Insurance Coverage for Regulatory Penalties Resulting from a Data Breach

BY GABRIELLE KELLY

In November, Marriott alerted guests that its reservation system had been compromised and thieves had potentially stolen personal information on 500 million guests. The company vowed to quickly investigate and resolve the matter, and offered credit monitoring services to guests. While the breach was a first for Marriott, consumers are quite familiar with receiving a notice that their Personal Identifying Information ("PII") may have been stolen. Unfortunately, data breaches have become so common that various states and countries have implemented regulatory measures to protect citizens. Companies are, in turn, looking to their insurance policies to cover any regulatory fines or penalties in addition to the routine expenses of handling a data breach.

REGULATORS' RESPONSE TO DATA BREACHES

In response to the pervasive number of data breaches, new consumer privacy laws have been enacted to address the security of consumer information. The number of companies that are now subject to regulation has enhanced and reshaped businesses' potential exposure. The application of these new regulations are not limited to companies within their jurisdiction; in fact, the laws are much more far-reaching in that they target all organizations that handle or process PII of data subjects within the jurisdiction. This higher level of security compliance that has been adopted by the European Union is suspected to be the model for other jurisdiction's laws and could become the benchmark.

European Union

The most widely discussed response by regulators is the General Data Protection Regulation (GDPR), which was enacted by the European Union and went into effect in May 2018. Under the GDPR, organizations that hold or process personal data (ex. name, address, medical information, social networking posts, or any other information directly associated with an identifiable living person) must clearly disclose any data collection, state how long the data is being retained and if it is being shared with any third parties. Data subjects then have the right to request a copy of the data, and under certain circumstances, the right to demand that the organization delete their data. Further, companies must report any data breaches to regulators within 72 hours if the breach may have an adverse effect on user privacy.

If an organization is found to have violated the GDPR, the organization may be liable for fines of up to €20 million or 4% of a company's annual worldwide revenue, whichever is higher. The focus on the data and not the location of the company has implications for

© 2019 Cleveland Metropolitan Bar Association. Reprinted with permission.

organizations outside the EU that monitor, process, or hold information that would be considered EU-based data. In fact, many U.S.-based companies that operate in the EU or have data from persons in the EU would be subject to compliance with the GDPR.

California

After the passage of the GDPR, California enacted the Consumer Privacy Act of 2018. The Consumer Privacy Act (CCPA) is similar to the GDPR in many ways. First, the focus of the CCPA is on where the data is from instead of the location of the company. Second, Californians will have the right to know the PII that is being collected, whether the information is being sold, and the right to request deletion of their information. Additionally, the concept of personal information is broadly worded to include any information that "identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This definition goes beyond traditional PII to potentially include IP address or social media information. Lastly, the CCPA also imposes fines for violation of the law. The fines for violation of the CCPA, however, will largely depend on the number of records held by the company. Under the CCPA, each violation is fined up to $2,500 for negligent violations and $7,500 for intentional violations.

Colorado

In Colorado, a new law was enacted known as the Protections for Consumer Data Privacy Act that requires businesses of any size to do the following: have a written policy explaining how it will dispose of PII and follow through on the procedures, take "reasonable" steps to protect the PII that it keeps, and alert consumers of a data breach within 30 days, and alert the attorney general if more than 500 Coloradans are affected. Like the GDPR, a company may be liable for the actions of its third-party service provider. If a violation occurs, the Colorado Attorney General has authority to bring an action in law or equity, as well as other relief that may be appropriate to ensure compliance with the law.

INSURANCE COVERAGE REGULATORY FINES AND PENALTIES

Although cyber insurance has developed considerably from when it was first introduced to the market, cyber insurance policies are still not a universally standard form, but a type of insurance offered by insurers, whose terms and conditions vary from policy to policy. In general, though, cyber insurance protects against the typical costs associated with a data breach, such as investigation and notification expenses, credit monitoring and credit card re-issuing fees, data recovery, business interruption expenses, and liability for third-party claims. Since the regulations imposing fines and penalties for a data breach are a recent occurrence, it is unclear how cyber policies will respond to these costs.

In other types of insurance policies, coverage for fines and penalties has been viewed as being against public policy due to concerns of giving policyholders a way to lessen the blow for punishment that a court or agency bestowed on the company. And, criminal penalties are still considered uninsurable, but recently, there has been a shift in attitude to allow for coverage of presumably less reprehensible civil penalties when the amount was imposed by statute or there was no finding of a malicious, reckless, or intentional wrongdoing. Nonetheless, a review of local law and public policy principles would be necessary to determine whether such coverage provided by insurers would hold up in the legal systems of a particular jurisdiction.

While there is uncertainty on the insurability of regulatory fines, the shift away from a blanket denial of coverage for all fines and penalties is promising. And, insurers appear to be thoughtfully considering how to provide protection amid the changes in the landscape. Insurers are acknowledging the potential for coverage of regulatory fines under broad definitions of regulatory compliance that are included in the policy. Further, some insurers are writing specific provisions and endorsements designed to respond to GDPR and other regulatory fines. This does not guarantee that an insurer or others won't raise the insurability argument, but it is less likely that a policyholder will receive coverage, as parties in the insurance industry agree that these issues are far from settled.

Until there is routine enforcement of the regulations, policyholders and insurers will continue to grapple with the unresolved question of the insurability of data breach fines. In the meantime, companies should carefully review their internal cyber and other security controls, not only for compliance with government regulations, but also so that they can develop the best possible defense for the company's confidential and protected information. And, if they do not have coverage, companies should also strongly consider obtaining cyber insurance from their carriers, and ensuring that their business associates carry the appropriate insurance as well.

Gabrielle Kelly is an attorney at Brouse McDowell in its insurance coverage group where she represents policyholders in their disputes with insurance companies. She is recognized as a certified insurance coverage specialist by the State of Ohio. She has been a CMBA Member since 2007. She can be reached at (216) 830-6826 or gkelly@brouse.com.

© 2019 Cleveland Metropolitan Bar Association. Reprinted with permission.