**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).

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).

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).

1. **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.

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).

**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).

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).

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).

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).

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).