Newsflash | Technology

Navigating Privacy and Cyber Incident Notification and Disclosure Requirements

4 November 2019

Authors: F. Paul Pittman; Steven R. Chabinsky

Introduction

Fulfilling a company's data breach and cybersecurity incident notification and disclosure requirements is an increasing challenge. Companies operating across industry sectors and around the world must satisfy a wide range of statutory, regulatory and contractual requirements, often with differing thresholds, timelines and formats. This article offers six steps companies should consider when navigating this complex process.

Step 1: Understand the legal requirements

It is important at the outset to distinguish between a company's potential data breach notification obligations and other types of mandatory privacy and cybersecurity-related disclosures. A data breach notification requirement (whether as a matter of statute, regulation or contract) most commonly arises upon the loss or unauthorized access of a defined set of information. Prominent examples include data privacy breach notification laws (which apply to the loss of personal information) and contractual provisions (which often cover the loss of anything the parties define as "confidential"). Although data breach notification laws receive the greatest number of headlines, there are a number of emerging disclosure obligations that apply even in the absence of a data breach notification requirement. By way of example, the US Securities and Exchange Commission (SEC) issued interpretive guidance requiring publicly traded companies to affirmatively disclose material cybersecurity incidents of any nature (and regardless of breach notification requirements), as well as non-material incidents, when necessary, to effectively communicate potential risks. The SEC applies the same disclosure obligations for cybersecurity and privacy risks. As one would expect, regulators also are focused on the accuracy of privacy and security assurances when marketing their products and services. In the realm of consumer protection, the US Federal Trade Commission (FTC) has taken companies to task for misleading the public about privacy and data protection, including when companies represent "directly or indirectly, expressly or by implication" that they take reasonable steps to secure their products or services when, in the regulator's view, they have not.

With respect to the intricacies of personal data breach notification arising from a single incident, businesses have the misfortune of being subject to differing thresholds as to whether to report the breach, what to report, and to whom and under what time constraints to report it. Inconsistencies across the United States alone bring home the point. Because there is no overarching US federal data breach notification law, each of the 50 states has adopted its own statute. To prove the point, compare Minnesota, where data breach notification is required "without unreasonable delay" to residents and potentially "within 48 hours" to consumer reporting agencies, with Connecticut, which provides an outside window of 90 days to notify its residents. Odder still, Illinois prohibits businesses from letting victims know the number of residents that were impacted by a breach; Massachusetts prohibits letting victims know the nature of the breach or the number of residents affected; while to the contrary, California requires that breach notifications call attention to the nature and significance of the information. California even regulates the font size for a written notification! As for reporting thresholds, some state notification obligations may be triggered before others. State laws requiring notice when there is unauthorized "access" may trigger before laws requiring notice only upon the unauthorized "acquisition" of

personal information. In fact, the definition of “personal information” itself varies widely amongst the states, and globally for that matter, resulting in further variance across jurisdictions as to whether a “personal data breach” occurred. Because data breach investigations commonly take weeks (rather than hours or days) to conduct, significant forensic determinations may not be available when the first set of notifications go out, potentially leading to later reporting that materially contradicts initial reporting.

Outside the US, the vast majority of countries continue to establish or strengthen existing data breach notification laws. The emergence of the European Union’s General Data Protection Regulation (GDPR) has significantly expanded the data breach notification obligations of global organizations. Under the GDPR, a controller is required to notify the national supervisory authority or, if the matter is cross-border, the lead supervisory authority, of a personal data breach that presents any risk to the rights and freedoms of the data subject “without undue delay and, where feasible” within 72 hours of becoming aware of the breach. In addition, an organization must provide notice to individual data subjects where there is a high risk to their rights and freedoms. Since the GDPR broadly defines personal data as “any information related to an identified or identifiable natural person,” it occurs with some frequency that a breach triggers notification requirements in Europe, but not elsewhere.

Step 2: Understand potential liability

A company’s liability for failure to provide adequate breach notice, or to properly disclose prior or ongoing incidents, is as varied as the underlying obligations. In the US, in addition to the potential for breach of contract claims and consumer or shareholder civil class actions, multiple federal regulators and state attorneys general exercise substantial powers to enforce consumer and investor protection laws. To be sure, the harshest regulatory fines typically are meant to penalize companies for the breach itself, rather than the failure to notify. An exception to the general rule, however, exists when it comes to securities laws, where transparency is at a premium. In 2018, the SEC fined an internet service company US$35 million for its untimely disclosure of cybersecurity risks and prior security incidents in its public filings, as well as in its stock purchase agreement associated with the company’s anticipated purchase by a telecommunications firm. The SEC determined, among other things, that the company had inadequate controls and procedures in place to ensure proper disclosure.

In 2019, the SEC reached a US$100 million settlement with a social network company to resolve allegations that the company’s public disclosure indicated a hypothetical risk of improper access to or disclosure of user information at a time when the company actually knew that it had improperly sold data relating to tens of millions of users. As the SEC announced at the time, “Public companies must identify and consider the material risks to their business and have procedures designed to make disclosures that are accurate in all material respects, including not continuing to describe a risk as hypothetical when it has in fact happened.”

Financial fines are only one element of a regulator’s toolbox. When the FTC concluded that an IoT manufacturer’s product line failed to offer the “advanced network security” the company had claimed, the regulator planted its claws in the company for decades, requiring within a settlement that the manufacturer maintain a comprehensive software security program for 20 years (or get out of the market for selling IP cameras and routers).

In Europe, noncompliance with the breach notification requirements under the GDPR carries potential fines of *€10 million*or 2 percent of the companies’ total worldwide annual turnover of the preceding financial year, whichever is higher. Because this penalty for failing to provide proper notification may be substantial, an organization may find itself erring on the side of notification well before all of the facts are established, to include whether notification actually is required. Mindful that “full and comprehensive details of the incident may not always be available” within the 72-hour GDPR notification time frame, the European Data Protection Supervisor’s Guidelines include a notification template form allowing phased reporting in initial, follow-up and conclusive increments. The United Kingdom (UK) Information Commissioner’s Office (ICO) form allows controllers to submit reports without acknowledging a legal requirement to do so, either by declaring as their reason for submission that they are “unclear whether the incident meets the threshold to report,” or by affirmatively stating that reporting is not required but “I want you to be aware.” In 2018, the ICO fined a ride sharing company £385,000 based on a data breach where the company failed to notify the ICO or any other relevant regulator at the time, failed to notify any of the individuals whose personal data had been compromised, and failed to monitor affected users’ accounts or flag them for additional fraud protection at the time. In determining the penalty, the ICO specifically listed as an aggravating feature that “there was a significant delay in the Commissioner, and the data subjects, being notified of what had occurred.”

Step 3: Take into account business considerations

Considerations outside of the letter of the law create uncertainty for organizations attempting to determine whether and when to provide notification. Importantly, companies increasingly are having to balance non-legal considerations in determining whether and when to notify. In the current environment, lawmakers may scrutinize notification efforts for industry-leading companies entrusted with large amounts of consumer data. Typically, lawmakers only get involved where there is an incident impacting a significant number of consumers and public attention over an organization's data breach notification or disclosure. Consequently, the media response to an incident plays a critical role in raising awareness of both lawmakers and consumers. In this context, timeliness and content in accordance with legal requirements is of little concern to lawmakers who hold companies to a higher standard and expect faster notification. Lawmakers are also generally less familiar and comfortable with the technical aspect of an investigation than state and federal regulators who routinely handle and consider data breach notifications.

For example, in a recent high-profile US data breach the media and lawmakers chastised a company because the company waited six weeks after discovering a significant data breach to notify consumers. Yet, most breach notification laws in the US do not expressly require notification within 30 days of detecting an incident, and may not require notification until the fact of the breach has been determined with greater certainty. This example suggests that there is a lack of understanding by lawmakers and the public of the forensic investigation process and its importance and relationship to the notification and disclosure process. What emerges is a growing disconnect between the process for complying with legal notification and disclosure obligations and the expectations of the consuming public and lawmakers with regard to data breach notification. Consequently, organizations face uncertainty and often must exercise informed business judgment when developing a communications plan that provides a timely, controlled, consistent and accurate message that satisfies all stakeholders.

Step 4: Build flexibility into your communications plan

Typically, an organization will prepare a communications plan simultaneously with conducting an investigation. In a theoretical perfect world, communications are made only after the incident has been contained, the investigation completed, and the lawyers, marketing and business teams are consulted. However, regulatory requirements, public outcry, board inquiries, third-party disclosures and shareholder relations may dictate that an organization disclose the incident before the scope of the incident has been determined (indeed, perhaps before it is certain that an incident occurred). To the extent that an organization is required by law or circumstance to disclose an incident before it is fully aware of all of the facts, or before it has high confidence in the certainty of the initial forensic findings, the organization should be clear about its limitations, cautious about stating more than the minimum known facts demanded by the situation, provide assurances that it is taking the matter seriously and continuing to investigate it, and ensure that any misstatements are quickly corrected. In short, companies would do well to consider every communication along a continuum of minimal sufficiency with maximum flexibility on the one side and, on the other end, complete disclosure that locks down the company in ways that may prove costly, incompetent and difficult to correct should a new narrative develop over time.

Step 5: Incorporate risk management approaches

Organizations should be wary of focusing only on regulatory fines when determining whether and when to notify of a data breach, especially since in some instances the financial impacts associated with a data breach are unavoidable. For example, a public company's share price may be impacted by the disclosure of a data breach despite a well-prepared and timely disclosure that is compliant with notification and disclosure requirements. Sales teams need to prepare for the potential that competitors may seek to take advantage of an incident by approaching your customers.

As a result, a comprehensive risk management approach to notification and disclosure is necessary to balance regulatory and legal requirements, public and consumer perceptions, and lawmaker scrutiny. Effective risk management may require an organization to update and practice its incident response plan with a particular focus on its communications plan. Doing so better ensures companies identify incidents quickly and provide prompt notice with consideration given to the stage of the investigation and the certainty of findings. Incident response plans also would do well to consider internal communication strategies to employees and, for publicly traded companies, the need to put in place restrictions on insider trading while the

non-public facts unfold. The SEC specifically has noted that public companies should prepare an internal communications plan that prohibits the movement of any company stocks and take steps to limit the dissemination of information relating to security incidents to prevent leaks.

Step 6: Consider enlisting a forensics firms and outside counsel

As notification and disclosure obligations following a data breach continue to expand and become murkier, there is an ever-present need to have experienced forensic assistance, often engaged at the direction of outside counsel, to identify and ferret out the facts relevant to disclosure obligations, to prepare factual and legally sufficient statements, and to afford the benefits of attorney-client privilege to the fullest extent possible. As for this last point, organizations should approach their communications strategy with an eye towards potential litigation that may arise after a significant incident. In the midst of a fast-moving incident, there is no substitute for an experienced forensic firm and legal counsel when answering questions such as “has a data breach occurred here,” “is public notification required,” or “should I notify the regulator where the strict data breach notification requirements have not been triggered?”

Closing thoughts

Organizations are facing increasing uncertainty in assessing global notification and disclosure obligations and making a determination of whether to notify or disclose a privacy violation or security incident in today’s complex regulatory environment. Gone are the days where the timing of an organization’s notification was driven solely by the completion of a forensic investigation. Companies must consider what is legally required together with other important factors, such as potential scrutiny by lawmakers, public opinion, reputational harm and related financial impacts. These considerations—which fall outside of strict legal notification requirements—stress the organization’s ability to provide a timely, accurate and comprehensive notification, while retaining an appropriate degree of flexibility in the face of factual and regulatory uncertainty.

The importance of accuracy cannot be overstated. In most instances, the media rely on data breach notification press releases as a basis for reporting on the size and scope of an incident. In addition, plaintiffs’ counsel often use breach notifications to assess viable claims stemming from an incident and, in the US, typically attach these notifications to class action complaints. Unfortunately, given the dynamics between legal requirements and public and regulatory expectations, the key elements of timeliness and completeness are not always aligned. Regardless, the elements of timeliness and accuracy must remain aligned, even if any particular communication emphasizes the interim nature of the reporting and the uncertainty of the initial findings. Because of these tensions, organizations that are nimble, but have a firmly defined risk management and incident response process in place, will be best suited to handle the inevitability of an incident and the uncertainties that often accompany notification and disclosure requirements.

White & Case LLP
701 Thirteenth Street, NW
Washington, DC 20005-3807
United States

T +1 202 626 3600