LEGAL ADVISOR

A PilieroMazza Update for Federal Contractors and Commercial Businesses

When Hackers Attack: Disclosure Obligations and Litigation Risks When You Suffer a Data Breach

By Matthew Feinberg and Emily Rouleau

We are all familiar with the headlines: "Data Breach at Trusted Company Compromises Millions of Users' Personally Identifiable Information." Over the past few years, high-profile companies such as Marriott, Yahoo!, and Target Stores notified consumers that they suffered a data breach, exposing millions of customers' private information. There were nearly 1,500 reported data breaches in 2017 alone, affecting companies of all sizes over a wide range of industries. And, government contractors are not immune from the risk. So, what must you do and what must you be ready for when you have detected a data breach at your company?

There is no blanket federal law pertaining to data privacy and breach notifications for government contractors. But, that does not necessarily mean a government contractor has no duty to report a data breach. For instance, industry-specific laws may impose disclosure requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), which applies to contractors working with healthcare and health records. Individual agencies may also impose reporting requirements. In fact, in January 2017, the Office of Management and Budget (OMB) set minimum requirements for federal agencies to follow when responding to cyber breaches. And, agencies incorporate their own policies into awarded contracts. The DoD, for instance, requires contractors, by regulation, to report cyber incidents. And, the GSA is expected to formalize similar rulemaking over the next few months after relying on OMB's memorandum. Outside these requirements, government contracts may impose particularized data privacy and breach disclosure requirements as well, which may then flow down to subcontracts.

Currently, all 50 states maintain data breach laws. These statutes typically explain who must comply with the law, the types of information that must be protected, the type of data breach that requires notification, and the specific notification requirements that will apply. Some statutes also impose penalties or allow affected parties, or the state itself, to file lawsuits. Although the general concepts are the same, each state statute treats confidential information and data breaches somewhat differently.

In Virginia, for example, if unencrypted and unredacted personal information is accessed by an unauthorized person, whoever owns or licenses the personal information must disclose the breach to the Office of the Attorney General and any affected Virginia resident without unreasonable delay. If a breach affects the personal information of more than 1,000 people, the company also must notify consumer reporting agencies of the timing, distribution, and content of the notice. Notably, the Virginia statute provides the possibility for a lawsuit brought by the Commonwealth and potential civil fines of up to $150,000 per breach.

Similarly, Maryland's Personal Information Protection Act requires businesses that own or license a resident's personal information to maintain reasonable security procedures. When a business discovers a breach, it must conduct a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If, after investigating, the business determines that the breach created a likelihood that personal information has been or will be

Continued on page 2

PILIERO MAZZA

misused, it must notify individuals as soon as reasonably practicable, but not later than 45 days after conclusion of the investigation. If the company determines that notification is not required, it must record its determination and keep the record for three years. The business must also notify, without unreasonable delay, the Office of the Attorney General and, if more than 1,000 individuals must be notified, each consumer reporting agency. Violations of Maryland's law are considered unfair or deceptive trade practices, and individuals can bring an action to recover for injury or loss sustained.

For these reasons, the first step a company must take when facing a data breach is to engage knowledgeable counsel to guide the company through crisis management and internal investigation, assist with loss mitigation, ensure compliance with state laws, agency regulations, as well as prime and subcontract provisions, and make all required disclosures to the right parties at the right times. Compliance with agency regulations and contract requirements is particularly critical for government contractors, because the failure to make adequate disclosures of the data breach can result in potential liability under the False Claims Act. Contractors should also be ready to defend against a possible civil lawsuit from a state government or a class action from one or more affected parties.

Ultimately, a contractor will be best equipped to handle a data breach when it implements robust data privacy and security policies, understands the cybersecurity laws that apply to it, and maintains a relationship with a trusted legal advisor who can guide the company through the complex requirements of state laws, agency regulations, and federal contracts.

About the Authors: Matthew Feinberg is an associate in the Litigation, Labor and Employment Law, and Business and Corporate Groups. He may be reached at mfeinberg@pilieromazza.com. Emily Rouleau is an associate in the Government Contracts, Business and Corporate, Litigation, and Labor and Employment Law Groups. She may be reached at erouleau@pilieromazza.com.