ARCHER
ATTORNEYS AT LAW

September 2017

Client Advisory

New Delaware Statute Expands Duties to Prevent and Report Data Breaches and Applies to Anyone Who Conducts Business in Delaware

Anyone who conducts business in Delaware - even if they are located outside that state - has until April 14, 2018 to comply with new requirements to protect personal information from data breaches and to meet expanding duties to give notice of those breaches under an Act recently signed into law by Gov. John Carney.

Consistent with recent trends in cybersecurity law, the Act requires persons who maintain certain types of personal and confidential information to take proactive measures to prevent data breaches. It requires persons who conduct business in Delaware to "implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business." The Act does not specify the measures that would qualify as "reasonable procedures and practices," presumably leaving it to be determined on a case-by-case basis if and as breaches occur.

The Act also expands the types of information that constitute "personal information" that is subject to protection under Delaware law. Maintaining the current requirement that "personal information" be associated with an individual's last name combined with their first name or first initial, the Act then provides a longer list than the current statutes of the types of non-public data that qualifies as "personal information." In addition to social security numbers, account numbers (such as payment card numbers) in combination with passwords or codes that permit access to the accounts, and driver's license numbers, the Act adds to the list passport numbers; state or federal ID cards; certain medical information and health insurance information; certain biometric and DNA data; tax ID numbers; and usernames or email addresses in combination with a password or security question and answer that would permit access to information that would give access to online accounts.

The Act encourages persons who maintain personal information to encrypt it. But, it also provides that the unauthorized acquisition of encrypted personal information is a breach of security triggering certain notice obligations if the unauthorized acquisition includes, or is reasonably believed to include, the encryption key.

The Act also tweaks aspects of the requirements that a person who suffered a data breach give notice to Delaware residents whose personal information is involved. Among other things, the new statute requires a person suffering the breach to provide notice within 60 days unless he investigates and reasonably determines that the breach is unlikely to result in harm. It also requires a vendor to whom personal information is disclosed to immediately notify its customers (commonly other businesses who collect personal information about their customers or employees) of a breach regardless of whether the vendor determines that the disclosure of the information created a risk of harm.

Finally, the Act requires persons who suffer a data breach to offer one year of free credit monitoring services to Delaware residents if the breach includes Social Security numbers.

If you have any questions about the Act or cybersecurity issues in general, please contact Archer's Privacy and Cybersecurity Group members Robert T. Egan at 856-354-3079 or regan@archerlaw.com or Mark J. Sever, Jr. at 856-354-3079 or msever@archerlaw.com.