Cybersecurity Enforcement Deadlines in the Wake of COVID-19

04/24/2020

While some regulations have been relaxed a bit to provide flexibility during shelter-in-place or other restrictive measures, one area that is generally not slowing down is privacy and cybersecurity. The past few years have seen a rollout of new privacy and cybersecurity measures at the state, federal and international level - and very few of those enforcement deadlines have changed. So what has happened since we've been home and what do we have to look forward to?

New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") *(deadline for data security requirements March 21, 2020)*

- The Act requires any person or company that holds private information of a New York resident, regardless of whether the person or company does business in New York, to adopt reasonable safeguards to protect the security, confidentiality and integrity of private information. There is an exception for small businesses of fewer than 50 employees, less than $3 million in gross revenues in each of last three (3) fiscal years, or less than $5 million in year-end total assets. These businesses may scale their data security program according to their size and complexity, the nature and scope of its business activities and the nature and sensitivity of the information collected. For most businesses, these safeguards include specific measures, including risk assessments, employee training, vendor contracts and timely data disposal.
- The SHIELD Act does not mandate specific safeguards. However, it does identify some examples of reasonable administrative, physical and technical safeguards. It is important to note that in addition to the measures we may be somewhat familiar with, all safeguards regardless of type include a risk assessment element from the effectiveness of current safeguards to information processing.
- The Act also broadens the definition of private information. The definition under the SHIELD Act now includes biometric information, user name and email addresses in combination with a password or security questions/answers. However, it also includes account numbers or credit or debit card numbers, even without a security code, access code or password if the account can be accessed without the codes or passwords.
- In addition to broadening the definition of private information, it also broadens the definition of breach which requires notification under the Act. A "breach of the security system" now includes unauthorized access of computerized data that compromises the security, confidentiality or integrity of private information rather than acquisition of the private information. Factors to consider include indications that the information was viewed, communicated with, used or altered by a person without valid authorization or by an unauthorized person. There is an exception to the notification obligation if disclosure was due to an inadvertent disclosure by persons authorized to access the private information and a reasonable determination is made that such exposure will not likely result

in misuse, financial or emotional harm to affected person. Documentation evidencing the determination must be maintained for at least five years.

- The penalty for violating the Act is a $20.00 for each instance of a failed notification with a cap of $250,000. There also a $5,000 per violation penalty for violating the data security standards that does not have a cap.

California Consumer Privacy Act ("CCPA") *(deadline for enforcement July 1, 2020)*

- In response to an open letter from a coalition of industry leaders to delay the enforcement of the CCPA, the CA Attorney General has not only declined to push back the July 1 deadline, but also emphasized data security in the current pandemic setting by recommending review of the types of information a business is collecting in response to COVID-19, such as employees health information. Under CCPA, employee health information is not subject to the exclusion of health information that is already subject to the Health Insurance Portability and Accountability Act ("HIPAA").
- CCPA applies to for-profit entities doing business in California, collects personal information and determines the purpose or means of processing the personal information (solely or jointly) and meets one of the three thresholds: (1) annual gross revenue in excess of $25 million; (2) on an annual basis, buys, receives, sells or shares personal information (alone or in combination) for commercial purposes of at lest 50,000 or more consumers, households or devices; or (3) derives at least 50% of its annual revenue from selling consumers' personal information. It is important to note that "households" and "devices" are not defined so could include data that is not linked to an individual. Businesses may be considered doing business if a business conducts online transactions with persons who reside in California.
- By July 1, companies are expected to: update categories of personal information and the definition of unique identifiers to address changes in technology, data collection practices, obstacles to implementation and privacy concerns and to address submitted requests to facilitate consumer requests for information; establish exceptions necessary to comply with state or federal law; establish rules and procedures regarding response to, compliance and providing consumer awareness of consumer opt-out requests; establish a process to adjust the annual gross revenue that determines whether a "business" is subject to CCPA to align with any increases in the Consumer Price Index each January of every odd numbered year; establish appropriate notice procedures to communicate to consumers (including those with disabilities) in an easy to understand manner; and establish rules and procedures regarding consumer or a consumer's agent's request for personal information to minimize the administrative burden on consumers.
- The CCPA includes a private right of action for consumers if their unencrypted or unredacted personal information is subject to an unauthorized access, exfiltration, theft, or disclosure because the covered business did not meet its duty to implement and maintain reasonable safeguards to protect that information. Statutory damages for this private right of action are $100-$750 per consumer per incident or actual damages, whichever is greater.
- The penalty for violating CCPA can be up to $2,500 per violation and not more than $7,500 for each intentional violation, subject to a thirty (30) day notice and cure period.

State Insurance Data Security Laws *(deadline for data security requirements: OH March 20, 2020; AL May 1, 2020; MS July 1, 2020; DE July 31, 2020; deadline for third-party service provider requirements: SC July 1, 2020)*

- The Insurance Data Security Model Law generally applies to individuals and non-governmental entities licensed, authorized to operate, registered or required to be licensed, authorized or registered pursuant to the state's insurance laws. It does not include purchasing or risk retention groups chartered or licensed in a different state or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction. The Model Law provides an exception for licensees that have fewer than ten employees, including independent contractors, as well as employees or other designees of a licensee who meet the definition of "Licensee" from the information security

program requirements of the act. Licensees subject to HIPAA that establish and maintain information security programs are considered to be compliant with the information security program requirements of the state law provided the licensee is compliant with the HIPAA requirements and submits a written certification of such compliance are also exempt from the information security requirements under the Model Law.

- The Model Law's information security program requirements include: assessing risk of potential threats and sufficiency of safeguards and policies (including employee training, information governance and management, and breach response and prevention); designing a program that mitigates the identified risks and includes determination regarding the use of specific security measures set forth in the Model Law; incorporating cybersecurity risks as part of the risk management process; staying informed on emerging threats; and providing cybersecurity awareness training. The Model Law also calls for oversight of the program by a licensee's board of directors, an incident response plan and for continued evaluation of the program. A licensee is also required to annually certify to compliance to the commissioner of its state.
- The Model Law incorporates oversight of third-party service provider arrangements. This oversight requires licensees to exercise due diligence in selecting third-party service providers and requiring these providers to implement appropriate administrative, technical and physical safeguards to protect information and systems that are held or accessed by the provider.

Because enforcement deadlines have not been delayed due to COVID-19, it is important to keep compliance efforts on track.