Articles + Publications | December 12, 2023

Navigating the Complexities of Regulatory Data Incident Investigations

WRITTEN BY

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

This article was originally published on December 12, 2023 in Reuters and Westlaw Today. It is republished here with permission.

It is indeed a tangled regulatory web woven to potentially trap an organization in the wake of a data incident. Navigating this web can involve significant resources, time, and stress. As we discussed in part two of this series, "Your organization has suffered a data incident: Now here are the regulators it will likely encounter," *Reuters Legal News* and *Westlaw Today*, Oct. 16, 2023, there is no shortage of regulators likely to come calling. Organizations therefore have little margin for error when assessing and responding to an incident.

Time and strategy are of the essence. Here are four tips for navigating data incident investigations to avoid the worst fates of the regulatory web.

Assess the incident immediately and identify potential regulators

A regulator will typically investigate a data incident when it occurs within its jurisdiction and involves some combination of aggravating factors. As noted in part one of this series, these factors include, among others, the size of the affected population, the sensitivity of the data breached, the demographic of the affected population, and the likelihood of consumer harm. It is therefore necessary that an affected organization, after it has contained the incident, quickly assess the nature of the incident and its scope to determine, among other things, those regulators that will likely be at play.

Importantly, jurisdiction among regulators will often overlap. For example, a data incident in which a bad actor accesses personally identifiable information of millions of consumers in 30 states may prompt those 30 states' attorneys general to investigate. A subset of these AGs may form a multistate group to further the investigation, with some or all interested states participating. Thus, depending on the incident and the tendencies of the state AGs involved, organizations may face one large multistate investigation, a series of individual ones, or a combination of both. In contrast, a smaller incident that affects a few hundred consumers in one state may only attract interest from that state's attorney general.

The type of information breached may also prompt action from state administrative agencies and federal authorities, in addition to state AGs. A breach of financial information held by a bank, for example, may prompt action from state financial regulators and the federal Securities and Exchange Commission. As discussed in our October 2023 article, other federal agencies like the Federal Trade Commission, the U.S. Department of Health

and Human Services (HHS) through its Office for Civil Rights, and the Federal Communications Commission may also investigate if they regulate the affected organization or data.

Organizations thus must be prepared to consider myriad regulators and address a data incident on multiple fronts.

Determine notification timing requirements at the outset

A top priority for regulators is to assess the timing of an organization's notice to affected consumers and regulators as part of its incident response. State laws vary greatly as to when an organization must provide such notice after a triggering data breach. Therefore, organizations need to know early on what state laws are implicated and the details of their statutory notification clocks.

Those clocks start ticking when the organization discovers the "breach," with most states requiring notification within 30, 45, or 60 days of discovery, or "without unreasonable delay." To comply with the stricter time limits, organizations should consider notifying appropriate regulators as soon as practicable, even if they have not fully determined the incident's scope. They then should provide supplemental notice to the regulator once they uncover additional pertinent details, along with notice to affected consumers containing all statutorily required information.

Proactively alerting appropriate regulators signals that an organization is taking a data incident seriously and acting with due diligence and speed. Notification timing should be top-of-mind for responding organizations.

Organizations must develop an incident response plan that alerts key stakeholders at the outset, such as company executives, insurance carriers, and in-house and outside counsel. Alerting counsel will help preserve legal rights and avenues as the investigation advances. Counsel should be privy to all relevant information contemporaneous to discovery of the incident so that they can effectively advise on the best course of action.

Legal counsel can guide an investigation and facilitate internal communications, which may blunt potential complications caused by inexperienced team members or shortcomings in a response plan. Most importantly, communication with counsel may be protected under the attorney-client privilege or other confidentiality protections that will prevent later disclosure. The organization can also potentially invoke such protections in parallel class actions or multi-district litigation derivative of the same incident.

Finally, experienced counsel can advise on those laws and regulations implicated in the incident's wake and properly assess each regulator that retains jurisdiction. State attorneys general, state administrative agencies, and federal regulators each require a tailored approach as part of the incident response.

Communicate often with regulators and determine their goals

Investigating government entities often have several goals when handling a data incident investigation, and it benefits an affected organization to determine those goals in an expedient manner. An overarching goal of regulators is to protect the public, including consumer interests, but other considerations such as advancing broad policy objectives and pursuing punitive measures may also materialize.

Several factors outside of the incident's facts will color how regulators approach a possible investigation. These can include the size (or notoriety) of the affected organization, how the organization has generally conducted itself in the wake of the incident, and the cybersecurity culture the organization fostered before the incident occurred.

To uncover these goals, an organization's counsel must engage with regulators consistently and ask penetrating questions to determine where the investigation is heading. This involves learning possible legal theories that may support potential claims, as well as the regulators' overall view of the facts. Regarding potential claims, regulators most commonly invoke consumer protection acts, consumer data protection acts, personal information protection acts, and data breach notification laws.

Along this vein, cooperation with the investigation is important to the extent the organization is not jeopardizing legal privilege and is preserving all defenses. This may lead to several meetings between the parties and presentations where both sides detail their positions. It often proves beneficial to the organization, as the longer an investigation lingers the greater the cost and the greater its liability exposure. It is thus essential that the parties work to maintain open lines of communication and that they set consistent and expedient deadlines throughout the process. A cooperative posture will likely move the case towards an amicable and satisfactory resolution.

Precedent reveals that most data breach investigations result in an agreed upon settlement. Settlement discussions often lead to a back and forth consisting of "redlining" draft agreements. While each case is different, regulators seek certain broad terms across all such agreements. They typically want affected organizations to provide remedial services to affected consumers, such as credit monitoring, and take reasonable efforts to publicize those services, such as by launching a dedicated website.

They also will require injunctive provisions generally aimed at improving organizational cybersecurity and information technology processes. Depending on the nature of the breach, they may also seek restitution for consumer damages. But in nearly every case they will press for a civil, monetary penalty. This monetary amount often corresponds to the size of the breach, the sensitivity of the breached information, and regulators' views of the level of culpability of the organization in failing to protect such data or failing to respond properly.

Regulators view larger breach incidents as an opportunity to establish precedent that shapes future data incident responses and settlements. To be sure, however, regulators will push forward with litigation should such settlement discussions break down, which undoubtedly raises the stakes for an organization.

By determining regulators' goals early and maintaining lines of communication, affected organizations can ultimately effectuate a resolution that is sufficiently narrowly tailored and prevents more severe consequences.

Conclusion

Navigating a data incident investigation is a complex undertaking. Preparing a response plan that includes assessing the incident promptly, identifying potential regulators, consulting counsel, evaluating pertinent laws, and communicating early and often with regulators, will position an organization to escape the regulatory web quickly and smoothly.

In the fourth and final installment of this series, we will discuss how data incident investigations conclude and how

organizations can forge a successful path ahead in their aftermath.

RELATED INDUSTRIES + PRACTICES

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