Articles + Publications | October 16, 2023

Your Organization Has Suffered a Data Incident: Now Here Are the Regulators It Will Likely Encounter

WRITTEN BY

Stephen C. Piepgrass | Samuel E. "Gene" Fishel | Sadia Mirza

This article was originally published on October 16, 2023 in Reuters and Westlaw Today. It is republished here with permission.

Government regulators are seemingly as numerous as the stars nowadays, especially in the universe of data incidents. When organizations experience a data incident, they will need to quickly assess what happened, why it happened, and who (e.g., clients, consumers, vendors, employees) was affected. They will also need to chart a course by which they resolve the incident while limiting their legal exposure.

While they do so, they may attract the interest of regulators. As we discussed in part one of this series —"Data protection: One of these incidents is not like the other," Reuters Legal News and Westlaw Today, Aug. 24, 2023 — regulators take particular interest in a data breach when it involves sensitive data, a large number of consumers, or a vulnerable consumer demographic, among other factors. But who are these regulators? Here are the regulators most likely to come calling.

State Attorneys General

State attorneys general play a significant role in regulating data incidents at the state level, as they usually enforce their respective states' data breach related laws. Indeed, every state has breach-related laws, including data breach notification statutes, personal information protection acts, data privacy laws, or consumer protection acts. Some states, like Connecticut, Florida, Indiana, Massachusetts, and Texas are known for their particularly aggressive pursuit of breach matters. California stands alone with significant resources devoted to data regulation, including the relatively new California Privacy Protection Agency.

State AGs can impose fines and demand that organizations take corrective actions. Organizations that experience data breaches may end up facing multiple state AGs. Multistate involvement makes the regulatory landscape particularly complex, requiring careful coordination and compliance efforts.

To facilitate multistate investigations, state and territorial AGs often collaborate through the National Association of Attorneys General (NAAG). Breaches that are national in scope will often attract the attention of all 50 states, the District of Columbia, and U.S. territories. The AGs will then typically form an executive committee of two to seven states early in the process to lead the investigation, with the remaining states participating within a larger working group.

Whether a particular state AG takes a leadership role in an investigation often depends on where the organization that experienced the incident is headquartered, where it maintains significant operations, the number of impacted residents of a state, or the applicability of a state's laws in the context of the incident.

A multistate executive committee serves as the mouthpiece for the investigating states, which makes it easier from a practical standpoint for affected organizations to negotiate. The AGs within the working groups routinely meet among themselves to discuss ongoing investigations and strategize. With their collective goals in mind, executive committee member states will issue civil investigative demands and subpoenas to a subject organization, and seek to engage the affected organization's counsel, which may lead to settlement negotiations.

Although they coordinate investigations, every state AG has its own nuanced legal requirements, policy agenda, and even personality that organizations must navigate to effectuate a satisfactory resolution. And occasionally states will disagree on the best approach, leading some to break away from the multistate group and, as sovereign entities, commence their own investigations. Handling an investigation can therefore take months or years to resolve, particularly where large AG working groups are involved or where parallel state investigations are opened.

Federal Agencies

Besides state AGs, many federal administrative agencies may respond to data breaches.

To safeguard consumer data, the Federal Trade Commission (FTC) enforces various laws, including the Federal Trade Commission Act and the Health Breach Notification Rule. Upon a data incident, the FTC often investigates an organization's data security practices, incident response plan, and breach notification procedures. If the FTC believes an organization's actions (or inaction) contributed to the incident, it can mandate implementation of robust security measures and impose hefty fines if an organization fails to comply.

The U.S. Department of Health and Human Services (HHS), through its Office for Civil Rights (OCR), investigates breaches of protected health information (PHI), and may coordinate its investigation with state AGs, who also retain power under HIPAA (Health Insurance Portability and Accountability Act). When a health care entity suffers a PHI breach, it may need to report it to HHS and affected individuals. Depending on the severity of an incident and the extent of an organization's non-compliance, HHS can impose civil penalties and require corrective action to prevent future incidents and breaches.

The Securities and Exchange Commission (SEC) may investigate when a data incident affects a publicly traded company, as public companies must now (as of July 2023) disclose any "material" cybersecurity incident within four business days. Companies must disclose the material aspects of the incident and any material or potentially material impact on the company.

The Federal Communications Commission (FCC) investigates data incidents that affect internet and telecommunications services. The FCC's Privacy and Data Protection Task Force has been tasked with strengthening the FCC's rules for when and how internet and telecommunication providers notify consumers and federal law enforcement about data incidents.

Several other federal agencies, including the Department of Transportation, Federal Aviation Administration, and

the Department of Education may also inquire in the wake of a breach that affects entities within their purview.

Law Enforcement Agencies

In contrast to civil investigative authorities, law enforcement agencies may open criminal investigations into data incidents. Factors that prompt criminal investigation include the egregiousness of the incident and the amount of loss suffered by victims. Law enforcement goals include bringing a perpetrator to justice, protecting the public, and deterring future criminal conduct.

Both state and federal law enforcement agencies retain jurisdiction over data breaches and investigate under criminal statutes prohibiting fraud, hacking, and espionage among others. Such agencies may issue subpoenas and search warrants for computers that an affected organization maintains.

On the federal side, the Federal Bureau of Investigation (FBI) is highly active in investigating large-scale breaches. The United States Secret Service investigates breaches that involve financial transactions. And the Department of Homeland Security may investigate breaches with an international scope. Regardless of the federal investigating agency, if the investigation develops into criminal charges, the Department of Justice (DOJ), often through local U.S. Attorneys' Offices, will handle the resulting prosecution in federal court.

As a general rule, investigating agencies will often try to minimize the impact on business operations when executing criminal processes, particularly if the organization is not criminally at fault. This said, representatives of affected organizations should not necessarily mistake law enforcement deference for aligned interests. Beyond mandatory compliance with criminal process, organizations that cooperate with law enforcement must be careful to not disclose certain privileged information. Thus, organizations would be well-advised to consult legal counsel before talking to law enforcement.

Other Players

Some industry-specific state administrative agencies also may maintain jurisdiction over a data breach if a breached organization falls within their purview. For instance, state insurance bureaus may investigate a breach of an insurance company if they act as that company's primary regulator. Additionally, if a financial institution suffers an incident, various states' divisions of banking or finance may initiate investigations. But because state AGs often have more statutory weapons in their arsenal, they typically serve as a state's lead investigating agency, unless they are statutorily divested of jurisdiction via a grant of primary authority to another state administrative agency.

On the international front, a significant cross-border data breach will likely garner scrutiny from multiple international data protection authorities especially in the European Union, United Kingdom, China, and Mexico. International law enforcement agencies such as Interpol and the Royal Mounted Canadian Police may also initiate investigations. An organization's counsel in the United States should therefore work closely with international counsel versed in the pertinent country's laws to address overlapping issues and privilege concerns.

Finally, organizations must always be cognizant of potential class actions and multidistrict litigation. If a data incident is large enough, plaintiffs' firms may seek to quickly file such actions in its wake. Information is not always

shared between regulators conducting investigations and plaintiff's counsel pursuing parallel class actions, but organizations need experienced counsel who can balance confidentiality issues and cross-litigative risks as they negotiate these multiple paths forward.

The Regulators Are Interested in Talking; Now What?

Navigating the labyrinth of federal and state regulators in the wake of a data incident has become increasingly complex over the past two decades. Organizations must strike a balance between cooperation and self-preservation. Each regulator requires a unique approach that should be grounded in institutional knowledge and experience. Therefore, an organization must consult with experienced counsel early and often to favorably position itself relative to regulators.

Once lines of communication are established between an affected organization and an investigating regulator, several factors will determine a successful resolution. In part three of this four-part series, we will discuss these factors in detail and map out a successful strategy for handling data breach investigations.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber
- Regulatory Investigations, Strategy + Enforcement
- State Attorneys General