit freeze.
Delayed Notice	Notification may be delayed if (1) law enforcement determines that notice will impede a criminal investigation and has made a request for delay to covered entity, or (2) covered entity cannot, through reasonable diligence, identify within 60 days that covered info of certain residents was affected in the breach (must notify those residents as soon as practicable after determining their info was affected, unless substitute notice was made).
Government Notice	If over 500 residents are to be notified, must also notify Attorney General no later than the time resident notice is provided.

Consumer Reporting Agency Notice	The Delaware general breach notification statute does not require notice to Consumer Reporting Agencies.
Exceptions for Other Laws	A covered entity will be deemed in compliance with the statute if it is regulated by state or federal law, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act (GLBA), and complies with the breach notification requirements of its functional regulators.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following determination of a breach. Must cooperate by sharing relevant information about breach.
Private Right of Action	The Delaware general breach notification statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

DISTRICT OF COLUMBIA

Data Breach Notification Summary

Davis Wright Tremaine LLP

D.C. Code §§ 28-3851 to 28-3853

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	Most expedient time possible without unreasonable delay	Yes, if 50+ residents notified

Scope of this Summary:

Notification requirements applicable to persons or entities that conduct business in DC and that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	N/A
Breach Defined	Unauthorized acquisition of electronic data or any equipment or device storing such data that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that has been rendered secure so as to be unusable to an unauthorized third party.
Form of Covered Info	Electronic Only
Covered Information	• An individual's first name or first initial and last name, or any other personal identifier, which, in combination with any of the following data elements, can be used to identify a person or the person's information: ○ Social security number, Individual Taxpayer Identification Number, passport number, driver's license number, District of Columbia identification card number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. ○ Account number, credit card number or debit card number, or any other number or code or combination of numbers or codes, such as an identification number, security code, access code, or password, that allows access to or use of an individual's financial or credit account. ○ Medical information, meaning any information about a consumer's dental, medical, or mental health treatment or diagnosis by a healthcare professional. ○ Genetic information and deoxyribonucleic acid profile has the meaning ascribed to it under the Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), approved August 21, 1996 (Pub. Law 104-191; I l0 Stat. 1936), as specified in 45 C.F.R. § 160.103. ○ Health insurance information, including a policy number, subscriber information number, or any unique identifier used by a health insurer to identify the person that permits access to an individual's health and billing information. ○ Biometric data of an individual generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that's used to uniquely authenticate the individual's identity when the individual accesses a system or account. ○ Any combination of data elements included in the bulleted list that would enable a person to commit identity theft without reference to a person's first name or first initial and last name or other independent personal identifier. • A username or email address in combination with a password, security question and answer, or other means of authentication, or with any combination of data elements included in the bulleted list above that permits access to an individual's email account.
Consumer Notice Timing	Must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

Consumer Notice Method	By written notice or by electronic notice if customer consented to receipt of electronic notice consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.

Consumer Notice Content	• Notice to affected individuals shall include the following:
	  ○ To the extent possible, a description of the categories of information, including the elements of personal information, that were or are reasonably believed to have been acquired.
	  ○ Contact information for the person or entity making the notification, including the business address, telephone number, and toll-free telephone number if one is maintained.
	  ○ The toll-free telephone numbers and addresses for the major Consumer Reporting Agencies, including a statement notifying the resident of the right to obtain a security freeze free of charge and information how a resident may request a security freeze.
	  ○ The toll-free telephone numbers, addresses, and websites for the following entities, including a statement that an individual can obtain information from these sources about steps to take to avoid identity theft: The Federal Trade Commission, The Office of the Attorney General for the District of Columbia.
	
	• In the event that the breach of information solely involved a username or email address in combination with a password, as defined in the above section regarding personal information, the person or entity may provide the notification in electronic format or other form that directs the person to change the person's password and security question or answer, or to take other steps appropriate to protect the email account with the person or entity and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question or answer.

Delayed Notice	Notification may be delayed if law enforcement determines that notice will impede a criminal investigation.
Government Notice	Notification to the AG must be made if the breach affects 50 or more residents and no later than when notice was sent to the individuals.
Consumer Reporting Agency Notice	If more than 1,000 residents notified, must notify all nationwide Consumer Reporting Agencies without unreasonable delay of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	A covered entity is deemed in compliance with the statute if it maintains procedures for breach notification and provides notice in accordance with: The Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Health Information Technology for Economic and Clinical Health (HITECH) Act.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it in the most expedient time possible following discovery of a breach.
Private Right of Action	A violation of the District of Columbia statute is considered an unfair or deceptive trade practice under D.C. Code § 28-3904(kk) and any consumer may bring an action seeking relief from the use of a trade practice in violation of this statute.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

FLORIDA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Fla. Stat. § 501.171

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	No later than 30 days	Yes, if 500+ residents notified

Scope of this Summary:
Notification requirements applicable to commercial entities that acquire, maintain, store, or use covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if, after investigation and consultation with relevant federal, state, or local law enforcement, covered entity reasonably determines breach has not and will not likely result in identity theft or other financial harm. Determination must be documented in writing, maintained for five years, and provided to Dept. of Legal Affairs within 30 days of determination.
Breach Defined	Unauthorized access to covered info, excluding certain good-faith access by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, secured, or modified to remove identifying elements or otherwise render it unusable.
Triggering Event	The Florida statute's notification obligations are triggered by a "breach of security," defined as an unauthorized access to electronic data containing personal information.
Form of Covered Info	Electronic Only

Covered Info	• An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:
	  ○ Social Security number.
	  ○ Driver's license number or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity.
	  ○ Financial account number, credit card number, or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account.
	  ○ Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by healthcare professional.
	  ○ An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
	• Personal information also includes a username or email address in combination with a password or security question and answer that would permit access to an online account.

Consumer Notice Timing	Must be made as expeditiously as practicable and without unreasonable delay but no later than 30 days after determination of breach or reason to believe breach occurred, consistent with time necessary to determine scope of the breach, identify those affected, and restore the reasonable integrity of the system. May receive 15 more days if good cause for delay provided to Dept. of Legal Affairs within original 30 days.
Consumer Notice Method	By written notice or email. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Notice must include the date(s), estimated date, or estimated date range of the breach of security; a description of the covered info that was or is reasonably believed to have been accessed; and the covered entity's contact info for inquiries.
Delayed Notice	Notification may be delayed for a specified period upon written request by law enforcement if law enforcement determines that notice will impede a criminal investigation. A covered entity can also receive an extra 15 days to provide notice to consumers if good cause for delay is provided in writing to the Dept. of Legal Affairs within 30 days of the breach.

Government Notice	If breach affects 500 or more residents, must notify the AG as expeditiously as practicable, but no later than 30 days after determination of breach or reason to believe breach occurred. Notice must include: synopsis of events surrounding breach; number of residents affected/potentially affected; info on services offered to affected individuals free of charge; copy of the notice to residents; and contact info for covered entity. Must provide additional info upon request by Dept.
Consumer Reporting Agency Notice	The Florida statute requires a covered entity to notify the major consumer reporting agencies if it must notify more than 1,000 individuals at one time. The notice to the consumer reporting agencies must include information regarding the timing, distribution, and content of the notice sent to individuals.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it as expeditiously as practicable but no later than 10 days following determination of a breach or reason to believe breach occurred. Must provide all info other entity needs to comply with its notice requirements.
Exceptions for Other Laws	A covered entity that notifies affected individuals of a breach according to the rules, regulations, procedures, or guidelines established by its primary or functional federal regulator is deemed in compliance with this statute's individual notification requirements. The covered entity is deemed in compliance with the law's requirement to notify the Florida Department of Legal Affairs if it timely provides the Department with a copy of the notice sent to individuals.
Consumer Reporting Agency Notice	If more than 1,000 residents notified, must, without reasonable delay, notify all nationwide Consumer Reporting Agencies of timing, distribution, and content of the consumer notice.
Private Right of Action	The Florida statute does not provide a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

GEORGIA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Ga. Code Ann. §§ 10-1-910 to -912

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	Most expedient time possible and without unreasonable delay	No

Scope of this Summary:
Notification requirements applicable to "data collectors" (meaning certain state or local governmental agencies), "information brokers" (meaning persons or commercial entities who engage in whole or in part in the business of collecting, evaluating, transmitting, or otherwise communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties), and persons maintaining covered info on their behalf.

Risk of Harm Threshold	N/A
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith access by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted.
Form of Covered Info	Electronic Only
Covered Information	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or state identification card number. ○ Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords. ○ Account passwords or personal identification numbers or other access codes. ○ Any of the data elements listed above when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.
Consumer Notice Timing	Must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the system.
Consumer Notice Method	By written notice, telephonic notice, or electronic notice if it is consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content of notice undefined.
Delayed Notice	Notification may be delayed if law enforcement determines that notice will compromise a criminal investigation.
Government Notice	The Georgia general breach notification statute does not require notice to any governmental or regulatory agencies.
Consumer Reporting Agency Notice	If more than 10,000 residents notified, must notify all nationwide Consumer Reporting Agencies without unreasonable delay of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	None
Third-Party Notice	If you maintain covered info on behalf of an information broker or data collector, you must notify them within 24 hours following discovery of a breach if the covered information was or is reasonably believed to have been accessed without authorization.

Private Right of Action	The Georgia general breach notification statute does not provide for a private right of action.
Potential Penalties	The Georgia general breach notification statute does not provide for regulatory enforcement.

Last revised on June 15, 2023

GUAM

Data Breach Notification Summary

Davis Wright Tremaine LLP

9 Guam Code Ann. §§ 48.10-.80

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Without unreasonable delay	No

Scope of this Summary:

Notification requirements applicable to persons and entities that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if acquisition of covered info does not cause, or covered entity does not reasonably believe has caused or will cause, identity theft or other fraud to a Guam resident.
Breach Defined	Unauthorized access and acquisition that compromises the security or confidentiality of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted.
Form of Covered Info	Electronic Only
Covered Info	The first name or first initial and last name in combination with and linked to any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or Guam identification card number issued in lieu of a driver's license. ○ Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.
Consumer Notice Timing	Must be without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system.
Consumer Notice Method	By written notice to postal address in covered entity's records, telephone notice, or electronic notice. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content of notice undefined.
Delayed Notice	Notification may be delayed if law enforcement determines and advises that notification will impede a criminal or civil investigation, or homeland or national security.
Government Notice	N/A
Exceptions for Other Laws	An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional federal regulator shall be in compliance.
Consumer Reporting Agency Notice	N/A
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it as soon as practicable following discovery of a breach.
Private Right of Action	The Guam statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

HAWAII

Data Breach Notification Summary

Davis Wright Tremaine LLP

Haw. Rev. Stat. §§ 487N-1- 487N-3

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Without unreasonable delay	Yes, if >1,000 individuals notified

Scope of this Summary:

Notification requirements applicable to commercial entities that own, license, or maintain covered info of state residents, or conduct business in the state and own or license covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if illegal use of covered info has not occurred nor is reasonably likely to occur, and incident does not create a risk of harm to the person.
Breach Defined	Unauthorized access to and acquisition of covered info where illegal use of the personal information has occurred or is reasonably likely to occur and creates risk of harm to the person, excluding certain good-faith access by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is redacted or encrypted so long as the encryption key was not accessed or acquired.
Form of Covered Info	Electronic or Paper
Covered Info	An individual's first name or first initial and last name in combination with any one or more of the following data elements: o Social Security number. o Driver's license number or Hawaii identification card number. o Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.
Consumer Notice Timing	Must be made without unreasonable delay, consistent with any measures to determine contact info, the scope of the breach, and to restore the reasonable integrity, security, and confidentiality of the system.
Consumer Notice Method	By written notice to last known address; by telephonic notice if direct contact is made; or by email if individual has consented to receive electronic communications and notice is consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The notice shall be clear and conspicuous and include a description of the following: o The incident in general terms. o The type of personal information that was subject to the unauthorized access and acquisition. o The general acts of the business or government agency to protect the personal information from further unauthorized access. o A telephone number that the person may call for further information and assistance, if one exists. o Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.
Delayed Notice	Notification may be delayed if law enforcement informs covered entity that notice may impede a criminal investigation or jeopardize national security and requests delay. Request must be in writing or documented contemporaneously in writing by covered entity.
Government Notice	If more than 1,000 individuals notified, must, without unreasonable delay, notify, in writing, the Hawaii Office of Consumer Protection of timing, distribution, and content of the consumer notice.
Consumer Reporting Agency Notice	If more than 1,000 individuals notified, must, without unreasonable delay, notify, in writing, all nationwide Consumer Reporting Agencies of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	A covered entity is deemed in compliance with the Hawaii statute if it is subject to either: The Health Insurance Portability and Accountability Act (HIPAA) and in compliance with HIPAA's standards for privacy or individually identifiable health information and the security standards for the protection of electronic health information;

	The federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (70 Fed. Reg. 15,736-01 (March 29, 2005)) or the National Credit Union Administration security program regulations.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	The Hawaii general breach notification statute provides for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

IDAHO

Data Breach Notification Summary

Davis Wright Tremaine LLP

Idaho Code Ann. §§ 28-51-104 to 107

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expedient time possible without unreasonable delay	No*

Scope of this Summary:

Notification requirements applicable to individuals or commercial entities that conduct business in the state and own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if, after reasonable and prompt investigation, the covered entity determines that misuse of a resident's covered info has not occurred or is not reasonably likely to occur.
Breach Defined	Illegal acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted.
Form of Covered Info	Electronic Only
Covered Info	An Idaho resident's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or Idaho identification card number. ○ Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.
Consumer Notice Timing	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, identify the residents affected, and restore the reasonable integrity of the system.
Consumer Notice Method	By written notice, telephonic notice, or electronic notice if it is consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content of notice undefined.
Delayed Notice	Notification may be delayed if law enforcement determines that notification will impede a criminal investigation.
Government Notice	N/A* – Public agencies have a duty to notify the AG.
Consumer Reporting Agency Notice	N/A
Exceptions for Other Laws	An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with section 28-51-105, Idaho Code, if the individual or the commercial entity complies with the maintained procedures when a breach of the security of the system occurs.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach if misuse of covered info has occurred or is reasonably likely to occur. Must cooperate by sharing relevant information about breach.
Private Right of Action	The Idaho statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

ILLINOIS

Data Breach Notification Summary

Davis Wright Tremaine LLP

815 Ill. Comp. Stat. §§ 530/1 to 530/50

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	Most expedient time possible without unreasonable delay	Yes, if >500 residents notified

Scope of this Summary:

Notification requirements applicable to commercial entities that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	N/A
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted, so long as encryption key was not acquired.
Form of Covered Info	Electronic Only

Covered Info	• An individual's first name or first initial and last name in combination with any one or more of the following data elements:
	  ○ Social Security number.
	  ○ Driver's license number or state identification card number.
	  ○ Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
	  ○ Medical information, meaning information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to a website or mobile application.
	  ○ Health insurance information, meaning an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history, including any appeals records.
	  ○ Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.
	• A username or email address, in combination with a password or security question and answer that would permit access to an online account.

Consumer Notice Timing	Must be made in the most expedient time possible and without unreasonable delay following discovery or notification of the breach, consistent with any measures to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the system.
Consumer Notice Method	By written notice or electronic notice if it is consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.

Consumer Notice Content	The notice shall include, but need not be limited to, information as follows:
	• With respect to personal information as defined in paragraph 1 of the "Personal information definition":
	  ○ The toll-free numbers and addresses for Consumer Reporting Agencies.
	  ○ The toll-free number, address, and website address for the Federal Trade Commission.
	  ○ A statement that the individual can obtain information from these sources about fraud alerts and security freezes.
	  ○ The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

	• With respect to personal information as defined in paragraph 2 of the "Personal information" definition: ○ Notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her username or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same username or email address and password or security question and answer.
Delayed Notice	Notification may be delayed if law enforcement determines notification will impede a criminal investigation and provides a written request for the delay.
Government Notice	If more than 500 Illinois residents are notified, must notify Director of the Attorney General no later than when residents are notified. Notice must include a description of the breach, number of residents affected, and steps taken in response. AG may publish name of company that suffered the breach, the types of personal information compromised, and the date range of the breach.
Consumer Reporting Agency Notice	N/A
Exceptions for Other Laws	Covered entities or business associates subject to and in compliance with Health Information Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) privacy and security standards shall be deemed in compliance with the statute if they provide the Attorney General with a copy of any breach notifications reported to the Secretary of Health and Human Services within five days of notifying the Secretary.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach and must cooperate in matters relating to the breach as specified in the statute.
Private Right of Action	A violation of the Illinois general data breach notification statute is an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act. Any person who suffers actual damages may bring an action under the statute.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

INDIANA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Ind. Code §§ 24-4.9-1 to 24-4.9-5

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	No later than 45 days	Yes

Scope of this Summary:

Notification requirements applicable to any persons that own or license covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if the breach has not resulted in and could not result in identity deception, identity theft, or fraud.
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted so long as encryption key was not accessed or acquired.
Form of Covered Info	Electronic or tangible medium (paper, microfilm, etc.) if transferred from computerized data.

Covered Info	• A Social Security number
	• An individual's first and last names, or first initial and last name, and one or more of the following data elements:
	  ○ A driver's license number.
	  ○ A state identification card number.
	  ○ A credit card number.
	  ○ A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

Consumer Notice Timing	Must be made without unreasonable delay but not more than 45 days after the discovery of the breach, consistent with measures necessary to restore the integrity of the system or necessary to discover the scope of the breach.
Consumer Notice Method	By mail, telephone, fax, or email. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content of notice undefined.
Delayed Notice	Notification may be delayed if law enforcement or the Attorney General requests delay because disclosure will impede a criminal or civil investigation or jeopardize national security.
Government Notice	If notice provided to one or more residents, must also notify the Indiana Attorney General within 45 days.
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must notify all Consumer Reporting Agencies with information necessary to assist the CRA to prevent fraud, including the types of covered info affected by the breach.

Exceptions for Other Laws	The statute exempts database owners that maintain data security procedures as part of an information security policy as stringent as the statute's disclosure requirements or in compliance with the following federal laws:
	  ○ The USA PATRIOT Act.
	  ○ Executive Order 13224 (66 Fed. Reg. 49,079 (Sept. 23, 2001)).
	  ○ The Driver's Privacy Protection Act (18 U.S.C. § 2721).
	  ○ The Fair Credit Reporting Act (FCRA).
	  ○ The Gramm-Leach-Bliley Act (GLBA).
	  ○ The Health Insurance Portability and Accountability Act (HIPAA).

Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it following discovery of a breach.

Private Right of Action	The Indiana general breach notification statute is silent on an individual's private right of action for violations.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

IOWA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Iowa Code §§ 715C.1-2

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expeditious manner possible and without unreasonable delay	Yes, if >500 residents notified

Scope of this Summary:

Notification requirements applicable to persons or business entities that own or license covered info that is used in the course of a business, vocation, occupation, or volunteer activities. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if after appropriate investigation or consultation with relevant federal, state, or local law enforcement, covered entity determines that there is no reasonable likelihood of financial harm to residents. Such determination must be documented in writing and retained for five years.
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, redacted, or otherwise altered by any method or technology pursuant to accepted industry standards in such a way that it is unreadable so long as the encryption key was not accessed or acquired. Effective July 1, 2023, if an organization has a compliant cybersecurity program, it can assert an affirmative defense against tort claims alleging a data breach resulted from failure to implement reasonable information security controls
Form of Covered Info	Electronic or any medium (paper, microfilm, etc.) if transferred from computerized data.
Covered Info	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or other unique identification number created or collected by a government body. ○ Financial account number, credit card number, or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account. ○ Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account. ○ Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.
Consumer Notice Timing	Must be made in most expeditious manner possible and without unreasonable delay, consistent with any measures necessary to sufficiently determine contact info for affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.
Consumer Notice Method	By written notice or electronic notice (if it is the customary method of communication with the consumer or is consistent with Iowa Code, Chapter 554D and E-SIGN). Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Notice shall include, at a minimum, all of the following: ○ A description of the breach of security. ○ The approximate date of the breach of security. ○ The type of personal information obtained as a result of the breach of security. ○ Contact information for Consumer Reporting Agencies. ○ Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.
Delayed Notice	Notification may be delayed if law enforcement determines that notification will impede a criminal investigation and the agency makes a written request that the notification be delayed.
Government Notice	If more than 500 Iowa residents are notified, must notify Director of the Iowa Attorney General's Consumer Protection Division within 5 business days after notifying residents.

Consumer Reporting Agency Notice	N/A
Exceptions for Other Laws	The statute exempts entities that are subject to and comply with: ○ A state or federal law that provides greater protection to personal information and has disclosure requirements for breach of security or personal information at least as thorough as Iowa's statute. ○ The Gramm-Leach-Bliley Act (GLBA). ○ The Health Information Portability and Accountability Act (HIPAA). ○ The Health Information Technology for Economic and Clinical Health Act.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	The Iowa general breach notification statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

KANSAS

Data Breach Notification Summary

Davis Wright Tremaine LLP

Kan. Stat. Ann. §§ 50-7a

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expeditious manner possible and without unreasonable delay	No

Scope of this Summary:

Notification requirements applicable to persons or businesses that conduct business in the state and own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if, after reasonable and prompt investigation, misuse of covered info has not and is not reasonably likely to occur.
Breach Defined	Unauthorized access and acquisition that compromises the security, confidentiality, or integrity of the covered info that the covered entity reasonably believes has caused or will cause identity theft to a resident, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted or otherwise secured by any method in such a way that it is unreadable or unusable.
Form of Covered Info	Electronic Only
Covered Info	First name or first initial and last name, plus: Social Security number; driver's license or state identification card number; or financial account, credit card, or debit card number, alone or in combination with any required security or access code or password that would permit access to a resident's financial account.
Consumer Notice Timing	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
Consumer Notice Method	By written notice or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content of notice undefined.
Delayed Notice	Notification may be delayed if law enforcement determines that notification will impede a criminal investigation.
Government Notice	N/A
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must, without unreasonable delay, notify all nationwide Consumer Reporting Agencies of timing, distribution, and content of the notices.
Exceptions for Other Laws	An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidance or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section. This section does not relieve an individual or a commercial entity from a duty to comply with other requirements of state and federal law regarding the protection and privacy of personal information.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it following discovery of a breach if covered info was or is reasonably believed to have been accessed and acquired by an unauthorized person.
Private Right of Action	The Kansas statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

KENTUCKY

Data Breach Notification Summary

Davis Wright Tremaine LLP

Ky. Rev. Stat. Ann. § 365.732

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expeditious manner possible and without unreasonable delay	No

Scope of this Summary:

Notification requirements applicable to persons or business entities that conduct business in the state. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if the covered entity reasonably believes that the breach has not and will not cause identity theft or fraud against any Kentucky resident.
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info that actually causes or that covered entity reasonably believes has caused or will cause identity theft or fraud against a resident, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted.
Form of Covered Info	Electronic Only
Covered Info	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number. ○ Account number, credit or debit card number, in combination with any required security code, access code, or password permit access to an individual's financial account.
Consumer Notice Timing	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
Consumer Notice Method	By written notice or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content of notice undefined.
Delayed Notice	Notification may be delayed if law enforcement determines that notification will impede a criminal investigation.
Government Notice	N/A
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must, without unreasonable delay, notify all nationwide Consumer Reporting Agencies and credit bureaus of timing, distribution, and content of the notices.
Third-Party Notice	If you conduct business in Kentucky and maintain covered info on behalf of another entity, you must notify it as soon as reasonably practicable after discovery of a breach if the covered info was or is reasonably believed to have been acquired by an unauthorized person.
Exceptions for Other Laws	The statute does not apply to information holders subject to either: the Health Insurance Portability and Accountability Act of 1996 (HIPAA); or the Gramm-Leach-Bliley Act (GLBA).
Private Right of Action	*The Kentucky general data breach notification statute does not provide for a private right of action, but an injured party may recover damages under KRS 446.070.
Potential Penalties	The Kentucky general breach notification statute does not provide for regulatory enforcement.

LOUISIANA

Data Breach Notification Summary

Davis Wright Tremaine LLP

La. Rev. Stat. Ann. §§ 51:3071 to 51:3077

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	No later than 60 days	Yes

Scope of this Summary:

Notification requirements applicable to any person or agency that conducts business in the state or that owns, licenses, or maintains covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if, after reasonable investigation, the covered entity determines that there is no reasonable likelihood of harm to residents. The covered entity must document determination in writing, retain the documentation for five years, and provide a copy to the Attorney General upon request.
Breach Defined	Compromise to the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable likelihood to result in, the unauthorized acquisition of and access to covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted.
Form of Covered Info	Electronic Only
Covered Info	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or state identification card number. ○ Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. ○ Passport number. ○ Biometric data, meaning data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account.
Consumer Notice Timing	Must be made in most expedient time possible and without unreasonable delay but no later than 60 days from discovery of the breach, consistent with any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.
Consumer Notice Method	By written notice or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content of notice undefined.
Delayed Notice	Notification may be delayed if law enforcement determines that notification will impede a criminal investigation or if covered entity requires additional time to determine scope of the breach, prevent further disclosures, and restore the reasonable integrity of the system. Within the original 60-day deadline the covered entity must provide in writing to the Attorney General reasons for delay.
Government Notice	If notice to Louisiana residents is required, the covered entity must also provide written notice to the Consumer Protection Section of the Attorney General's office. Notice must be received within 10 days of distribution of notice to Louisiana residents and must include the names of those affected residents.
Consumer Reporting Agency Notice	N/A
Exceptions for Other Laws	Financial institutions that must comply with the Gramm-Leach-Bliley Act (GLBA) and are in compliance with the federal banking regulators' notification requirements.

Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it following discovery of a breach if the covered info was or is reasonably believed to have been acquired by an unauthorized person.
Private Right of Action	The Louisiana general breach notification statute provides individuals with a private right of action to recover actual damages resulting from a covered entity's failure to disclose a breach of the security system that resulted in the disclosure of the individual's personal information in a timely manner.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

MAINE

Data Breach Notification Summary

Davis Wright Tremaine LLP

10 Me. Rev. Stat. §§ 1346-1349

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes*	As expeditiously as possible and without unreasonable delay	Yes

Scope of this Summary:

Notification requirements applicable to individuals, entities, and "information brokers" (as defined) that maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification to residents not required if, after a reasonable and prompt good-faith investigation, the covered entity determines that there is no reasonable possibility that the covered info has been or will be misused. * Harm threshold does not apply to information brokers.
Breach Defined	Unauthorized acquisition, release, or use of computerized data that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted, so long as encryption key was not accessed or acquired.
Form of Covered Info	Electronic Only

Covered Info	• An individual's first name, or first initial, and last name in combination with any one or more of the following data elements:
	  ○ Social Security number.
	  ○ Driver's license number or state identification card number.
	  ○ Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords.
	  ○ Account passwords or personal identification numbers or other access codes.
	• Any of the data elements in the above list when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

Consumer Notice Timing	Must be made as expeditiously as possible and without unreasonable delay, consistent with measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data in the system.
Consumer Notice Method	By written notice or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content of notice undefined.
Delayed Notice	Notification may be delayed by law enforcement if they determine that it will compromise a criminal investigation. Notice must be given within seven business days after they determine that notification will not compromise the investigation.
Government Notice	If notification to residents is required, must also notify the appropriate state regulator (either Dept. of Professional and Financial Regulation or, if not regulated by the Department, the Attorney General).
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must notify all nationwide Consumer Reporting Agencies without unreasonable delay. The notification must include the date of the breach, estimated number of affected individuals, if known, and the date those individuals were or will be notified.

Exceptions for Other Laws	A covered entity who complies with the security breach notification requirements established pursuant to federal or other Maine law is deemed to be in compliance as long as the notification procedures are at least as protective as this statute's notification requirements
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach if covered information was or is reasonably believed to have been acquired by an unauthorized person.
Private Right of Action	The Maine general breach notification statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

MARYLAND

Data Breach Notification Summary

Davis Wright Tremaine LLP

Md. Code Ann., Com. Law §§ 14-3501 - 14-3508

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	As soon as practicable but no longer than 45 days after concluding investigation into the breach	Yes

Scope of this Summary:

Notification requirements applicable to businesses that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and Code of Md. Regulations 10.25.18.07-08 provides additional notification requirements for health information exchanges.

Risk of Harm Threshold	Notification not required if the business reasonably determines that the breach of the security of the system does not create a likelihood that personal information has been or will be misused. Must document determination in writing and maintain for three years.
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of residents' covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, redacted, or otherwise protected by another method that renders the info unreadable or unusable.
Form of Covered Info	Electronic Only

Covered Information	• An individual's first name or first initial and last name in combination with any one or more of the following data elements:
	  ○ A Social Security number, an individual taxpayer identification number, a passport number, or other identification number issued by the federal government;
	  ○ A driver's license number or state identification card number;
	  ○ An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password that permits access to an individual's financial account;
	  ○ Health information, including information about an individual's mental health;
	  ○ A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's medical health information;
	  ○ Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account;
	  ○ Genetic information with respect to an individual.
	• A username or email address in combination with a password or security question and answer that permits access to an individual's email account.

Consumer Notice Timing	Must be made as soon as reasonably practicable but no later than 45 days after the business discovers or is notified of the breach of the security of a system.
Consumer Notice Method	By mail, by email (if resident expressly consented to receive electronic notices or if business is primarily conducted online), or by telephone. Substitute notice is available if certain criteria are satisfied. Electronic notice permitted in the case of a breach involving personal information that permits access to an email account only, but specific content and delivery requirements apply.

Consumer Notice Content	• To the extent possible, the notification shall include:
	  ○ A description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired.
	  ○ Contact information for the business making the notification, including the business' address, telephone number, and toll-free telephone number if one is maintained.
	  ○ The toll-free telephone numbers and addresses for the major Consumer Reporting Agencies.

	○ The toll-free telephone numbers, addresses, and website addresses for: The Federal Trade Commission and the Office of the Attorney General. ○ A statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft. • If a breach involves only a username or email address in combination with a password or security question and answer that permits access to the user's email account (and no other personal information), then an entity may comply with the notification requirements under the general statute by directing the individual to promptly: ○ Change their password and security question or answer, as applicable; or ○ Take other steps appropriate to protect the email account with the entity and all other online accounts for which the individual uses the same username or email and password or security question or answer.
Delayed Notice	Notification may be delayed: (1) if law enforcement determines that notice will impede a criminal investigation or jeopardize national or homeland security; or (2) to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system. Notice to affected individuals that is delayed due to law enforcement must be given within seven days after law enforcement determines notice will not impede investigation or jeopardize security or by the end of the original 45-day period.
Government Notice	If notice is required, must notify the MD Attorney General before providing consumer notice. The notice should include a copy of the notice sent to the consumers and a brief description that includes the nature of the breach, the type of affected personal information, and any steps taken to restore the integrity of the system.
Consumer Reporting Agency Notice	If required to notify 1,000 or more residents, must also notify all nationwide Consumer Reporting Agencies without unreasonable delay of timing, distribution, and content of the consumer notices.
Exceptions for Other Laws	The statute includes certain exceptions for any business that Is subject to and in compliance with: ○ the Gramm-Leach Bliley Act; ○ Section 216 (the ""Disposal Rule"") of the Fair and Accurate Credit Transactions Act (15 U.S.C. § 1681w); ○ The Health Insurance Portability and Accountability Act of 1996 (HIPAA) ○ The Interagency Guidelines Establishing Information Security Standards (66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77,610 (Dec. 28, 2004)) and Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (70 Fed. Reg. 15,736 (March 29, 2005).
Third-Party Notice	If maintaining covered info on behalf of another entity, must notify that entity as soon as practicable but no later than 45 days after discovery or notification of breach. Harm threshold does not apply to third-party notice. Businesses that maintain covered info on behalf of another entity may not charge that entity a fee for providing it information it needs in order to notify consumers.
Private Right of Action	A violation of the Maryland general breach notification statute is an unfair or deceptive trade practice under the Maryland Consumer Protection Act, for which an injured person may bring a private action to recover actual damages
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

MASSACHUSETTS

Data Breach Notification Summary

Davis Wright Tremaine LLP

Mass. Gen. Laws ch. 93H, §§ 1-6

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	As soon as practicable and without unreasonable delay	Yes

Scope of this Summary:

Notification requirements applicable to persons and businesses, that own, license, maintain, or store covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if the breach does not create a substantial risk of identity theft or fraud against a resident.
Breach Defined	Unauthorized acquisition or use of covered info that creates a substantial risk of identity theft or fraud against a resident, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, so long as encryption key was not compromised.
Form of Covered Info	Electronic or Paper
Covered Information	A Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements: Social Security number. ○ Driver's license number or state-issued identification card number. ○ Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.
Consumer Notice Timing	Must be made as soon as practicable and without unreasonable delay when covered entity knows or has reason to know a breach or other unauthorized acquisition or use of covered info has occurred.
Consumer Notice Method	By written notice or electronic notice (if consistent with E-SIGN and Mass. Gen Laws ch 110G). Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The notification shall include but not be limited to: ○ The consumer's right to obtain a police report. ○ How to request a security freeze and the necessary information to be provided when requesting the security freeze. ○ That there shall be no charge for a security freeze. ○ Mitigation services to be provided. ○ The notification shall **not** include the nature of the breach or unauthorized acquisition or use or the number of affected residents.
Delayed Notice	Notification may be delayed if law enforcement determines notice may impede a criminal investigation and notifies the Attorney General in writing. The entity must cooperate with law enforcement, including sharing information relevant to the incident.
Government Notice	Must notify the Attorney General and the Director of the Office of Consumer Affairs and Business Regulation as soon as practicable and without unreasonable delay. Notice must include the nature of the incident, the number of residents affected, and any steps the entity has taken or plans to take relating to the incident.
Consumer Reporting Agency Notice	Covered entity must notify any consumer reporting agency identified by the Director of Consumer Affairs and Business Regulation. The notice to Consumer Reporting Agencies must include the same information required in notices to the attorney general and other governmental or regulatory agencies.
Exceptions for Other Laws	Under the statute, covered entities that maintain and comply with breach response procedures under federal laws, rules, regulations, guidance, or guidelines will be deemed in compliance with the statute if they notify: Massachusetts residents of the breach; the attorney general and Director of the Office of Consumer Affairs and Business Regulation as soon as practicable and without unreasonable delay of the breach; and

	any steps the entity has taken or plans to take relating to the breach under the applicable federal law, rule, regulation, guidance, or guidelines.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it as soon as practicable and without unreasonable delay when you know or have reason to know of a breach or other unauthorized acquisition or use of covered info. Must also cooperate with owner or licensor of the covered info (including specific disclosure obligations).
Private Right of Action	*The Massachusetts statute does not explicitly provide for a private right of action, but individuals may have a private right of action for a Chapter 93H violation by enforcing the statute through Chapter 93A (see *Portier v. NEO Tech. Sols.,* 2019 WL 7946103, at *26-*28 (D. Mass. 2019)).
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

MICHIGAN

Data Breach Notification Summary

Davis Wright Tremaine LLP

Mich. Comp. Laws §§ 445.61, 445.63, 445.72

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Without unreasonable delay	No

Scope of this Summary:

Notification requirements applicable to individuals or entities that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if entity determines that the breach has not and is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more Michigan residents.
Breach Defined	Unauthorized access and acquisition that compromises the security or confidentiality of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted so long as encryption key was not accessed or acquired.
Form of Covered Information	Electronic Only
Covered Info	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or identification card number. ○ Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
Consumer Notice Timing	Must be made without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
Consumer Notice Method	Written notice to the most recent available address the person or business has in its records. Electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures in United States Code, title 15, section 7001. Substitute notice is available if certain criteria are satisfied
Consumer Notice Content	Michigan statute does not specify notice content requirements.
Delayed Notice	Notification may be delayed if law enforcement determines that notification will impede a criminal or civil investigation or jeopardize national or homeland security and if a delay is necessary to determine the scope of the breach and restore the reasonable integrity of the database.
Government Notice	The Michigan breach notification statute does not require notice to any government or regulatory agencies.
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, after notifying those residents the covered entity must notify all major Consumer Reporting Agencies without unreasonable delay of timing and number of resident notices.
Exceptions for Other Laws	Financial institutions that are subject to and in compliance with applicable interagency regulatory guidance provided at 70 Fed. Reg. 15,736 (March 29, 2005) or entities covered by and in compliance with the Health Information Portability and Accountability Act of 1996 (HIPAA)
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it of a breach unless you determine that the breach has not and is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more Michigan residents.

Private Right of Action	Michigan's general breach notification statute does not include a private right of action but explicitly notes that it does not eliminate other remedies available by law (MCL 445.72(15)).
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

MINNESOTA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Minn. Stat. §§ 325E.61, 325E.64

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	Most expedient time possible and without unreasonable delay	No

Scope of this Summary:

Notification requirements applicable to persons or businesses that conduct business in Minnesota and own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	N/A
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or secured by another method of technology that renders it unreadable or unusable, so long as the encryption key is not also acquired.
Form of Covered Information	Electronic Only
Covered Information	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or Minnesota identification card number. ○ Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
Consumer Notice Timing	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, identify those affected, and restore the reasonable integrity of the system.
Consumer Notice Method	By written notice, or electronic notice if the primary method of communication with the resident or if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content Requirements are not specified.
Delayed Notice	Notification may be delayed to a specific date if law enforcement determines notice may impede a criminal investigation.
Government Notice	The Minnesota general data breach notification statute does not require notice to any government or regulatory agency.
Consumer Reporting Agency Notice	If more than 500 residents are notified, entity must notify the major Consumer Reporting Agencies within 48 hours of consumer notice of the timing, distribution, and content of the notices.
Exceptions for Other Laws	The statute includes certain exceptions for covered entities that comply with the Gramm-Leach-Bliley Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA).
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach if covered data was or is reasonably believed to have been acquired by an unauthorized person.
Private Right of Action	The Minnesota general data breach notification statute does provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

MISSISSIPPI

Data Breach Notification Summary

Davis Wright Tremaine LLP

Miss. Code Ann. § 75-24-29

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Without unreasonable delay	No

Scope of this Summary:

Notification requirements applicable to persons who conduct business in Mississippi and who, in the ordinary course of business, own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notice is not required if, after an appropriate investigation, the entity reasonably determines that the breach is not likely to result in harm to the affected individuals
Breach Defined	Unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of Mississippi when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.
Encryption Safe Harbor	Statute does not apply to information that is secured by encryption or any other method or technology that renders the covered info unreadable or unusable.
Form of Covered Information	Electronic Only
Covered Information	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social security number. ○ Driver's license number or state identification card number. ○ An account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.
Consumer Notice Timing	Must be made without unreasonable delay, subject to the completion of an investigation to determine the nature and scope of the breach or to restore the reasonable integrity of the system.
Consumer Notice Method	By written notice, telephone notice, or electronic notice (if that is the primary means of communication with the affected resident or if it is consistent with E-SIGN). Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content requirements are not specified.
Delayed Notice	Notification may be delayed for a reasonable period of time if law enforcement determines that notification will impede a criminal investigation or national security and agency has requested that the notification be delayed.
Government Notice	The Mississippi general breach notification statute does not require notice to any governmental or regulatory agencies
Consumer Reporting Agency Notice	The Mississippi general breach notification statute does not require notice to the credit reporting agencies.
Exceptions for Other Laws	Security breach procedures pursuant to the rules, regulations, procedures, or guidelines established by its primary or functional federal regulator.
Third-Party Notice	If you conduct business in Mississippi and maintain covered info on behalf of another entity, you must notify it as soon as practicable following discovery of a breach if the covered info was or is reasonably believed to have been acquired by an unauthorized person for fraudulent purposes.
Private Right of Action	The Mississippi general data breach notification statute does provide for a private right of action.
Potential Penalties	Violations may result in civil or criminal penalties.

Last revised on June 15, 2023

MISSOURI

Data Breach Notification Summary

Davis Wright Tremaine LLP

Mo. Rev. Stat. § 407.1500

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Without unreasonable delay	Yes, if >1,000 residents notified

Scope of this Summary:

Notification requirements applicable to individuals or entities that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local law enforcement agencies, the covered entity determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. The covered entity must document its determination in writing and maintain it for five years.
Breach Defined	Unauthorized access and acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, redacted, or otherwise altered in such a manner to make it unreadable or unusable.
Form of Covered Info	Electronic Only
Covered Info	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or other unique identification number created or collected by a government body. ○ Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. ○ Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account. ○ Medical information. ○ Health insurance information.
Consumer Notice Timing	Must be made without unreasonable delay, consistent with any measures necessary to determine scope of the breach and sufficient contact information for affected residents and to restore the reasonable integrity, security, and confidentiality of the system.
Consumer Notice Method	In writing, by telephone (if contact made directly with affected resident), or electronic notice (if entity has valid email address, resident agreed to receive communications electronically, and notice is consistent with E-SIGN). Substitute notice available if certain criteria are satisfied.
Consumer Notice Contents	The notification shall at minimum include a description of the following: ○ The incident in general terms. ○ The type of personal information that was obtained as a result of the breach of security. ○ A telephone number that the affected consumer may call for further information and assistance, if one exists. ○ Contact information for Consumer Reporting Agencies. ○ Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.
Delayed Notice	Notification may be delayed if law enforcement determines that notification will impede a criminal investigation or jeopardize national or homeland security. The request must be in writing or documented by the covered entity contemporaneously and include the officer name and agency.
Government Notice	If more than 1,000 residents are notified, must, without unreasonable delay, notify Attorney General's office of timing, distribution, and content of the consumer notice.

Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must, without unreasonable delay, notify all Consumer Reporting Agencies of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	A covered entity is deemed in compliance if it is: a financial institution subject to the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice (70 Fed. Reg. 15,736 (March 29, 2005)); the National Credit Union Administration security program regulations (12 CFR §§ 748.0 to 748.2); or the Gramm-Leach-Bliley Act (GLBA).
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	The Missouri statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

MONTANA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Mont. Code Ann. §§ 30-14-1701 to -1705

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Without unreasonable delay	Yes

Scope of this Summary:

Notification requirements applicable to persons or businesses, excluding insurance companies, that conduct business in Montana and that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if the covered entity reasonably believes that breach has not and will not reasonably cause loss or injury to a Montana resident.
Breach Defined	Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by an entity and causes or is reasonably believed to cause loss or injury to a Montana resident. Good-faith acquisition of personal information by an employee or agent of an entity for the purposes of the entity is not a breach of the security of the data system, provided that the personal information is not used or subject to further unauthorized disclosure.
Encryption Safe Harbor	Statute does not apply to information that is encrypted.
Form of Covered Info	Electronic Only
Covered Information	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number, state identification card number, or tribal identification card number. ○ Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. ○ Medical record information as defined in § 33-19-10 (personal information that relates to an individual's physical or mental condition, medical history, medical claims history, or medical treatment and is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent, or legal guardian). ○ A taxpayer identification number. ○ An identity protection personal identification number issued by the United States Internal Revenue Service.
Consumer Notice Timing	Must be made without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
Consumer Notice Method	By written notice, telephone notice, or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The statute does not contain any content requirements.
Delayed Notice	Notification may be delayed if law enforcement determines notice may impede a criminal investigation.
Government Notice	If notice to residents is required, must simultaneously submit electronic copy of notification to Attorney General along with a statement detailing the date and method of distributing the notice and number of residents notified.
Consumer Reporting Agency Notice	If notice to residents suggests, indicates, or implies that they may obtain a copy of their consumer report from a CRA, entity must coordinate with the CRA as to the timing, content, and distribution of the notice. Coordination may not unreasonably delay notice to affected residents.
Exceptions for Other Laws	None
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.

Private Right of Action	*The Montana statute does not provide for a private right of action. Notably, the US District Court for the Northern District of Georgia found that the general breach notification statute is privately enforceable through the state's unfair trade practices statute (*In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1340, n. 304 (N.D. Ga. 2019)).
Potential Penalties	Violations may result in civil or criminal penalties.

Last revised on June 15, 2023

NEBRASKA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Neb. Rev. Stat. §§ 87-801 to -807

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	As soon as possible and without unreasonable delay	Yes

Scope of this Summary:

Notification requirements applicable to individuals or commercial entities that conduct business in the state and that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	None
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, redacted, or otherwise altered in such a manner to make it unreadable, so long as the encryption key was not accessed or acquired.
Form of Covered Info	Electronic Only

Covered Information	• A Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements:
	  ○ Social Security number.
	  ○ Motor vehicle operator's license number or state identification card number.
	  ○ Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.
	  ○ Unique electronic identification number or routing code, in combination with any required security code, access code, or password.
	  ○ Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation.
	• A username or email address, in combination with a password or security question and answer, that would permit access to an online account.

Consumer Notice Timing	If, after a reasonable and prompt investigation conducted in good faith, covered entity determines that covered info has been or is reasonably likely to be used for an unauthorized purpose, notice to affected resident must be made as soon as possible and without unreasonable delay, consistent with any measures necessary to determine the scope and restore the reasonable integrity of the system.
Consumer Notice Method	By written notice, telephone notice, or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The Nebraska statute does not include content requirements for the notice to affected individuals.
Delayed Notice	Notification may be delayed if law enforcement determines notice may impede a criminal investigation.
Government Notice	If notice to residents is required, must also notify the Attorney General of the breach no later than the time when residents are notified.
Consumer Reporting Agency Notice	The Nebraska statute does not require notification to credit reporting agencies.
Exceptions for Other Laws	None
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify and cooperate with it after becoming aware of a breach if covered info has been or is reasonably likely to be used for an unauthorized purpose. Cooperation includes but is not limited to sharing the information relevant to the breach but does not include sharing proprietary information.

Private Right of Action	The Nebraska general breach notification statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

NEVADA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Nev. Rev. Stat. §§ 603A.010-.100, 603A.220, 603A.900-.920

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	Most expedient time possible and without unreasonable delay	No

Scope of this Summary:

Notification requirements applicable to businesses that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	The notification obligation is not subject to a risk assessment.
Breach Defined	Unauthorized acquisition that materially compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted.
Form of Covered Info	Electronic Only
Covered Information	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social security number. ○ Driver's license number, driver authorization card number or identification card number. ○ Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account. ○ A medical identification number or a health insurance identification number. ○ A username, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.
Consumer Notice Timing	Must be made in the most expedient time possible and without unreasonable delay, consistent with any measures to determine the scope of the breach and restore the reasonable integrity of the system.
Consumer Notice Method	By written notice or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The Nevada statute does not include any content requirements.
Delayed Notice	Notification may be delayed if law enforcement determines notice may impede a criminal investigation.
Government Notice	The Nevada statute does not require notification of any government or regulatory agency.
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must, without unreasonable delay, notify all nationwide Consumer Reporting Agencies of timing and content of the consumer notice.
Exceptions for Other Laws	The statute includes exceptions for entities subject to and in compliance with the Gramm-Leach-Bliley Act (GLBA).
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	The Nevada statute does not provide a private right of action for violations.
Potential Penalties	Violations may result in civil penalties. Willful violation can result in criminal penalties.

Last revised on June 15, 2023

NEW HAMPSHIRE

Data Breach Notification Summary

Davis Wright Tremaine LLP

N.H. Rev. Stat. Ann. §§ 359-C:19 to C:21

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	As soon as possible	Yes

Scope of this Summary:

Notification requirements applicable to persons who conduct businesses in the state or who own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if entity determines that misuse of the covered info has not occurred and is not reasonably likely to occur.
Breach Defined	Unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a covered entity.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or secured by a method that renders the covered info completely unreadable or unusable so long as encryption key was not also acquired.
Form of Covered Info	Electronic Only
Covered Information	An individual's first name or initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or other government identification number. ○ Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
Consumer Notice Timing	Must be made as soon as possible following determination that covered information has been or is reasonably likely to be misused or following conclusion that such determination cannot be made.
Consumer Notice Method	By written notice, electronic notice (if the primary means of communication with affected individuals), or by telephone notice (if a log of the notification is kept). Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The notification shall include at a minimum: ○ A description of the incident in general terms. ○ The approximate date of breach. ○ The type of personal information obtained as a result of the security breach. ○ The telephonic contact information of the person required to notify affected individuals
Delayed Notice	The covered entity may delay giving notice if a law enforcement or national security agency determines that the notice will impede a criminal investigation or jeopardize national security.
Government Notice	All entities that do not fall under the jurisdiction of a regulator specified below must notify the Attorney General's office of the breach. Such notice must include the anticipated date of the notice to individuals and the approximate number of individuals who will be notified. Different regulators may have different notification requirements and deadlines. Entities subject to the jurisdiction of the bank commissioner, director of securities regulation, insurance commissioner, public utilities commission, the financial institutions and insurance regulators of other states, or federal banking or securities regulators must notify their primary regulator of the breach.
Consumer Reporting Agency Notice	If required to notify more than 1,000 persons, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of the anticipated date of notification, approximate number of consumers to be notified, and the content of the notice.
Exceptions for Other Laws	Licensees will be exempt from the statute's notification provisions if they are subject to the Gramm-Leach-Bliley Act (GLBA) and provide notice to affected consumers for security breaches consistent with the GLBA's requirements.

Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify and cooperate with it immediately following discovery of a breach if the covered info was acquired by an unauthorized person. Cooperation includes sharing information relevant to the breach but not disclosure of confidential info or trade secrets.
Private Right of Action	Under New Hampshire's general data breach notification statute, affected persons injured as a result of a security breach may bring an action for damages.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

NEW JERSEY

Data Breach Notification Summary

Davis Wright Tremaine LLP

N.J. Stat. Ann. §§ 56:8-161 to -166

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expedient time possible and without unreasonable delay	Yes

Scope of this Summary:

Notification requirements applicable to entities that conduct business in the state and that compile or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if entity established that misuse of the covered info is not reasonably possible. Any determination must be documented in writing and retained for five years.
Breach Defined	Unauthorized access that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or secured by any other method or technology that renders it unreadable or unusable.
Form of Covered Info	Electronic Only

Covered Information	• An individual's first name or first initial and last name linked with any one or more of the following data elements:
	  ○ Social Security number.
	  ○ Driver's license number or state identification card number.
	  ○ Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
	  ○ Username, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account.
	• Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Consumer Notice Timing	Must be made in the most expedient time possible and without unreasonable delay and consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the system.
Consumer Notice Method	By written notice or electronic notice if consistent with E-SIGN. Substitute notice if only a username and password were breached, notification can be in electronic or other form that directs the individual to promptly secure their account(s). A business that provides email accounts shall not send notification to email accounts that were breached but must use other specified methods of notification. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content requirements are not specified.
Delayed Notice	Notification may be delayed if law enforcement determines that notification will impede a criminal or civil investigation and requests that notification be delayed.
Government Notice	In advance of any disclosure to the consumers, must report breach and any information pertaining to it to the Division of State Police in the Department of Law and Public Safety. The notice must include any information pertaining to the breach.
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	None
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	The New Jersey general breach notification statute allows for a private right of action.

Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

NEW MEXICO

Data Breach Notification Summary

Davis Wright Tremaine LLP

N.M. Stat. Ann. §§ 57-12C-1 to -12

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expedient time possible, but no later than 45 days	Yes, if >1,000 residents notified

Scope of this Summary:
Notification requirements applicable to entities that own or license elements that include covered info on a resident. Some types of businesses may be exempt from some or all of these requirements.

Risk of Harm Threshold	Notification not required if, after an appropriate investigation, the covered entity determines that the breach does not give rise to a significant risk of identity theft or fraud.
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to covered info that is encrypted, redacted, or otherwise rendered unreadable or unusable, so long as the encryption key was not accessed or acquired.
Form of Covered Info	Electronic Only
Covered Information	An individual's first name or first initial and last name in combination with one or more of the following data elements: ○ Social Security number. ○ Driver's license number. ○ Government-issue identification number. ○ Account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account. ○ Biometric data, meaning a record generated by automatic measurements of an identified individual's fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry that is used to uniquely and durably authenticate an individual's identity when the individual accesses a physical location, device, system or account.
Consumer Notice Timing	Must be made in the most expedient time possible but no later than 45 calendar days following discovery of the breach, subject to the delay provision discussed below.
Consumer Notice Method	By written notice (delivered by US mail) or electronic notice (if primary method of communication with resident or if consistent with E-SIGN). Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Notifications to New Mexico residents shall contain: ○ The name and contact information of the notifying person. ○ A list of the types of personally identifying information that are reasonably believed to have been the subject of a security breach, if known. ○ The date of the security breach, the estimated date of the breach or the range of dates within which the security breach occurred, if known. ○ A general description of the security breach incident. ○ The toll-free telephone numbers and addresses of the major Consumer Reporting Agencies. ○ Advice that directs the recipient to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. ○ Advice that informs the recipient of the notification of the recipient's rights pursuant to the federal Fair Credit Reporting Act.
Delayed Notice	Notification may be delayed (1) if law enforcement determines that notification will impede a criminal investigation; or (2) as necessary to determine the scope of the breach and restore the integrity, security, and confidentiality of the system.

Government Notice	If more than 1,000 residents are notified, must notify AG in the most expedient time possible but no later than 45 days after discovery of breach, unless delayed notice provision applies. Must include number of residents who were notified and a copy of the notice.
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must notify major Consumer Reporting Agencies in the most expedient time possible but no later than 45 days, unless delayed notice provision applies.
Exceptions for Other Laws	The statute exempts from compliance the following entities: Any person who is subject to the federal Gramm-Leach-Bliley Act (GLBA). Any person who is subject to the federal Health Insurance Portability and Accountability Act (HIPAA).
Third-Party Notice	If you maintain or possess covered info on behalf of another entity, you must notify it in the most expedient time possible, but no later than 45 days following discovery of a breach, subject to the harm threshold and delayed notice provisions.
Private Right of Action	The New Mexico general breach notification statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

NEW YORK

Data Breach Notification Summary

Davis Wright Tremaine LLP

N.Y. Gen. Bus. Law § 899-AA

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	Most expedient time possible and without unreasonable delay	Yes

Scope of this Summary:

Notification requirements applicable to persons or businesses that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notice to affected individuals is not required if the covered entity determines the private information was inadvertently disclosed by an authorized person and the person or entity reasonably determines that the exposure is not likely to result in: misuse of the private information, financial harm to the affected individuals, or emotional harm to the affected individuals, in the case of unknown disclosure of online credentials.
Breach Defined	Unauthorized access to or acquisition of covered info that compromises the data's security, confidentiality, or integrity, excluding certain good-faith acquisitions by employees or agents. The statute lists factors that can be considered to determine if covered info was "acquired."
Encryption Safe Harbor	Statute does not apply to information that is encrypted, so long as encryption key was not accessed or acquired.
Form of Covered Info	Electronic Only
Covered Information	• Information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person, in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or non-driver identification card number. ○ Account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account. ○ Account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password. ○ Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity. ○ A consumer credit card that can be used without a CVV code may trigger a breach. • A username or email address in combination with a password or security question and answer that would permit access to an online account.
Consumer Notice Timing	Must be made in the most expedient time possible and without unreasonable delay and consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the system.
Consumer Notice Method	By written notice, telephone notice (if a log of notifications is kept), or electronic notice (if resident expressly consented to receiving electronic notice, a log of each notification is kept, and business does not require resident to consent to receive notice electronically as a condition of the business relationship). Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The notification shall include: ○ Contact information for the person or business making the notification. ○ Telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information. ○ A description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the

	elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.
Delayed Notice	Notification may be delayed if law enforcement determines notice may impede a criminal investigation.
Government Notice	If residents are notified, must notify the NY Attorney General, the NY Department of State Division of Consumer Protection and New York State Police of the timing, content, and distribution of the notices and the approximate number of affected persons. Collaboration affords affected businesses the ability to effectuate notice to all required recipients via the Office of the Attorney General's online portal. This notice must not delay consumer notice. Regardless of whether a breach affects private information as defined by the general data breach statute, if a covered entity notifies the secretary of health and human services of a breach under HIPAA or HITECH requirements, the covered entity must also notify the NY attorney general within five days
Consumer Reporting Agency Notice	If more than 5,000 residents are notified, must notify Consumer Reporting Agencies of timing, distribution, and content of the consumer notice and the approximate number of affected persons. CRA notice must not delay consumer notice.
Exceptions for Other Laws	Entities subject to breach notification requirements under the following laws are not required to send additional state law notice to affected individuals: Gramm-Leach-Bliley Act, Health Information Portability and Accountability Act (HIPAA), and Health Information Technology for Economic and Clinical Health Act (HITECH Act).
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	*The New York general breach notification statute does not provide for a private right of action; however, it expressly states that it does not exclude other remedies permitted by law (N.Y. Gen. Bus. Law § 899-aa(6)(b)).
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

NORTH CAROLINA

Data Breach Notification Summary

Davis Wright Tremaine LLP

N.C. Gen. Stat. §§ 75-61, 75-65

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Without unreasonable delay	Yes

Scope of this Summary:

Notification requirements applicable to businesses that own or license covered info. Some types of businesses may be exempt from some or all of these requirements; non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if no illegal use of covered info has occurred or is reasonably likely to occur and breach does not create a material risk of harm to resident.
Breach Defined	Unauthorized access and acquisition of covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted, so long as encryption key was not compromised.
Form of Covered Info	Electronic or Paper

Covered Information	• A person's first name or first initial and last name in combination with identifying information:
	  ○ Social Security or employer taxpayer identification numbers.
	  ○ Driver's license, state identification card, or passport numbers.
	  ○ Checking account numbers.
	  ○ Savings account numbers.
	  ○ Credit card numbers.
	  ○ Debit card numbers.
	  ○ Personal Identification (PIN) Code
	  ○ Digital signatures.
	  ○ Any other numbers or information that can be used to access a person's financial resources.
	  ○ Biometric data.
	  ○ Fingerprints.
	
	• Personal information may also include a person's first name or first initial and last name in combination with the following if this information would permit access to a person's financial account or resources:
	  ○ Electronic identification numbers.
	  ○ Electronic mail names or addresses.
	  ○ Internet account numbers.
	  ○ Internet identification names.
	  ○ Parent's legal surname prior to marriage.
	  ○ Passwords.

Consumer Notice Timing	Must be made without unreasonable delay, taking any necessary measures to determine sufficient contact info, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the system.
Consumer Notice Method	By written notice, telephone notice (provided that contact is made directly with the affected persons), or electronic notice (if residents have agreed to receive communications electronically, the entity has a valid email address for the affected persons, and notice is consistent with E-SIGN). Substitute notice is available if certain criteria are satisfied.

Consumer Notice Content	The notification shall be clear and conspicuous and include all of the following:
	  ○ A description of the incident in general terms.
	  ○ A description of the type of personal information that was subject to the unauthorized access and acquisition.
	  ○ A description of the general acts of the business to protect the personal information from further unauthorized access.

	○ A telephone number for the business that the person may call for further information and assistance, if one exists. ○ Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. ○ The toll-free numbers and addresses for the major Consumer Reporting Agencies. ○ The toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.
Delayed Notice	Notification shall be delayed if law enforcement determines that the notification may impede a criminal investigation or jeopardize homeland or national security and makes the request in writing, or the covered entity documents the request contemporaneously in writing, including the name of the officer and agency.
Government Notice	If residents are notified, must notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's office and provide the nature of the breach; number of consumers affected; steps taken to investigate the breach; steps taken to prevent a similar breach in the future; and information regarding the timing, distribution, and content of the consumer notices.
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	None
Third-Party Notice	If you maintain covered info on behalf of another entity, must notify immediately following discovery of a breach.
Private Right of Action	A violation of the general breach notification statute is a violation of the North Carolina unfair and deceptive trade practices statute and an injured person may bring a civil action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

NORTH DAKOTA

Data Breach Notification Summary

Davis Wright Tremaine LLP

N.D. Cent. Code §§ 51-30-01 to -07

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	Most expedient time possible and without unreasonable delay	Yes, if >250 individuals affected

Scope of this Summary:

Notification requirements applicable to persons who own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	The notification obligation is not subject to a risk assessment.
Breach Defined	Unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is secured by encryption or any other method or technology that renders the covered info unreadable or unusable.
Form of Covered Info	Electronic Only
Covered Info	An individual's first name or first initial and last name in combination with any of the following data elements: ○ The individual's Social Security number. ○ The operator's license number assigned to an individual by the department of transportation under section 39-06-14. ○ A non-driver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1. ○ The individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts. ○ The individual's date of birth. ○ The maiden name of the individual's mother. ○ Medical information, meaning any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional. ○ Health insurance information, meaning an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. ○ An identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password. ○ The individual's digitized or other electronic signature.
Consumer Notice Timing	Must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the system.
Consumer Notice Method	By written notice or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The North Dakota general breach notification and insurance data security statutes do not set out specific content requirements for the notice to affected persons and consumers.
Delayed Notice	Notification may be delayed if law enforcement determines notice will impede a criminal investigation.
Government Notice	Must notify without unreasonable delay the Attorney General via mail or email of any breach that affects more than 250 individuals.
Consumer Reporting Agency Notice	The North Dakota general breach notification and insurance data security statutes do not require notice to credit reporting agencies.

Exceptions for Other Laws	The statute includes certain exceptions for entities that are subject to the breach notification requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	The North Dakota general breach notification does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

OHIO

Data Breach Notification Summary

Davis Wright Tremaine LLP

Ohio Rev. Code Ann. §§ 1349.19, 1349.191, 1349.192

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expedient time possible but no longer than 45 days	No

Scope of this Summary:

Notification requirements applicable to individuals or commercial entities that conduct business in the state and own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if the covered entity reasonably believes that the breach has not and will not cause a material risk of identity theft or other fraud to any Ohio resident.
Breach Defined	Unauthorized access and acquisition that compromises the security or confidentiality of the covered info, excluding certain good-faith acquisitions by employees or agents and acquisitions pursuant to a warrant, subpoena, or other court order.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, redacted, or altered in a manner that renders it unreadable.
Form of Covered Info	Electronic Only
Covered Info	An individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or state identification card number. ○ Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.
Consumer Notice Timing	Must be made in the most expedient time possible but no later than 45 days following discovery of the breach, consistent with any measures necessary to determine the scope of the breach, including which residents were affected, and to restore the reasonable integrity of the system.
Consumer Notice Method	By written notice, telephone notice, or electronic notice if it is the covered entity's primary method of communication with resident. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The Ohio general breach notification statute does not set out specific content requirements for the notice to affected individuals.
Delayed Notice	Notification may be delayed if law enforcement determines that the notification will impede a criminal investigation or jeopardize homeland or national security.
Government Notice	The Ohio general breach notification statute does not require notice to any government or regulatory agencies.
Consumer Reporting Agency Notice	If more than 1,000 Ohio residents are notified, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of timing, distribution, and content of the consumer notice. CRA notice may not delay any other required notifications.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it in an expeditious manner following determination of a breach if the breach causes or is reasonably believed will cause a material risk of identity theft or fraud to a resident.
Private Right of Action	The Ohio breach notification statutes do not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

OKLAHOMA

Data Breach Notification Summary

Davis Wright Tremaine LLP

24 Okla. Stat. §§ 161-166

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Without unreasonable delay	No

Scope of this Summary:

Notification requirements applicable to individuals or entities that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if covered entity reasonably believes that breach has not and will not cause identity theft or other fraud to any Oklahoma resident.
Breach Defined	Unauthorized access and acquisition that compromises the security or confidentiality of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted so long as encryption key was not accessed or acquired.
Form of Covered Info	Electronic Only
Covered Info	The first name or first initial and last name in combination with and linked to any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or state identification card number issued in lieu of a driver's license. ○ Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident. ○ Personal information does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.
Consumer Notice Timing	Must be made without unreasonable delay, consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
Consumer Notice Method	By written notice, telephone notice, or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Oklahoma's general breach notification statute does not set out specific content requirements for the notice to affected persons.
Delayed Notice	Notification may be delayed if law enforcement determines and advises that notification will impede a criminal or civil investigation or homeland or national security.
Government Notice	The Oklahoma general breach notification statute does not require notice to any government or regulatory agencies.
Consumer Reporting Agency Notice	The Oklahoma general breach notification statute does not require notice to Consumer Reporting Agencies.
Exceptions for Other Laws	A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (70 Fed. Reg. 15,736 (March 29, 2005)).
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it as soon as practicable following discovery of a breach.
Private Right of Action	Oklahoma's general breach notification statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

OREGON

Data Breach Notification Summary

Davis Wright Tremaine LLP

Or. Rev. Stat. §§ 646A.600-.604, 646A.624-.626

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	No later than 45 days	Yes, if >250 residents affected

Scope of this Summary:

Notification requirements applicable to persons who own, license, or otherwise possess covered info in the course of business, vocation, occupation, or volunteer activities. Some types of businesses may be exempt from some or all of these requirements but may be required to notify AG of breach even if exempt.

Risk of Harm Threshold	Notification not required if, after an appropriate investigation or after consultation with relevant federal, state, or local law enforcement, covered entity reasonably determines that affected residents are unlikely to suffer harm. The determination must be documented in writing and retained for five years.
Breach Defined	Unauthorized acquisition that materially compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, redacted, or rendered unusable with other methods.
Form of Covered Info	Electronic Only
Covered Information	• First name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or state identification card number issued by the Department of Transportation. ○ Passport number or other identification number issued by the United States. ○ Financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account, or any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account. ○ Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction. ○ A health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer. ○ Any information about a consumer's medical history or mental or physical condition or about a healthcare professional's medical diagnosis or treatment of the consumer. • A username or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the username or means of identification.
Consumer Notice Timing	Must be made in the most expeditious time possible and without unreasonable delay but no later than 45 days following discovery or notification of breach. In providing notice, covered entity should undertake reasonable measures necessary to determine sufficient contact info, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.
Consumer Method	In writing, electronically, if consistent with the ESIGN Act. By telephone. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	○ A description of the breach of security in general terms. ○ The approximate date of the breach of security. ○ The type of personal information that was subject to the breach of security. ○ Contact information for the covered entity. ○ Contact information for national Consumer Reporting Agencies. ○ Advice to the consumer to report suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission.
Delayed Notice	Notification to consumers and AG may be delayed only if law enforcement determines that notice will impede criminal investigation and has made a written request that the notification be delayed.
Government Notice	Must notify AG of breaches affecting over 250 residents within 45 days of discovery or notification of breach.

Exceptions for Other Laws	The statute includes certain exceptions for covered entities that comply with: The Gramm-Leach-Bliley Act (GLBA); the Health Insurance Portability and Accountability Act (HIPAA); or the Health Information Technology for Economic and Clinical Health (HITECH) Act.
Consumer Reporting Agency Notice	If more than 1,000 residents affected, must notify, without unreasonable delay, nationwide Consumer Reporting Agencies of timing, distribution, and content of consumer notice, and include police report number, if any. This may not delay consumer notice.
Third-Party Notice	Vendors must notify covered entities as soon as practicable, but no later than 10 days after discovery of a breach, and are not required to notify consumers themselves.
Private Right of Action	* Although the Oregon statute does not explicitly provide for a private right of action, it anticipates that affected consumers may pursue a civil action (Or. Rev. Stat. § 646A.624(3); see Question 12). Notably, two federal district courts have addressed this issue and reached different conclusions (see *Patton v. Experian Data Corp.,* 2018 WL 6190349, at *10 (C.D. Cal. Jan. 8, 2018) and *In re Target Corp. Data Sec. Breach Litig.*, 66 F.Supp.3d 1154, 1167 (D.Minn. 2014)).
Potential Penalties	Violations may result in civil penalties.

Last revised June 15, 2023

PENNSYLVANIA

Data Breach Notification Summary

Davis Wright Tremaine LLP

2005 Pa. Laws 474 (unofficially consolidated in 73 P.S. §§ 2301-2329 (West 2019))

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Without unreasonable delay	No

Scope of this Summary:

Notification requirements applicable to entities that conduct business in the state and maintain, store, or manage covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if the covered entity reasonably believes that the breach has not and will not cause loss or injury to any Pennsylvania resident.
Breach Defined	Unauthorized access and acquisition that materially compromises the security or confidentiality of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted so long as encryption key was not accessed or acquired.
Form of Covered Info	Electronic only
Covered Information	Personal information means an individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements: ○ Social Security number; ○ driver's license number or a state identification card number issued in lieu of a driver's license; ○ financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; ○ medical information; ○ health insurance information; or ○ a username or email address, in combination with a password or security question and answer that would permit access to an online account. • Personal information, or a username or email address in combination with a password or security question and answer that would permit access to an online account.
Consumer Notice Timing	Must be made without unreasonable delay, taking any necessary measures to determine the scope of the breach and to reasonably restore the integrity of the system.
Consumer Notice Method	• By written notice (to the last-known home address), by telephone notice (if the consumer can be reasonably expected to receive it), or by email notice (if a prior business relationship exists and the entity has a valid email address). Substitute notice is available if certain criteria are satisfied • Effective May 2, 2023, a covered entity may comply with notice requirements by providing notice in electronic or another form that directs the person whose personal information has been materially compromised to promptly change their password and security question or answer if the breach involves either.
Consumer Notice Content	The Pennsylvania statute does not set out specific content requirements for the notice to affected persons.
Delayed Notice	Notification may be delayed if law enforcement determines and advises the covered entity in writing specifically referencing this section that notification will impede a criminal or civil investigation.
Government Notice	The Pennsylvania statute does not require notice to any government or regulatory agencies.
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of timing, distribution, and number of consumer notices.
Exceptions for Other Laws	Effective May 2, 2023, any covered entity that is subject to and in compliance with the privacy and security standards for the protection of electronic personal health information established under the Health Insurance

	Portability and Accountability Act of 1996 or Health Information Technology for Economic and Clinical Health (HITECH) Act are deemed in compliance with the statute (§ 5.3, S.B. 696).
Third-Party Notice	If you maintain, store, or manage covered info on behalf of another entity, you must notify it following discovery of a breach.
Private Right of Action	The Pennsylvania statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

PUERTO RICO

Data Breach Notification Summary

Davis Wright Tremaine LLP

10 P.R. Laws Ann. § 4051-4055

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	As expeditiously as possible*	Yes

Scope of this Summary:
Notification requirements applicable to entities authorized to operate or do business in Puerto Rico and that own or are custodians of covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	None
Breach Defined	Unauthorized access that compromises the security, confidentiality, or integrity of the covered info; or where authorized persons or entities accessed and violated professional confidentiality standards or obtained authorization under false representation with intent to make illegal use of covered info.
Encryption Safe Harbor	Statute does not apply to information that needs a special cryptographic code to access.
Form of Covered Information	Electronic Only
Covered Information	At least the name or first initial and the surname of a person, together with any of the following data: ○ Social Security number. ○ Driver's license number, voter's identification or other official identification. ○ Bank or financial account numbers of any type with or without passwords or access code that may have been assigned. ○ Names of users and passwords or access codes to public or private information systems. ○ Medical information protected by the HIPAA. ○ Tax information. ○ Work-related evaluations.
Consumer Notice Timing	As expeditiously as possible, consistent with any measures to restore the security of the system.
Consumer Notice Method	By written notice, telephone notice, or electronic notice (if it is the primary method of communication with the resident or is consistent with E-SIGN Act). Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The notification shall be clear and conspicuous and include the following: ○ A description of the breach in general terms. ○ A description of the type of sensitive information compromised. ○ A toll-free number and an Internet site for people to use in order to obtain information or assistance.
Delayed Notice	Notification may be delayed if law enforcement needs to secure possible crime scenes and evidence.
Government Notice	* Must notify the Department of Consumer Affairs within a non-extendable term of 10 days after discovery of the breach, and the Department must make a public announcement of the fact within 24 hours of receiving the notification.
Consumer Reporting Agency Notice	N/A
Exceptions for Other Laws	No provision of this chapter shall be interpreted as being prejudicial to those institutional information and security policies that an enterprise or entity may have in force prior to its effectiveness and whose purpose is to provide protection equal to or better than the information on security herein established.
Third-Party Notice	If you resell or provide access to digital data banks containing covered info, you must notify the proprietor, custodian, or holder of said covered info of any breach that allows access to files containing covered info.
Private Right of Action	The Puerto Rico statute allows for private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

This summary is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. Additional requirements or conditions may apply to any or all provisions referenced herein. For more information about the state data breach notification laws or other data security matters, please seek the advice of counsel.

www.dwt.com

RHODE ISLAND

Data Breach Notification Summary

Davis Wright Tremaine LLP

R.I. Gen. Laws §§ 11-49.3-1 to 11-49.3-6

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expedient time possible but no later than 45 days	Yes, if >500 residents

Scope of this Summary:

Notification requirements applicable to persons who store, own, collect, process, maintain, acquire, use, or license covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification of a breach is not required if, after an appropriate investigation, it is determined that the breach has not and will not likely result in a significant risk of identity theft to the individuals whose personal information was acquired.
Breach Defined	Unauthorized access or acquisition that materially compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted so long as encryption key was not accessed or acquired.
Form of Covered Information	Electronic or Paper
Covered Information	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number, Rhode Island identification card number, or tribal identification number. ○ Account number, credit or debit card number, in combination with any required security code, access code, password, or personal identification number that would permit access to an individual's financial account. ○ Medical information, meaning any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional or provider. ○ Health insurance information, meaning an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual. ○ E-mail address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance or financial account.
Consumer Notice Timing	Must be made in the most expedient time possible but no later than 45 days after confirmation of the breach and the ability to ascertain information that must be included in the consumer notice.
Consumer Notice Method	By written notice or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	• Notifications to individuals must include the following information to the extent known: ○ A general and brief description of the incident, including how the security breach occurred and the number of affected individuals. ○ The type of information that was subject to the breach. ○ Date of breach, estimated date of breach or the date range within which the breach occurred. ○ Date that the breach was discovered. ○ A clear and concise description of any remediation services offered to affected individuals including toll-free numbers and websites to contact: the major credit reporting agencies, remediation service providers and the attorney general. • A clear and concise description of the consumer's ability to file or obtain a police report; how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the Consumer Reporting Agencies.

Delayed Notice	Notification may be delayed if law enforcement determines and notifies the entity that notice will impede a criminal investigation.
Government Notice	If more than 500 residents are notified, must notify the Attorney General of timing, distribution, and content of the consumer notice and the number of affected individuals. Notification may not delay consumer notice.
Consumer Reporting Agency Notice	If more than 500 residents are notified, must notify the major Consumer Reporting Agencies of timing, distribution, and content of the consumer notice and the number of affected individuals. Notification may not delay consumer notice.
Exceptions to Other Laws	Entities subject to and comply with the Health Insurance Portability and Accountability Act (HIPAA). Entities that comply with the notification requirements of their primary or functional federal regulators as defined in 15 USC § 6809(2).
Third-Party Notice	In Rhode Island, any state agency or person that maintains computerized unencrypted data that includes personal information it does not own must directly notify the affected persons of the breach.
Private Right of Action	The Rhode Island general breach notification statute does not provide for a private cause of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

SOUTH CAROLINA

Data Breach Notification Summary

Davis Wright Tremaine LLP

S.C. Code Ann. § 39-1-90

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expedient time possible and without unreasonable delay	Yes, if >1,000 residents notified

Scope of this Summary:

Notification requirements applicable to persons conducting business in the state and who own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if you reasonably believe that illegal use has not and is not reasonably likely to occur or if use of covered info does not create a material risk of harm to the resident.
Breach Defined	Unauthorized access and acquisition that materially compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, redacted, or rendered unusable with other methods.
Form of Covered Information	Electronic Only
Covered Information	The first name or first initial and last name in combination with and linked to any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or state identification card number issued instead of a driver's license. ○ Financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account. ○ Other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.
Consumer Notice Timing	Must be made in the most expedient time possible without unreasonable delay, consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
Consumer Notice Method	By written notice, telephone notice, or electronic notice (if it is the primary method of communication with the resident or is consistent with E-SIGN and Chapter 6, Title 11 of the 1976 Code). Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	South Carolina does not have specific content requirements for the notification letter.
Delayed Notice	Notification may be delayed if law enforcement determines notice may impede a criminal investigation.
Government Notice	If more than 1,000 residents notified pursuant to this statute, must notify Consumer Protection Division of the South Carolina Department of Consumer Affairs, without unreasonable delay, of timing, distribution, and content of the consumer notice.
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	Does not apply to a bank or financial institution that is subject to and in compliance with the privacy and security provision of the Gramm-Leach-Bliley Act (GLBA).
Third-Party Notice	If you conduct business in the state and maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	The South Carolina general breach notification statute allows for private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

SOUTH DAKOTA

Data Breach Notification Summary

Davis Wright Tremaine LLP

SDCL §§ 22-40-19 to 22-40-26

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	No later than 60 days	Yes, if >250 residents are affected

Scope of this Summary:

Notification requirements applicable to individuals or entities that conduct business in the state and own or license covered info. Some types of businesses may be exempt from some or all of these requirements.

Rick of Harm Threshold	Notification is not required if, after appropriately investigating the breach and notifying the South Dakota attorney general, the information holder reasonably determines that the security breach is not likely to result in harm to the affected individual. Covered entities must document and retain the determination for at least three years.
Breach Defined	Unauthorized acquisition that materially compromises the security, confidentiality, or integrity of covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to covered info that is encrypted so long as the encryption key was not also acquired.
Form of Covered Information	Electronic Only
Covered Information	• A South Dakota resident's first name or first initial and last name, in combination with any one or more of the following data elements: ○ Social security number. ○ Driver's license number or other unique identification number created or collected by a government body. ○ Account, credit card, or debit card number, in combination with any required security code, or information that would permit access to a person's financial account. ○ Health information, meaning information that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. ○ An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes. ○ Personal information does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable; and • The following information is also protected, even when not combined with a resident's name: ○ A username or email address, in combination with a password, security question answer, or other information that permits access to an online account. ○ Account number or credit or debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account.
Consumer Notice Timing	Must be made no later than 60 days after discovery or notification of breach.
Consumer Notice Method	By written notice or electronic notice if consistent with E-SIGN or if primary method of communication with affected resident. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The South Dakota Statute does not include content requirements for the notice to affected individuals.
Delayed Notice	Notification may be delayed if law enforcement determines that notification will impede a criminal investigation. If notification is delayed, it must be made no later than 30 days after law enforcement determines notification will not compromise the investigation.

Government Notice	If over 250 residents are affected, must notify the attorney general.
Consumer Reporting Agency Notice	If required to notify any residents, must also notify, without unreasonable delay, all national Consumer Reporting Agencies of timing, distribution, and content of notice.
Exceptions for Other Laws	The statute deems in compliance any information holder that is regulated by federal law or regulation, including the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA), and notifies affected South Dakota residents in accordance with those laws.
Third-Party Notice	The South Dakota statute does not list requirements for third-party notice.
Private Right of Action	The South Dakota statute does not provide a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

TENNESSEE

Data Breach Notification Summary

Davis Wright Tremaine LLP

Tenn. Code Ann. § 47-18-2105 to 47-18-2107

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	No later than 45 days	No

Scope of this Summary:

Notification requirements applicable to persons or businesses that conduct business in the state that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification is required only if the unauthorized acquisition of computerized data materially compromises the security, confidentiality, or integrity of personal information the information holder maintains.
Breach Defined	Unauthorized acquisition that materially compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	The unauthorized acquisition of encrypted nonpublic information is not considered a cybersecurity event if the encryption, process, or key is not also acquired, released, or used without authorization.
Form of Covered Info	Electronic Only
Covered Information	An individual's first name or first initial and last name, in combination with any one or more of the following data elements: ○ Social security number. ○ Driver's license number. ○ Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
Consumer Notice Timing	Must be made no later than 45 days after discovery or notification of the breach.
Consumer Notice Method	By written notice or electronic notice (if consistent with E-SIGN or the primary method of communication with the resident). Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Tennessee does not have specific content requirements for the notice to affected individuals.
Delayed Notice	Notification may be delayed if law enforcement determines notice will impede a criminal investigation. If notification is delayed, it must be made no later than 45 days after law enforcement determines that notification will not compromise the investigation.
Government Notice	The Tennessee statute does not require notice to any government or regulatory agencies.
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of timing, distribution, and content of the consumer notice.
Exceptions for other laws	Information holders subject to either the Gramm-Leach-Bliley Act (GLBA) or the Health Information Portability and Accountability Act (HIPAA) are exempt from the statute.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it no later than 45 days following discovery of a breach.
Private Right of Action	Under the Tennessee general breach notification statute, a Tennessee person or business entity who is a customer of an information holder and is injured by a violation of the statute may institute a civil action to recover damages and enjoin the information holder from further action in violation of the statute.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

TEXAS

Data Breach Notification Summary

Davis Wright Tremaine LLP

Tex. Bus. & Com. Code Ann. §§ 521.002, 521.053, 521.151

*****Amendments to TX Data Breach Notification Statute scheduled to go into effect on 9/1/23**

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	Without unreasonable delay, but no later than 60 days	Yes, if 250+ residents are affected

Scope of this Summary:

Notification requirements applicable to persons who conduct business in Texas and who own, license, or maintain covered info associated with any individual (whether or not they are a Texas resident, though individuals who are residents of another state that requires notice of a data breach may be notified under that state's law). Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	The notification obligation is not subject to a risk assessment.
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted so long as encryption key was not accessed or acquired.
Form of Covered Info	Electronic Only
Covered Information	An individual's first name or first initial and last name in combination with any one or more of the following items: ○ Social Security number. ○ Driver's license number or government-issued identification number. ○ Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. ○ Information that identifies an individual and relates to: ▪ The physical or mental health or condition of the individual. ▪ The provision of health care to the individual. ▪ Payment for the provision of health care to the individual.
Consumer Notice Timing	Must be made as quickly as possible except as necessary to determine the scope of the breach and restore the reasonable integrity of the system.
Consumer Notice Method	By written notice or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The statute does not provide content requirements for the notice to affected persons.
Delayed Notice	Notification may be delayed if law enforcement determines notice will impede a criminal investigation. Notification must be made as soon as law enforcement determines that the notification will not compromise the investigation.
Government Notice	Effective September 1, 2023, must notify the Attorney General no later than 30 days after the discovery of the breach if it involves at least 250 residents. Notification must include a detailed description of the breach or the use of covered information acquired as a result of the breach; the number of residents affected; measures taken and intended to be taken regarding the breach; and whether law enforcement is investigating the breach.
Consumer Reporting Agency Notice	If more than 10,000 persons are notified, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	The statute does not include exceptions for entities subject to other laws.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of action	The Texas statute does not provide for a private right of action.

Potential Penalties	Violations may result in civil penalties.

**Last Revised on June 15, 2023*

UTAH

Data Breach Notification Summary

Davis Wright Tremaine LLP

Utah Code Ann. §§ 13-44-101 to -301

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expedient time possible and without unreasonable delay	Yes, if 500+ residents are affected

Scope of this Summary:

Notification requirements applicable to persons who own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if, after reasonable and prompt investigation, the covered entity determines that identity theft or fraud has not occurred and is not reasonably likely to occur.
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or protected by another method that renders the data unreadable or unusable.
Form of Covered Info	Electronic Only
Covered Information	A person's first name or first initial and last name, combined with any one or more of the following data elements: ○ Social Security number. ○ Financial account number, or credit or debit card number and any required security code, access code, or password that would permit access to the person's account. ○ Driver's license number or state identification card number.
Consumer Notice Timing	Must be made in the most expedient time possible without unreasonable delay, consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
Consumer Notice Method	By written notice sent by first-class mail to the most recent known address, telephone notice (including by automatic dialing technology not prohibited by other law), electronic notice (if it is the primary method of communication with resident or is consistent with E-SIGN). Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The Utah general breach notification statute does not set out specific content requirements for the notice to affected persons.
Delayed Notice	Notification may be delayed if law enforcement determines notice may impede a criminal investigation.
Government Notice	The Utah general breach notification statute requires notification to the AG office if 500 or more residents are affected. Notification must also be made to the Utah Cyber Center (once the department has been created).
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	Breach of system security procedures as required by its primary state or federal regulator under applicable law and, in accordance with that law, each affected Utah resident is notified of a breach.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach if misuse of covered info has or is reasonably likely to occur. Must cooperate by sharing with the data owner info relevant to the breach.
Private Right of Action	The Utah general breach notification statute does not create a private right of action, but explicitly provides that it does not affect any private right of action that may exist under other law, including contract or tort (Utah Code § 13-44-301(2)(b)).
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

VERMONT

Data Breach Notification Summary

Davis Wright Tremaine LLP

9 Vt. Stat. Ann. §§ 2430-2435

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expedient time possible without unreasonable delay but no later than 45 days	Yes

Scope of this Summary:

Notification requirements applicable to commercial entities that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if covered entity determines misuse of covered info is not reasonably possible and provides documentation of determination to Attorney General or Dept. of Financial Regulation, as appropriate. However, the covered entity must notify affected persons if it later gathers facts that indicate the misuse of personal information or login credentials is reasonably possible.
Breach Defined	Unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information or login credentials maintained by a data collector.
Encryption Safe Harbor	Statute does not apply to info that is encrypted, redacted, or protected by another method that renders it unreadable or unusable.
Form of Covered Information	Electronic Only
Covered Information	An individual's first name or first initial and last name in combination with one or more of the following data elements: ○ Social Security number. ○ Driver's license or nondriver state identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction. ○ Financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords. ○ A password or personal identification number or other access code for a financial account. ○ Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. ○ Genetic information. ○ Health records or records of a wellness program or similar program of health promotion or disease prevention; a healthcare professional's medical diagnosis or treatment of the individual; or a health insurance policy number. The statute also protects login credentials, defined as a consumer's username or email address, in combination with a password or an answer to a security question, that together permit access to an online account.
Consumer Notice Timing	The Vermont statute requires covered entities to give notice to affected persons in the most expedient time possible and without unreasonable delay, but not later than 45 days after discovery, consistent with the legitimate needs of a law enforcement investigation or a national or homeland security investigation.
Consumer Notice Method	By written notice, telephone notice (if direct contact with resident via a live call), or electronic notice (if primary method of communication with resident or is consistent with E-SIGN). Substitute notice available if certain criteria are satisfied.

Consumer Notice Content	Notice shall be clear and conspicuous and include a description of each of the following, if known: ○ The incident in general terms. ○ The type of personally identifiable information that was subject to the security breach. ○ The general acts of the entity to protect the personally identifiable information from further security breach. ○ A telephone number, toll-free if available, that the individual may call for further information and assistance. ○ Advice that directs the individual to remain vigilant by reviewing account statements and monitoring free credit reports. ○ The approximate date of the security breach. If a breach is limited to login credentials for an online account other than an email account, an entity shall: ○ Provide notice of the security breach to the individual electronically or through one or more of the methods specified in the section below and shall advise the individual to take steps necessary to protect the online account, including to change his or her login credentials for the account and for any other account for which the individual uses the same login credentials.
Delayed Notice	Notification shall be delayed if law enforcement believes notice may impede an investigation or jeopardize public safety or national or homeland security interests. If law enforcement makes the request in a form other than in writing, the covered entity must document the request in writing, including name of officer and agency making the request.
Government Notice	Subject to a law enforcement delay, must provide preliminary notice to the Attorney General (or Dept. of Financial Regulation if regulated by the Dept.) within 14 business days of discovery of the breach. Notice should include date of the breach (if known), date of discovery, and a preliminary description of the breach. This requirement is subject to certain limitations. When consumer notice is provided, the covered entity must provide follow-up notice to the Attorney General or Department, as appropriate, identifying the number of Vermont residents affected, if known, and a copy of the consumer notice.
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	Covered entities that are subject to the privacy, security, and breach notification rules set by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are deemed in compliance with the state's notification laws, if the covered entity: Experiences a breach that is limited to health records and provides notice to affected consumers as required by HIPAA's breach notification rule.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	The Vermont statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on November 15, 2023

VIRGIN ISLANDS

Data Breach Notification Summary

Davis Wright Tremaine LLP

14 V.I. Code Ann. §§ 2209-2212

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
No	Most expedient time possible and without unreasonable delay	No

Scope of this Summary:

Notification requirements applicable to persons and businesses that conduct business in the territory and that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	N/A
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted.
Form of Covered Information	Electronic Only
Covered Information	An individual's first name or first initial and last name in combination with any one or more of the following data elements: ○ Social Security number. ○ Driver's license number. ○ Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
Consumer Notice Timing	Must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system.
Consumer Notice Method	By written notice or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Content not specified
Delayed Notice	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Government Notice	The Virgin Islands statute does not require notice to any government or regulatory agencies.
Consumer Reporting Agency Notice	The Virgin Islands statute does not require notice to any Consumer Reporting Agencies.
Exceptions for Other Laws	A covered entity that notifies affected individuals of a breach according to the rules, regulations, procedures, or guidelines established by its primary or functional federal regulator is deemed in compliance with this statute's individual notification requirements.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	The Virgin Island Statute provides for a private right of action.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

VIRGINIA

Data Breach Notification Summary

Davis Wright Tremaine LLP

Va. Code Ann. § 18.2-186.6; as amended (2019)

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Without unreasonable delay	Yes, in the event that more than 1,000 residents are notified at one time

Scope of this Summary:

Notification requirements applicable to individuals or entities that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements and non-commercial entities may be subject to different requirements. Incidents involving medical information may be subject to different requirements (Va. Code Ann. § 32.1-127.1:05).

Risk of Harm Threshold	Notification not required if covered entity reasonably believes that breach has not and will not cause identity theft or other fraud to any Virginia resident.
Breach Defined	Unauthorized access and acquisition that compromises the security or confidentiality of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted, so long as encryption key was not accessed or acquired.
Form of Covered Information	Electronic Only
Covered Information	The first name or first initial and last name in combination with and linked to any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or state identification card number issued in lieu of a driver's license number. ○ Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts. ○ Passport number. ○ Military identification number.
Consumer Notice Timing	Must be made without unreasonable delay following discovery or notification of the breach, consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
Consumer Notice Method	By written notice to last known postal address, telephonically, or electronic notice. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Notice shall include a description of the following: ○ The incident in general terms. ○ The type of personal information or medical information that was subject to the unauthorized access and acquisition. ○ The general acts of the individual or entity to protect the personal information or medical information from further unauthorized access. ○ A telephone number that the person may call for further information and assistance, if one exists. ○ Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.
Delayed Notice	Notification may be delayed if law enforcement determines and advises that notice will impede a criminal or civil investigation or national or homeland security.
Government Notice	If more than 1,000 residents are notified, must notify Attorney General without unreasonable delay following discovery or notification of the breach.
Consumer Reporting Agency Notice	If more than 1,000 residents are notified, must notify all nationwide Consumer Reporting Agencies without unreasonable delay of timing, distribution, and content of the consumer notice.

Exceptions for Other Laws	An entity that is subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) (GLBA) and maintains procedures for notification of a breach of the security of the system in accordance with the provision of that Act and any rules, regulations, or guidelines promulgated thereto shall be deemed to be in compliance with this section.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it without unreasonable delay following discovery of the breach.
Private Right of Action	The Virginia general breach notification statute allows an injured person to recover economic damages.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

WASHINGTON

Data Breach Notification Summary

Davis Wright Tremaine LLP

Wash. Rev. Code §§ 19.255.005-.040

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	No more than 30 Days after discovery of the breach	Yes, if more than 500 Washington residents are affected

Scope of this Summary:

Notification requirements applicable to persons or businesses that conduct business in the state and own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if the breach is not reasonably likely to subject consumers to a risk of harm.
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted in a manner that meets or exceeds the National Institute of Standards and Technology standard or has been otherwise modified so that covered info is unreadable, unusable, or undecipherable so long as encryption key was not accessed or acquired.
Form of Covered Information	Electronic or Paper

Covered Information	• An individual's first name or first initial and last name in combination with any one or more of the following data elements:
	  ○ Social security number.
	  ○ Driver's license number or Washington identification card number.
	  ○ Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account.
	  ○ Full date of birth.
	  ○ Private key that is unique to an individual and that is used to authenticate or sign an electronic record.
	  ○ Student, military, or passport identification number.
	  ○ Health insurance policy number or health insurance identification number.
	  ○ Any information about a consumer's medical history or mental or physical condition or about a healthcare professional's medical diagnosis or treatment of the consumer.
	  ○ Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual.
	  ○ For state and local agencies only under RCW § 42.56.590 as amended by SB 6187, effective June 11, 2020: the list of regulated data elements is expanded to include the last four digits of a Social Security number.
	• Username or email address in combination with a password or security questions and answers that would permit access to an online account.

Consumer Notice Timing	Must be made in the most expedient time possible without unreasonable delay but no more than 30 calendar days after the breach was discovered, consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
Consumer Notice Method	By written notice or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied. By email if the breach involves a username or password, except that if the breach involves the login credentials of an email account provided by the covered entity then notice cannot be provided to that email address.

Consumer Notice Content	Notifications to affected individuals must be written in plain language and include, at a minimum, the following:
	  ○ The name and contact information of the reporting entity.
	  ○ A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

	○ A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach. ○ The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.
Delayed Notice	Notification to consumers may be delayed if data owner or licensee contacts a law enforcement agency after discovery of a breach and the agency determines notification will impede a criminal investigation.
Government Notice	If more than 500 residents must be notified, must provide notice to the Attorney General within 30 days of discovering the breach. *This notice must be updated if any required information is unknown at the time the notice is due. While entities subject to HIPAA and federal banking regulators are generally exempt from this statute, they must still notify the state Attorney General.
Consumer Reporting Agency Notice	The Washington statutes do not require notice to credit reporting agencies.
Exceptions for Other Laws	Entities that are subject to the breach notification requirements and comply with either of the following will be deemed in compliance with the consumer notification requirements, but may be required to notify the Washington Attorney General (see Reporting to Government or Regulatory Agencies): The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and are subject to HIPAA breach notification requirements. The Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it immediately following discovery of a breach.
Private Right of Action	In Washington, any consumer injured by a violation of the general breach notification statute may institute a civil action to recover damages.
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

If you have questions about data breach notification requirements, please contact one of the members of our Privacy & Security group who counsels businesses and individuals about such requirements, including Mike Borgia. If you have questions or comments about this summary, please contact DWTBreach@dwt.com.

WEST VIRGINIA

Data Breach Notification Summary

Davis Wright Tremaine LLP

W. Va. Code §§ 46A-2A-101 to -105

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Without unreasonable delay	No

Scope of this Summary:

Notification requirements applicable to individuals or commercial entities that own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if covered entity reasonably believes that breach has not and will not cause identity theft or other fraud to any resident.
Breach Defined	Unauthorized access and acquisition that compromises the security or confidentiality of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted or redacted so long as encryption key was not accessed or acquired.
Form of Covered Info	Electronic Only
Covered Information	The first name or first initial and last name linked to any one or more of the following data elements: ○ Social Security number. ○ Driver's license number or state identification card number issued in lieu of a driver's license. ○ Financial account number, or credit card or debit card number, in combination with any required security code, access code or password that would permit access to a resident's financial accounts.
Consumer Notice Timing	Must be made without unreasonable delay, consistent with any measures to determine the scope of the breach and restore the reasonable integrity of the system.
Consumer Notice Method	By written notice to postal address in covered entity's records, telephone notice, or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	Notification shall include, to the extent possible: ○ A description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person, including social security numbers, driver's licenses or state identification numbers and financial data. ○ A telephone number or website address that the individual may use to contact the entity or the agent of the entity and from whom the individual may learn: ▪ What types of information the entity maintained about that individual or about individuals in general. ▪ Whether or not the entity maintained information about that individual. ▪ The toll-free contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a fraud alert or security freeze.
Delayed Notice	Notification may be delayed if law enforcement determines and advises that notice will impede a criminal or civil investigation or homeland or national security.
Government Notice	The West Virginia statute does not require notice to any government or regulatory agencies.
Consumer Reporting Agency Notice	If more than 1,000 residents are notified under this statute, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	An entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures or guidelines established by the entity's primary or functional regulator shall be in compliance with this article.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it as soon as practicable following discovery of a breach.
Private Right of Action	The West Virginia statute does not provide for a private right of action.

Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

If you have questions about data breach notification requirements, please contact one of the members of our Privacy & Security group who counsels businesses and individuals about such requirements, including Mike Borgia. If you have questions or comments about this summary, please contact DWTBreach@dwt.com.

WISCONSIN

Data Breach Notification Summary

Davis Wright Tremaine LLP

Wis. Stat. § 134.98

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Within reasonable time not greater than 45 days	No

Scope of this Summary:

Notification requirements applicable to entities, other than individuals, that conduct business in the state and maintain covered info in ordinary course of business, license covered info in the state, maintain deposit accounts for a resident, or lend money to a resident. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if acquisition of covered info does not create a material risk of identity theft or fraud to the affected person.
Breach Defined	Unauthorized acquisition of covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information that is encrypted, redacted, or altered in a manner that renders it unreadable.
Form of Covered Information	Electronic or Paper
Covered Information	An individual's last name and first name or first initial, in combination with and linked to any of the following elements: ○ The individual's Social Security number. ○ The individual's driver's license number or state identification number. ○ The individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account. ○ The individual's deoxyribonucleic acid profile, as defined in s. 939.74 (2d) (a). ○ The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.
Consumer Notice Timing	Must make reasonable efforts to notify affected residents within a reasonable time not to exceed 45 days after discovery of the breach, subject to law enforcement delay.
Consumer Notice Method	By mail or by a method the entity has previously used to communicate with the affected person. If address is not known and covered entity has not previously communicated with the affected person, covered entity must provide notice by a method reasonably calculated to actually notify the affected person.
Consumer Notice Content	Notice must indicate that covered entity knows of the unauthorized acquisition of covered info pertaining to the resident. Upon written request from a notified individual, the covered entity must identify the covered info that was acquired.
Delayed Notice	Notification must be delayed if law enforcement determines delay necessary to protect an investigation or homeland security.
Government Notice	The Wisconsin general notification statute does not require notice to any government or regulatory agencies.
Consumer Reporting Agency Notice	If more than 1,000 individuals are notified, must notify, without unreasonable delay, all nationwide Consumer Reporting Agencies of timing, distribution, and content of the consumer notice.
Exceptions for Other Laws	The statute includes certain exceptions for entities that are subject to and in compliance with either: The Gramm-Leach-Bliley Act or the privacy and security regulations implemented under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), if it complies with the regulations, including the breach notification requirements.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it as soon as practicable following determination of a breach.

Private Right of Action	Although Wisconsin's general breach notification statute does not explicitly provide for a private right of action, it provides that, while a violation itself is not negligence or a breach of any duty, it may be evidence of negligence or a breach of a legal duty (Wis. Stat. § 134.98(4)).
Potential Penalties	Violations may result in civil penalties.

Last revised on June 15, 2023

If you have questions about data breach notification requirements, please contact one of the members of our Privacy & Security group who counsels businesses and individuals about such requirements, including Mike Borgia. If you have questions or comments about this summary, please contact DWTBreach@dwt.com.

WYOMING

Data Breach Notification Summary

Davis Wright Tremaine LLP

Wyo. Stat. Ann. §§ 40-12-501 to -502

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
Yes	Most expedient time possible without unreasonable delay	No

Scope of this Summary:

Notification requirements applicable to individuals and commercial entities that conduct business in the state and own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements, and non-commercial entities may be subject to different requirements.

Risk of Harm Threshold	Notification not required if, after a reasonable and prompt investigation, covered entity determines that misuse of covered info about a Wyoming resident has not occurred and is not likely to occur.
Breach Defined	Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Encryption Safe Harbor	Statute does not apply to information where data elements are redacted.
Form of Covered Information	Electronic Only
Covered Information	The first name or first initial and last name of a person in combination with one or more of the data elements: ○ Social Security number. ○ Driver's license number. ○ Account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person. ○ Tribal identification card. ○ Federal or state government-issued identification card. ○ Shared secrets or security tokens that are known to be used for data-based authentication. ○ A username or email address, in combination with a password or security question and answer that would permit access to an online account. ○ A birth or marriage certificate. ○ Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional. ○ Health insurance information, meaning a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person or information related to a person's application and claims history. ○ Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes. ○ An individual taxpayer identification number.
Consumer Notice Timing	Must be made in the most expedient time possible without unreasonable delay following determination that covered info has been or will be misused, consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
Consumer Notice Method	Written notice. Electronic mail notice. Substitute notice is available if certain criteria are satisfied.
Consumer Notice Content	The notification shall be clear and conspicuous and shall include, at a minimum: ○ A toll-free number ▪ That the individual may use to contact the person collecting the data, or his agent; and

	▪ From which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies. ○ The types of personally identifying information that were or are reasonably believed to have been the subject of the breach. ○ A general description of the breach incident. ○ The approximate date of the breach of security, if that information is reasonably possible to determine at the time notice is provided. ○ In general terms, the actions taken by the individual or commercial entity to protect the system containing the personally identifying information from further breaches. ○ Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports. ○ Whether notification was delayed as a result of a law enforcement investigation, if that information is reasonably possible to determine at the time the notice is provided.
Delayed Notice	Notification may be delayed if law enforcement determines in writing that notification may seriously impede a criminal investigation.
Government Notice	The Wyoming statute does not require notice to any government or regulatory agencies.
Consumer Reporting Agency Notice	The Wyoming statute does not require notification to credit reporting agencies.
Exceptions for Other Laws	The statute includes certain exceptions for entities that are subject to either the Gramm-Leach-Bliley Act (GLBA) or Health Insurance Portability and Accountability Act (HIPAA) if those entities notify affected Wyoming residents in compliance with the requirements of those laws.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify it as soon as practicable following determination of a breach.
Private Right of Action	The Wyoming statute does not provide for a private right of action.
Potential Penalties	Violations may result in civil penalties.

**Last revised on June 15, 2023*

If you have questions about data breach notification requirements, please contact one of the members of our Privacy & Security group who counsels businesses and individuals about such requirements, including Mike Borgia. If you have questions or comments about this summary, please contact DWTBreach@dwt.com.

Davis Wright Tremaine's Privacy & Security practice group maintains this summary of the 50 state data breach notification statutes (plus the statutes for Washington, D.C., Guam, Puerto Rico, and the U.S. Virgin Islands). The summary should help answer questions about state data breach notification requirements, but it is not intended to provide legal advice, which can only be given in response to inquiries regarding particular situations.

If you have questions about data breach notification requirements, please contact one of the members of our Privacy & Security group who counsels businesses and individuals about such requirements, including Mike Borgia. If you have questions or comments about this summary, please contact DWTBreach@dwt.com.

Please note that states may periodically amend their respective data breach notification statutes and these amendments may affect or modify any current data breach notification requirements. DWT's State Data Breach Notification Summaries will be updated as those amendments go into effect. Please refer to the last revised date on each summary page for information on when the most recent updates have been made to the individual state summaries.