Cooley

New Law Heightens Cybersecurity Requirements for Delaware Residents

October 4, 2017

On August 17, 2017, Governor John Carney signed into law bi-partisan legislation that increases cybersecurity protections for Delaware residents whose personal information may be compromised as a result of a data breach. **House Substitute 1 for House Bill 180** ("House Bill 180"), sponsored by Representative Paul Baumbach, is the first piece of legislation passed since 2005 to amend Delaware's data breach notification laws. The legislation will go into effect April 14, 2018. Baumbach **describes the law** as a "meaningful step forward in addressing [data] breaches so that we guarantee better protections for our residents and help them rebuild their lives after a cyber-attack." House Bill 180 implements additional notification requirements and focuses on identity theft mitigation services in the event of breaches involving social security numbers. It also imposes a requirement on companies holding personal information to implement reasonable security measures.

Heightened notification requirements

Delaware law already required that businesses who own or license computerized data that includes personal information provide notice of any breach of security to all Delaware residents if an investigation determines that the misuse of their personal information had occurred or is reasonably likely to occur. Notice was required to be made without unreasonable delay.

The new law requires that notice to residents *whose personal information was breached or is reasonably believed to have been breached* must be made no later than 60 days following discovery of the breach, except in limited circumstances. Moreover, if more than 500 Delaware residents are affected by a single security breach, notice must be given to the Delaware Attorney General. In such an event, notice to residents must be given no later than the time that notice is given to the Delaware Attorney General.

Expanded definition of personal information

Under the new law, the definition of "personal information" is expanded. Existing law defined "personal information" to include a resident's first name or first initial and last name combined with either a social security number, a driver's license number, or financial account information. The amendment expands this definition to also include resident's first name or first initial and last name in combination with medical information, health insurance information, biometric data, a user name or email address (with information sufficient to gain access to that account), passport number, and taxpayer identification number.

The full list of data elements, as amended, is below:

- 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.

Obligation to provide credit monitoring services

The law also requires that businesses provide reasonable identity theft prevention services and identity theft mitigation services, such as credit monitoring services, for no less than one (1) year, if the breach of security involves social security numbers. This makes Delaware the second state, behind California, to implement such a requirement. Such businesses must also instruct each affected resident on how to place a credit freeze on such resident's credit file. Delaware is only the second state, following Connecticut, to impose a legal requirement to provide identity theft prevention or mitigation services to individuals whose information may be compromised following a cybersecurity breach.

Private sector obligation to maintain security measures

Significantly, House Bill 180, which was drafted with the input of the state and various stakeholders, imposes an express and proactive data security obligation on private businesses, who are now required to implement and maintain reasonable procedures to prevent the unauthorized access and use of personal information collected. Daniel Eliot, the manager of Technology Business Development at University of Delaware's Small Business Development Center, which provides resources to small businesses in protecting against cybersecurity threats, **explained**, "It's a matter of fact: all businesses today are technology-based businesses and are vulnerable to cyber breach. We want to be sure Delaware's businesses are technologically and behaviorally prepared to combat such attacks." Delaware **joins several other states** (including Arkansas, California, Connecticut, Florida, Indiana, Kansas, Maryland, Massachusetts, Minnesota, Nevada, New Mexico, Oregon, Rhode Island, Texas and Utah) in imposing an affirmative legal obligation on the private sector to maintain reasonable security measures.

Conclusion

Delaware's enactment of House Bill 180 is the most recent example of states' continued focus on addressing cybersecurity threats. Delaware joins several other states in enacting additional safeguards to protect their residents affected by cybersecurity breaches. With the advances in cyber threats, we expect to see additional states evaluating their current data protection legislation. Cooley will continue to monitor state data protection legislation and will provide updates as they become available.

Cooley has significant expertise with cybersecurity regulatory issues. Our privacy & data protection practice is consistently designated as one of the best in the country. Please feel to reach to contact of the identified attorneys on this alert for more information or assistance with any of these issues.

is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. This content may be considered **Attorney Advertising** and is subject to our legal notices.

Key Contacts

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090
Kimberly Nguyen Reston	knguyen@cooley.com +1 703 456 8501
