**Information Extraction Questions**

1. **Does Delaware require entities to notify the state attorney general or other governmental agency in the event of a data breach?**

Answer

Delaware’s data breach notification statute requires that if the affected number of Delaware residents to be notified exceeds 500 residents, the person required to provide notice shall provide notice of the breach of security to the attorney general. 6 Del. C. § 12B-102(d).

**RAG response:**

Looking into the following states:

1. Delaware

Delaware:

Delaware requires entities to notify the state Attorney General if the affected number of Delaware residents to be notified exceeds 500 residents in the event of a data breach (12B -102. Disclosure of breach of security; notice.pdf, 18 Del. C. \_ 8606.pdf).

References:

1. Current Cybersecurity Law\Delaware\Data breach Notification\\_ 12B-102. Disclosure of breach ofsecurity; notice.pdf

2. Current Cybersecurity Law\Delaware\Insurance\18 Del. C. \_ 8606.pdf

1. **How does Connecticut’s Data Breach Notification statute define a breach of security?**

Answer

Connecticut’s data breach notification statute defines the term breach of security as the:

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

Conn. Gen. Stat. § 36a-701b(a)(1).

**RAG Response:**

Looking into the following states:

1. Montana

Montana:

Personal information in Montana's Data Breach Notification Statute is defined as an individual’s first name or first initial and last name in combination with specific data elements, which include:

- Social security number

- Driver’s license number, state identification card number, or tribal identification card number

- Account number or credit or debit card number with security code, access code, or password for financial access

- Medical record information as defined in 33-19-104

- Taxpayer identification number

- Identity protection personal identification number issued by the United States internal revenue service

Personal information does not include publicly available information made lawfully available to the general public from government records.

References:

1. Current Cybersecurity Law\Montana\Identity Theft\30-14-1704 Computer security breach.pdf

2. Current Cybersecurity Law\Montana\Identity Theft\30-14-1704 Computer security breach.pdf

3. Current Cybersecurity Law\Montana\Identity Theft\30-14-1704 Computer security breach.pdf

4. Current Cybersecurity Law\Montana\Identity Theft\30-14-1702 Definitions.pdf

1. **How does Montana’s Data Breach Notification Statute define personal information?**

Answer

Under Montana’s data breach notification statute, personal information means an individual’s first name or first initial and last name, in combination with one or more of the following data elements, when either the name or the data elements are not encrypted:

• 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 Mont. Code Ann. § 33-19-104

• A taxpayer identification number –or–

• An identity protection personal identification number issued by the United States internal revenue service

Mont. Code Ann. § 30-14-1704(4)(b)(i).

Under the statute, personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Mont. Code Ann. § 30-14-1704(4)(b)(ii).

**RAG Response:**

Looking into the following states:

1. Montana

Montana:

Montana's Data Breach Notification Statute defines personal information as an individual’s first name or first initial and last name in combination with specific data elements, including social security number, driver’s license number, account numbers with access codes, medical record information, taxpayer identification number, or identity protection personal identification number. Personal information does not include publicly available information from government records. This definition is outlined in the Montana Code Annotated under Section 30-14-1704, in paragraphs (4)(b)(i) and (ii) of the statute (File: 30-14-1704 Computer security breach.pdf).

References:

1. Current Cybersecurity Law\Montana\Identity Theft\30-14-1704 Computer security breach.pdf
2. **Under what circumstances must disclosure of a data breach be made in North Dakota?**

Answer

North Dakota’s data breach notification statute requires disclosure following the discovery or notification of a breach of the security system. N.D. Cent. Code § 51-30-02.

**RAG response:**

Looking into the following states:

1. North Dakota

North Dakota:

Disclosure of a data breach in North Dakota must be made under the following circumstances:

1. Any person that owns or licenses computerized data containing personal information must disclose any breach of the security system to any resident of the state whose personal information was acquired by an unauthorized person.

2. If the breach affects more than two hundred fifty individuals, the person must also disclose the breach to the attorney general by mail or electronic mail.

3. Disclosure must be made without unreasonable delay, taking into account the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and restore the integrity of the data system.

References:

1. Current Cybersecurity Law\North Dakota\Data Breach Notification\51-30-02. Notice to attorney general and consumers.pdf

2. Current Cybersecurity Law\North Dakota\Data Breach Notification\51-30-03. Notice to owner.pdf

3. Current Cybersecurity Law\North Dakota\Data Breach Notification\51-30-04. Delayed notice.pdf

1. **What are the acceptable methods of notice of a data breach in Tennessee?**

Answer

Tennessee’s data breach notification statute provides that notice shall be made by one of the following methods:

• Written notice

• Electronic notice, provided that the notice is consistent with provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 or if the information holder’s primary method of communication with the Tennessee resident has been by electronic means

• Substitute notice as discussed below in Substitute Notice

Tenn. Code Ann. § 47-18-2107(e).

An information holder will be deemed in compliance with Tennessee’s data breach notification statute if it maintains its own notification procedures as part of an information security policy for the treatment of personal information, and is otherwise consistent with the timing requirements of the statute, provided it notifies subject persons in accordance with its policies in the event of a breach security system. Tenn. Code Ann. § 47-18-2107(f).

**RAG Response:**

Looking into the following states:

1. Tennessee

Tennessee:

The acceptable methods of notice of a data breach in Tennessee are as follows:

1. Written notice

2. Electronic notice, if consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 or if the licensee's primary method of communication with the consumer has been by electronic means, which may include email notification

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

- Email notice when the licensee has an email address for the consumer

- Conspicuous posting of the notice on the licensee's website, if the licensee maintains a website page

- Notification to major statewide media

References:

1. Current Cybersecurity Law\Tennessee\Insurance\Tenn. Code Ann. § 56-2-1006.pdf

2. Current Cybersecurity Law\Tennessee\Consumer Protection\47-18-2107. Release of personal consumer information.pdf

**Information Comparison Questions**

1. **What are the maximum penalties for failing to follow the data breach notification statutes in Ohio and Oklahoma?**

Answer

In Ohio, a person who fails to comply with the data breach notification statute can be fined up to $10,000 per day after the 90th day of noncompliance. Ohio Rev. Code Ann. § 1349.192(A)(1). In Oklahoma, an individual may be issued a civil penalty of up to $150,000 per breach of the security system. Okla. Stat. tit. 24, § 165(B).

**RAG Response:**

Looking into the following states:

1. Oklahoma

2. Ohio

Oklahoma:

The maximum penalties for failing to follow the data breach notification statutes in Oklahoma include fines up to $150,000 per breach incident. Repeat offenders may be subject to fines up to $250,000 per breach incident. In addition to fines, non-compliance can also result in injunctive relief and attorneys' fees.

References:

1. Current Cybersecurity Law\Oklahoma\Data Breach Notifcation\\_ 163. Disclosure of Security Breach\_Notice.pdf

2. Current Cybersecurity Law\Oklahoma\Data Breach Notifcation\\_ 165. Enforcement\_Authority to Bring Action.pdf

Ohio:

The maximum penalties for failing to follow the data breach notification statutes in Ohio are as follows:

- For each day of intentional or reckless failure to comply, a civil penalty of up to $1,000 per day for the first sixty days, and up to $5,000 per day thereafter.

- If the failure continues for more than ninety days, a civil penalty of up to $10,000 per day is imposed.

References:

1. Current Cybersecurity Law\Ohio\Data Breach Notification\\_ 1349.192.pdf

2. Current Cybersecurity Law\Ohio\Data Breach Notification\\_ 1349.19 Disclosure or notification of.pdf

The maximum penalties for failing to follow the data breach notification statutes in Oklahoma include fines up to $150,000 per breach incident, with repeat offenders potentially facing fines of up to $250,000 per breach incident. In addition to fines, non-compliance can also result in injunctive relief and attorneys' fees.

In Ohio, for each day of intentional or reckless failure to comply with data breach notification statutes, a civil penalty of up to $1,000 per day is imposed for the first sixty days, which can increase to $5,000 per day thereafter. If the failure continues for more than ninety days, a civil penalty of up to $10,000 per day may be imposed.

1. **What information must be provided in a data breach notification in South Carolina and Wyoming?**

Answer

South Carolina’s data breach notification statute does not provide specific guidelines concerning the contents of a notice of security breach. Wyoming’s data breach notification statute requires that notice be “clear and conspicuous” and, at minimum, include all of the following:

• A toll-free number to contact the person collecting the data, or his agent, and from which to learn the toll-free contact numbers and addresses for the major credit reporting agencies

• The types of personal 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, if reasonably possible to determine

• In general terms, actions taken by the individual or commercial entity to protect the system containing the personal 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 because of a law enforcement investigation, if reasonably possible to determine

Wyo. Stat. Ann. § 40-12-502(e).

**RAG Response:**

Looking into the following states:

1. Wyoming

2. South Carolina

Wyoming:

The information that must be provided in a data breach notification in South Carolina and Wyoming includes:

1. A toll-free number for individuals to contact the person collecting the data or their agent, along with toll-free contact telephone numbers and addresses for major credit reporting agencies.

2. The types of personal identifying information that were or are reasonably believed to have been the subject of the breach.

3. A general description of the breach incident.

4. The approximate date of the breach of security if that information is reasonably possible to determine at the time the notice is provided.

5. Actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches.

6. Advice directing the person to remain vigilant by reviewing account statements and monitoring credit reports.

7. 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.

References:

1. Current Cybersecurity Law\Wyoming\Data Breach Notification\Wyo. Stat. -º 40-12-502.pdf

South Carolina:

In South Carolina, the information that must be provided in a data breach notification includes:

1. The date of the cybersecurity event.

2. A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers.

3. How the cybersecurity event was discovered.

4. Whether any lost, stolen, or breached information has been recovered and if so, how this was done.

5. The identity of the source of the cybersecurity event.

6. Whether the licensee has filed a police report or has notified any regulatory, governmental, or law enforcement agencies and when such notification was provided.

7. A description of the specific types of information acquired without authorization, including types of medical information, financial information, or information allowing identification of the consumer.

8. The period during which the information system was compromised by the cybersecurity event.

9. The number of total consumers affected by the cybersecurity event in the state, providing the best estimate in the initial report and updating this estimate with each subsequent report to the director.

10. The results of any internal review identifying a lapse in automated controls or internal procedures or confirming compliance with automated controls or internal procedures.

11. Description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur.

12. A copy of the licensee’s privacy policy and steps outlined for investigating and notifying affected consumers.

13. The name of a contact person familiar with the cybersecurity event and authorized to act on behalf of the licensee.

References:

1. Current Cybersecurity Law\South Carolina\Insurance\S.C. Code Ann. § 38-99-40.pdf

2. Current Cybersecurity Law\South Carolina\Insurance\S.C. Code Ann. § 38-99-40.pdf

3. Current Cybersecurity Law\South Carolina\Insurance\S.C. Code Ann. § 38-99-40.pdf

The information that must be provided in a data breach notification in South Carolina and Wyoming includes:

1. A toll-free number for individuals to contact the person collecting the data or their agent, along with toll-free contact telephone numbers and addresses for major credit reporting agencies.

2. The types of personal identifying information that were or are reasonably believed to have been the subject of the breach.

3. A general description of the breach incident.

4. The approximate date of the breach of security if that information is reasonably possible to determine at the time the notice is provided.

5. Actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches.

6. Advice directing the person to remain vigilant by reviewing account statements and monitoring credit reports.

7. 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.

8. The date of the cybersecurity event.

9. A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers.

10. How the cybersecurity event was discovered.

11. Whether any lost, stolen, or breached information has been recovered and if so, how this was done.

12. The identity of the source of the cybersecurity event.

13. Whether the licensee has filed a police report or has notified any regulatory, governmental, or law enforcement agencies and when such notification was provided.

14. A description of the specific types of information acquired without authorization, including types of medical information, financial information, or information allowing identification of the consumer.

15. The period during which the information system was compromised by the cybersecurity event.

16. The number of total consumers affected by the cybersecurity event in the state, providing the best estimate in the initial report and updating this estimate with each subsequent report to the director.

17. The results of any internal review identifying a lapse in automated controls or internal procedures or confirming compliance with automated controls or internal procedures.

18. Description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur.

19. A copy of the licensee’s privacy policy and steps outlined for investigating and notifying affected consumers.

20. The name of a contact person familiar with the cybersecurity event and authorized to act on behalf of the licensee.

1. **Who must receive notice of a data breach in either Texas or Nebraska?**

Answer

Texas law requires notice of a breach of system security be given to any individual (including non-Texas residents) whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Tex. Bus. & Com. Code § 521.053(b). If residents of other states are affected by a breach, the statute provides that an entity subject to compliance may provide notice in accordance with that state’s laws or pursuant to Texas law. Tex. Bus. & Com. Code § 521.053(b-1). Any individual or commercial entity subject to Nebraska’s data breach notification statute must give notice to any Nebraska resident if an investigation determines that the use of information about the resident for an unauthorized purpose has occurred or is reasonably likely to occur. Neb. Rev. Stat. Ann § 87-803(1).

**RAG Response:**

Looking into the following states:

1. Texas

2. Nebraska

Texas:

In Texas, a person who conducts business in the state and owns or licenses computerized data that includes sensitive personal information must disclose any breach of system security to any individual whose sensitive personal information was acquired by an unauthorized person. This disclosure should be made without unreasonable delay and not later than the 60th day after determining the breach occurred. Additionally, if the breach involves at least 250 residents of Texas, the attorney general must be notified electronically with specific details of the breach within 30 days of its occurrence. The attorney general will then post a listing of notifications received on their publicly accessible Internet website.

References:

1. Current Cybersecurity Law\Texas\Business\Tex. Bus. & Com. Code § 521.053.pdf

2. Current Cybersecurity Law\Texas\Government\Tex. Code § 2054.603.pdf

Nebraska:

In Nebraska, if there is a data breach, notice must be provided to the affected Nebraska resident and also to the Attorney General. Additionally, if an individual or entity maintains data they do not own or license, they must give notice to and cooperate with the owner or licensee of the information regarding any breach of the security system. This includes sharing relevant information about the breach, excluding proprietary information of the individual or entity. The notice required by law enforcement agencies may be delayed if it will impede a criminal investigation, but must be provided in good faith without unreasonable delay once it no longer hinders the investigation.

References:

1. Current Cybersecurity Law\Nebraska\Financial\R.R.S. Neb. § 87-803.pdf

The Attorney General must receive notice of a data breach in either Texas or Nebraska.

1. **Who must comply with the data breach notification statute in Pennsylvania and Virginia?**

Answer

Under Pennsylvania’s data breach notification statute, any “entity that maintains, stores, or manages computerized data that includes personal information” is subject to the statute's data breach notification requirements. 73 Pa. Stat. Ann. § 2303(a).

Under the statute, an entity includes a ""State agency, a political subdivision of Pennsylvania, or an individual or a business doing business in Pennsylvania.” 73 Pa. Stat. Ann. § 2302. State Agency is defined as “any agency, board, commission, authority, or department of the Commonwealth and the General Assembly.” Individual is defined as a natural person. 73 Pa. Stat. Ann. § 2302. The term “business” includes a “sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered or holding a license or authorization certificate under the laws of [Pennsylvania], or any other state, the United States or any other country, or the parent or the subsidiary of a financial institution.” A business also includes any entity that destroys records. 73 Pa. Stat. Ann. § 2302.

Under Virginia's data breach notification statute, any individual or entity that owns or licenses computerized data that includes personal information is subject to the statute's data breach notification requirements. Va. Code Ann. § 18.2-186.6(B). For purposes of the statute, the term “entity” includes: Corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit.

Va. Code Ann. § 18.2-186.6(A).

**RAG Response:**

Looking into the following states:

1. Pennsylvania

2. Virginia

Pennsylvania:

Entities that maintain, store, or manage computerized data containing personal information must comply with the data breach notification statute in Pennsylvania and Virginia. State agencies, state agency contractors, counties, public schools, municipalities, and vendors are specifically outlined as entities required to provide notification of any breach of the security of the system involving personal information. This notification must be made to the affected individuals within specified timeframes, following the determination of the breach, in accordance with the relevant provisions outlined in the statutes.

References:

1. Current Cybersecurity Law\Pennsylvania\\_ 2303. Notification of the breach of the security of the system.pdf

2. Current Cybersecurity Law\Pennsylvania\\_ 2307. Notice exemption.pdf

Virginia:

Entities in Virginia that own or license computerized data containing personal information must comply with the data breach notification statute. This includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, whether for profit or not for profit.

References:

1. Current Cybersecurity Law\Virginia\Criminal\Va. Code Ann. § 18.2-186.6.pdf

2. Current Cybersecurity Law\Virginia\Insurance\Va. Code Ann. § 38.2-626.pdf

Entities that maintain, store, or manage computerized data containing personal information must comply with the data breach notification statute in Pennsylvania and Virginia. State agencies, state agency contractors, counties, public schools, municipalities, and vendors are specifically outlined as entities required to provide notification of any breach of the security of the system involving personal information. This notification must be made to the affected individuals within specified timeframes, following the determination of the breach, in accordance with the relevant provisions outlined in the statutes. In Virginia, corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, whether for profit or not for profit, that own or license computerized data containing personal information are also required to comply with the data breach notification statute.

1. **When do you have to provide notice to affected individuals of a data breach in California, Utah, Florida, and Michigan?**

Answer

Under both of California’s data breach notification statutes, notice to affected individuals must be made “in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement” or “with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” Cal Civ Code § 1798.82(a) and Cal Civ Code § 1798.29(a).

Under Utah’s data breach notification statute, notification must be made “in the most expedient time possible without unreasonable delay,” considering the legitimate investigative needs of law enforcement, after determining the scope of the breach of system security, and after restoring the reasonable integrity of the system. Utah Code Ann. § 13-44-202(2).

Under Florida law, notice shall be made as expeditiously as practicable and without unreasonable delay, but no later than 30 days after the determination of a breach or reason to believe that a breach has occurred. Fla. Stat. Ann. § 501.171(4)(a).

In Michigan, the statute provides that notice to affected individuals must be made without unreasonable delay. Mich. Comp. Laws Serv. § 445.72(4).

**RAG Response:**

Looking into the following states:

1. Florida

2. California

3. Michigan

4. Utah

Florida:

You have to provide notice to affected individuals of a data breach as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized under paragraph (b) or waiver under paragraph (c) in California, Utah, Florida, and Michigan.

References:

1. Current Cybersecurity Law\Florida\Consumer Protection\Fla. Stat. \_ 501.171.pdf

2. Current Cybersecurity Law\Florida\Consumer Protection\Fla. Stat. \_ 501.171(2).pdf

California:

To provide notice to affected individuals of a data breach in California, Utah, Florida, and Michigan, you must do so without unreasonable delay. California, Utah, Florida, and Michigan all have similar provisions regarding the timeline for providing notice of a data breach. References:

1. Current Cybersecurity Law\California\California Consumer Privacy Act of 2018\Files(46).pdf

Michigan:

You must provide notice to affected individuals of a data breach in Michigan when a person or agency that owns or licenses data included in a database discovers a security breach that is likely to cause substantial loss or injury, or result in identity theft. This notice must be provided without unreasonable delay and can be delivered through various methods such as written notice, electronic notice, telephone notice, or substitute notice if the cost exceeds a certain threshold. Additionally, notification to the media and major statewide media may be required in certain situations ("MCLS § 445.72," Sec. 12).

References:

1. Current Cybersecurity Law\Michigan\Commerce\MCLS \_ 445.72.pdf

2. Current Cybersecurity Law\Michigan\Insurance\MCLS \_ 500.559.pdf

3. Current Cybersecurity Law\Michigan\Insurance\MCLS \_ 500.561.pdf

Utah:

You must provide notice to affected individuals of a data breach in California, Utah, Florida, and Michigan after determining the scope of the data breach, restoring the reasonable integrity of the affected system if necessary, and without unreasonable delay, except as provided by law. Additionally, notification can be delayed at the request of a law enforcement agency if it may impede a criminal investigation, and the notification must include a description of the breach, the personal data accessed, steps taken to mitigate the impact, recommendations on protecting against identity theft, and any other language required by the Cyber Center. The notification methods include email, mail, text message, or telephone message, following specific guidelines based on availability and law, and additional steps should be taken if contact information is not readily available for more than 500 affected individuals.

References:

1. Current Cybersecurity Law\Utah\Government\Utah Code Ann. § 63A-19-406.pdf

2. Current Cybersecurity Law\Utah\Government\Utah Code Ann. § 63A-19-406.pdf

3. Current Cybersecurity Law\Utah\Government\Utah Code Ann. § 63A-19-406.pdf

To provide notice to affected individuals of a data breach in California, Utah, Florida, and Michigan, you must do so as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, identify individuals affected by the breach, and restore the reasonable integrity of the data system that was breached. This notice must be provided no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized under paragraph (b) or waiver under paragraph (c) in California, Utah, Florida, and Michigan.