Cybersecurity Data Breach Rule Compliance within Major Jurisdictions

Daily Journal | Journal Technologies

California data breach law – what you need to know

By Peter Stockburger

In 2003, California became the first state to adopt a data breach notification law. Since that time, every state has adopted a similar law although they differ in scope and application. The California data breach notification law requires covered persons and organizations to provide timely and thorough notice to California residents (and in some instances, law enforcement) in the wake of a data breach.

Below we highlight key features of California's data breach notification law, including the type of information covered, when notice is triggered, the substantive requirements for the notice, and enforcement trends.

General Overview

California's data breach notification law requires any person or organization conducting business in California and that owns or licenses "computerized data" that includes the personal information of California residents to provide notice in the event there is a discovery or notification of a "breach in the security" of the unencrypted personal information of California residents where there is knowledge that such personal information was acquired or is "reasonably believed to have been" acquired by an unauthorized person. (Cal. Civ. Code Section 1798.82(a)-(b).)

Type of Information Covered

Personal information is broadly defined under the statute to include information that: (i) can be used to commit identity theft (e.g., social security number, driver's license number, etc.); (ii) medical and health information; (iii) biometric information; (iv) online account information; and (v) data collected through the use or operation of an automated license plate recognition system. Publicly available information is excluded. (Cal. Civ. Code Section 1798.82(h)-(i).)

Notice Trigger

Notice is required upon discovery or notification of the "breach in the security" of the California resident's unencrypted personal information such that there is knowledge of acquisition or a reasonable belief of acquisition by an unauthorized person. (Cal. Civ. Code Section 1798.82(a).)

Timing of Disclosure

Notice must be provided in the most "expedient time possible" and without "unreasonable delay", consistent with the needs of law enforcement or any measures "necessary to determine" the scope of the breach and restore the "reasonable integrity" of the system at issue. (Cal. Civ. Code Section 1798.82(a).) This standard allows for flexibility and encourages law enforcement engagement.

Notice Requirements

The notice must be written in plain language and in a for-

mat designed to call attention to the nature and significance of the information contained in the notice. (Cal. Civ. Code Section 1798.82(D)(1)(A).) The notice must also contain the title "Notice of Data Breach" and the following headings, displayed in a clear and conspicuous manner: (i) "What Happened"; (ii) "What Information Was Involved"; (iii) "What Are We Doing"; (iv) "What You Can Do"; and (v) "For More Information". (Cal. Civ. Code Sections 1798.82(d)(1)(A)-(B).) The notice must contain, at a minimum, the following information:

1. The name and contact information of the reporting person or business;
2. A list of the types of personal information that were or are reasonably believed to have been the subject of the breach;
3. If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach; (ii) the estimated date of the breach; or (iii) the date range within which the breach occurred; and (iv) the date of the notice;
4. Whether the notification was delayed as a result of law enforcement intervention;
5. A general description of the breach incident, if possible;
6. A toll-free number and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or a California identification number; and
7. If the person or business providing the notification was the "source of the breach," an offer to provide appropriate identity theft prevention and mitigation services, provided at no cost to the affected person for no less than twelve months along with information necessary to take advantage of the offer.

(Cal. Civ. Code Section 1798.82(d)(2).)

Additional information may be provided in the notice, including: (i) information about what the person or business providing the notification has done to protect individuals whose information was breached; (ii) advice on steps that people whose information has been breached may take to protect themselves; and (iii) in breaches dealing with biometric information, instructions on how to notify other entities that used the same biometric data as an authenticator to no longer rely on data for authentication purposes. (Cal. Civ. Code Section 1798.82(d)(3).)

Notification to Law Enforcement

If the breach involves 500 or more California residents, notice must also be provided to the California Attorney General. (Cal. Civ. Code Section 1798.82(f).)

Enforcement

Individuals aggrieved by a violation of the California data breach notification law can seek damages in a court action, or seek to recover civil penalties. The state can also seek civil penalties.

Even if notice is not triggered under the California data breach law, it does not mean you're out of the woods.

4 Key Takeaways

- Encryption Is Key**.** Notification is not required if the personal information at issue in the breach was encrypted and the encryption key was also not compromised. What constitutes effective encryption may vary depending on industry.

- Consider Law Enforcement**.** In the event of a breach, involving law enforcement may allow more time to complete an investigation into the root causes and culprit behind a breach. Local, state, and federal law enforcement should all be considered in the wake of a breach.

- Even If There Is No Notice, There Still May Be Risk. Even if notice is not triggered under the California data breach law, it does not mean you're out of the woods. The California Consumer Privacy Act, as amended by the California Privacy Rights Act (CCPA), allows California residents to bring a private right of action if they believe the organization did not maintain reasonable security tracking the standard set forth in the California Records Act (CRA). Thus, even if notice is not triggered under California's data breach notification law, there still may be risk under the CCPA and CRA, requiring additional mitigation measures to be considered.

- Consider Overlapping Requirements. Complying with California's data breach notification law may not be the only breach notification requirement an organization faces. Often in the wake of a breach there are several overlapping notification requirements. Thus, it's important to consider other statutory and legal regimes when looking at breach notification requirements.

Peter Stockburger *is the managing partner at Denton's San Diego office.*

You've suffered a privacy breach. Now what? Learn about breach reporting and notification obligations in Canada

By Imran Ahmad, Travis Walker, and Suzie Suliman

In the private sector in Canada, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") governs the collection, use, and disclosure of personal information in the course of commercial activities, except in provinces where "substantially similar" legislation has been enacted. Currently, only three provinces - British Columbia, Alberta, and Quebec – have private-sector legislation, which qualifies as "substantially similar" to PIPEDA. As a result, privacy breaches impacting residents of Alberta, British Columbia, or Quebec are governed by provincial legislation, whereas those affecting residents of all other provinces and territories, or where the information at issue was transferred between provinces or internationally, are governed by PIPEDA.

So how do PIPEDA's breach notification and reporting obligations compare or differ from those requirements outlined in various provincial acts? Let's take a look.

PIPEDA

PIPEDA defines personal information broadly as "information about an identifiable individual," which can include an individual's name, address, date of birth, income, social insurance number, credit rating, etc.

In the event of a loss of unauthorized access to or unauthorized disclosure of personal information under an organization's control which results in a "real risk of significant harm," organizations subject to PIPEDA are required to report to Canada's federal privacy regulator (the Office of the Privacy Commissioner of Canada) and notify (1) affected individuals and (2) any third parties which may be able to reduce the risk of harm resulting from the breach such as law enforcement.

Several factors must be considered in determining whether the real risk of significant harm threshold has been met, including the sensitivity of the information involved and the probability that the information has been or will be misused. Significant harm encompasses a broad range of potential outcomes, including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, etc.

Where the threshold is met, organizations are required to notify and report "as soon as feasible," which should not be interpreted to invite delay, offering more flexibility than a number of US state laws and the EU's General Data Protection Regulation.

Notification to affected individuals can be carried out directly (via email, letter, telephone) or, in limited cases, indirectly (via website notice or similar public communication). The content of notifications is prescribed by regulation and

include:

1. Description of the breach;
2. Date or period in which the breach occurred;
3. Description of the personal information impacted;
4. Description of steps the organization has taken to reduce the risk of harm resulting from the breach;
5. Description of steps individuals can take to reduce the risk of harm resulting from the breach; and
6. Contact information of someone in the organization who can provide further information.

When reporting a breach to the Office of the Privacy Commissioner of Canada, organizations must provide the following:

1. The organization's contact information and that of someone who can answer questions on behalf of the organization;
2. Description of the circumstances of the breach;
3. Number of affected individuals;
4. Description of the personal information that is the subject of the breach;
5. Whether individuals have been notified, and if so, particulars of the notification; and
6. Description of steps the organization has taken to reduce the risk of harm resulting from the breach.

Alberta PIPA

Similar to PIPEDA, Alberta's provincial equivalent, the *Personal Information Protection Act*, requires a report to the provincial Privacy Commissioner "without unreasonable delay," where a privacy breach results in a real risk of significant harm. The Privacy Commissioner will then decide if affected individuals ought to be notified, but, in practicality, notification and reporting will often take place contemporaneously to avoid any harm resulting from administrative delay. Requirements for the contents of breach reports and notifications are largely similar to PIPEDA.

British Columbia PIPA

Under British Columbia's *Personal Information Protection Act*, notification to affected individuals and reporting to the provincial Privacy Commissioner is not mandatory but should be considered as part of the organization's risk mitigation strategy in response to a breach. If the organization elects to notify and report, the Privacy Commissioner's guidance is that both take place "as soon as possible" following discovery of the breach. Contents of the notifications and breach report once again mirror PIPEDA with some minor variations, including that individuals be informed of their right to complain to the Privacy Commissioner regarding the incident.

Quebec Privacy Act

Recent amendments to Quebec's *Act respecting the protection of personal information in the private sector* introduced mandatory reporting and notification obligations in the event of a "confidentiality incident" (i.e., privacy breach), which results in a risk of "serious injury." Factors to consider when evaluating the risk of serious injury are similar to those under PIPEDA's real risk of significant harm threshold, namely, the sensitivity of the information, the anticipated consequences of the use of the information, and the likelihood that the information has been or will be used for a harmful purpose. Content requirements for notifications to affected individuals are substantially similar to those under PIPEDA. When reporting confidentiality incidents to Quebec's Privacy Commissioner, additional information is required, including:

If the organization elects to notify and report, the Privacy Commissioner's guidance is that both take place "as soon as possible" following discovery of the breach.

1. The date on which the incident was discovered;
2. A description of the elements that led to the organization concluding there is a risk of serious injury; and
3. If applicable, other persons or bodies outside of Quebec that have been notified of the incident.

As this high-level summary was intended to depict, there are a number of statutory regimes that can be triggered in the event of a private sector privacy breach affecting Canadians. Most, if not all, of them are pertinent to large-scale breaches as they govern the most populous areas of the country. Organizations that have experienced a privacy breach should consult with a local privacy lawyer to ensure their reporting and notification obligations are properly met.

Imran Ahmad *is a partner at Norton Rose Fulbright's Toronto and Montreal offices.* **Travis Walker** *is a senior associate and* **Suzie Suliman** *is an associate at Norton Rose Fulbright's Toronto office.*

Compliance with the UK and EU rules on data breaches: do's and don'ts

By Eve-Christie Vermynck, Alistair Ho, and Robert Greene

Threats against data are one of the primary cybersecurity threats in Europe, according to the European Union Agency for Cybersecurity (ENISA). Cyber attacks are becoming more common and sophisticated, with stolen credentials, ransomware, and phishing attacks ranking as the main basis for data breaches. At the same time, cybersecurity insurance premiums are climbing and one of Europe's biggest insurance companies, Zurich, has even warned that certain cyber attacks may become uninsurable; many cybersecurity insurance policies already exclude ransomware attacks. This creates an increasingly challenging landscape to navigate, particularly as data breaches can result in significant financial, operational, reputational, and legal ramifications. In this article, we examine data breach preparation and response within the context of European data protection laws.

What Is a Personal Data Breach?

European data protection laws define 'personal data' as any information that relates to an identified or identifiable natural person. A personal data breach is widely defined as a "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*."

Preparation and Detection

Organisations are required to report notifiable personal data breaches to supervisory authorities within 72 hours of becoming aware of such breaches (see below). Given this tight timeframe, it is imperative that organisations have appropriate procedures in place to detect and respond to personal data breaches, including an incident response team. All employees should undertake regular data protection and cybersecurity training (including tabletop exercises) and be aware of how to identify and report incidents.

An effective incident response plan should detail, *inter alia*, the incident response team, scenario-specific responses, and the organisation's communication strategy. This plan should be regularly tested to identify areas for improvement, and copies should be kept offline in case an incident prevents system access. The incident response team should be cross-functional, escalate any findings to the board and have relationships with external stakeholders (e.g., forensic investigators, legal counsel, and ransomware negotiators).

Organisations are required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the personal data they

process. Such measures should include policies, plans, and procedures which enable the organisation to prevent, detect, respond to, and report personal data breaches.

Containment, Recovery, and Restoration

Where a personal data breach occurs, supervisory authorities will expect to see evidence of the actions taken to mitigate impacts on affected individuals. For sophisticated cybersecurity attacks (e.g., ransomware), an organisation should consider engaging cybersecurity experts to assist with containment, threat actor negotiations, and recovery and restoration of systems and affected personal data.

Notifications

Under European data protection laws, organisations are required to notify the "competent" supervisory authorities without undue delay and within 72 hours of "becoming aware" of a personal data breach, unless the breach is unlikely to result in a risk to affected individuals' rights and freedoms. The competent supervisory authorities will depend on the scope of the breach and the organisation's structure. However, supervisory authorities will expect the organisation to have appropriate measures in place to detect a breach in a timely manner. If an organisation fails to meet the 72-hour timeline, it must provide reasons for the delay.

The notification must detail the nature of the breach, the name and contact details of the data protection officer or other point of contact, the likely consequences of the breach, and the measures taken or proposed to address the breach. Where the full extent of a personal data breach is unclear, organisations can notify supervisory authorities in phases; *provided* that the required information is notified thereafter without undue delay. This may be necessary for more complex breaches where forensic investigation is required to fully understand the nature and scope of the incident.

Organisations are required to report notifiable personal data breaches to supervisory authorities within 72 hours of becoming aware of such breaches.

Communication of a personal data breach to affected individuals is also required (subject to certain limitations) without undue delay where the breach is likely to result in a high risk to their rights and freedoms. This is a higher threshold than the supervisory authority notification requirement.

Where an organisation fails to notify the competent supervisory authorities and affected individuals (if applicable), such supervisory authorities may take enforcement action, including the imposition of administrative fines up to £17.5 million/€20 million or 4% of the organisation's global annual turnover, whichever is higher.

Post-Breach Activities

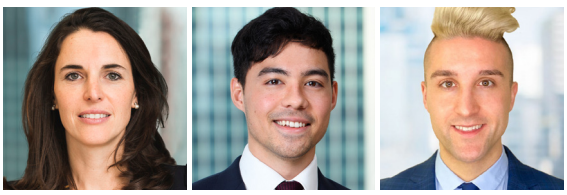
Cybersecurity experts may need to be engaged to conduct forensic investigations and data mining to determine how the attack occurred, how long the attackers were in the network, what systems and data were exfiltrated, which data subjects were affected, and whether the threat actor has been removed from the network. They can also assist with continued monitoring of the recovered or rebuilt network. These investigations will inform notifications to competent supervisory authorities and affected data subjects.

Organisations should produce a post-incident report to document actions taken and lessons learned, which is reviewed against the organisation's incident response plan to identify areas in need of improvement (e.g., training for employees, software patches, and cybersecurity testing).

The incident and actions taken must be documented. This documentation can be requested by supervisory authorities to verify compliance with applicable data protection laws.

Key Takeaways

As the volume of data produced and consumed worldwide continues to grow rapidly, data is increasingly seen as an engine for business growth. However, this explosive growth of data also presents risks for organisations, not the least of which is the threat from cybercriminals deploying increasingly sophisticated methods to access and exfiltrate such data. Organisations need to prioritise cybersecurity, particularly as personal data breaches are an enforcement priority amongst supervisory authorities. The UK Information Commissioner, John Edwards, recently warned that the "*biggest cyber risk is complacency, not hackers*."



Eve-Christie Vermynck *is counsel,* **Alistair Ho** *is an associate, and* **Robert Greene** *is a trainee solicitor at Skadden, Arps, Slate, Meagher & Flom (UK) LLP.*

The evolution of Florida's Information Protection Act

By John Carlin and Katherine Fang

Though cybersecurity issues and data breaches have drawn increasing public scrutiny, Congress has been unable to address them comprehensively. While it has passed piecemeal legislation – including the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA, 6 U.S.C. §§ 681-681g), which requires rapid reporting to the federal government for certain entities in critical infrastructure sectors – the lion's share of data breach regulation has been left to the states.

In this vacuum, all fifty states, including Florida, have enacted laws to address data breaches. Like the laws in other states, Florida's Information Protection Act's (FIPA) primary focus is to impose duties on entities to notify affected parties following a breach exposing personally identifiable information (PII).

Statutory Requirements

Since taking effect in July 2014, FIPA has required commercial and government entities, and their third party agents, to "take reasonable measures to protect and secure data" containing PII. (Fla. Stat. § 501.171 (2).) But the bulk of the statute is dedicated to setting forth procedures for notifying individuals, the state attorney general, and consumer reporting agencies in the event of a breach.

Generally – with some exceptions, including for ongoing criminal investigations or when a reasonable determination has been made that the breach will not result in harm – affected individuals must be notified within thirty days of a breach. (§ 501.171(3)-(4).) The state attorney general also must be timely notified of larger breaches involving more than 500 individuals (§ 501.171(3)), and consumer reporting agencies must be notified if over 1,000 individuals were exposed (§ 501.171(5)). Failure to comply with these requirements can result in a fine of up to $500,000 per breach.

FIPA and Other State Laws

Several aspects of the FIPA distinguish it from similar laws in other states. First, Florida is among only a handful of other states – including Colorado, Maine, and Washington – to require notification of affected individuals within 30 days. The rest of the states allow for longer timelines or simply require expeditious notification, without specifying a deadline.

Second, FIPA's scope remains unsettled in certain respects. For example, it is unclear whether the law was intended to foreclose common law causes of action, such as negligence. Courts addressing the interaction of statutory remedies for data breaches and common law remedies for

injuries in other states have reached different results. Pennsylvania and Massachusetts are likely to permit recovery for breaches under a negligence theory (*Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111-TSH, 2019 WL 7946103, at *22 (D. Mass. Dec. 31, 2019), *report and recommendation adopted*, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020) (noting that "there is support for Massachusetts to join the other state that permits recovery for economic losses in data breach cases" under a common law cause of action)), but Illinois does not (*Cooney v. Chicago Pub. Sch.*, 407 Ill. App. 3d 358, 363, 943 N.E.2d 23, 28 (2010) (finding under Illinois law no "'new common law duty' to safeguard information")).

Enforcement

Since FIPA's enactment, the attorney general has instituted compliance actions in a handful of cases. One successful settlement flowed from the 2017 Equifax data breach. (*Office of the Attorney General, State of Florida v. Equifax,* 2019 WL 4856098 (Broward Cir. Ct. 2019).) Along with a maximum of $425M in restitution for affected individuals across the country and $175M divided among participating state attorneys general, the ultimate settlement ordered Equifax to comply with FIPA and FDUTPA. It also imposed other remedial measures, including requiring an enhanced information security program and personal information safeguards. (*Id.*at *4, *14-*15, 21.) A similar settlement awarded $148M to several states' attorneys general, including Florida's, for Uber's 2016 data breach. (*State ex rel. Rosenblum v. Uber Techs.*, 2018 Ore. Cir. LEXIS 9714.) Notably, neither settlement required the companies to admit liability.

Several aspects of the FIPA distinguish it from similar laws in other states.

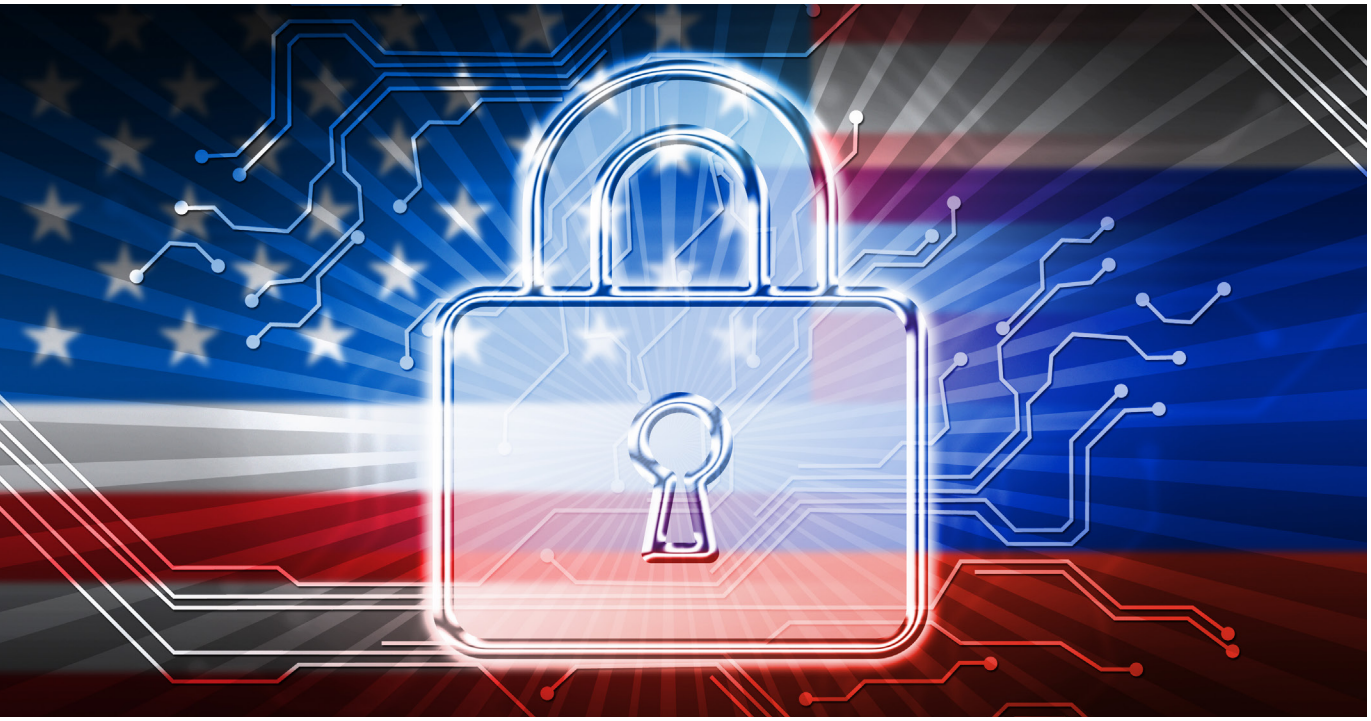
Private Actions

An interesting enforcement wrinkle arises in the context of individual claims. FIPA explicitly prohibits a private cause of action. (Fla. Stat. § 501.171(10); *see Owens-Benniefield v. Nationstar Mortg. LLC*, 258 F. Supp. 3d 1300 (M.D. Fla. 2017) (dismissing a case for failure to state a claim upon which relief can be granted); *Torres v. Wendy's Int'l, LLC*, No. 616CV210ORL40DCI, 2017 WL 8780453 (M.D. Fla. Mar. 21, 2017) (same).) But at the same time, its passage expanded the potential for private enforcement actions for data breaches by authorizing non-compliance to be a basis for an unfair or deceptive practice claim under the Florida Unfair and Deceptive Trade Practices Act (FDUTPA).(§ 501.171(10).) And the FDUTPA does permit private causes of action where plaintiffs meet statutory criteria. (*Samuels v. King Motor Co. of Boca Raton*, 782 So.2d 489, 499 (Fla. 4th DCA 2001); *Millennium Communications & Fulfillment, Inc. v. Office of the Attorney Gen.,* 761 So.2d 1256, 1263 (Fla. 3d DCA 2000).) One of these requirements is that plaintiffs prove actual damages.

While the interaction between the two statutes remains unclear, a recent class action in which the plaintiff alleged violations of FIPA – as enforced through the FDUTPA – survived a motion to dismiss in federal court. The defendant company had allegedly sent a misleading notice of privacy practices, indicating compliance with relevant laws, when it had in fact failed to implement adequate data security measures. (*Griffey v. Magellan Health Inc.*, No. CV-20-01282-PHX-MTL, 2022 WL 1811165, at *7 (D. Ariz. June 2, 2022) (citing Fla. Stat. § 501.171(2)).) The plaintiff's suit alleges that Magellan failed to "take reasonable measures to protect and secure data in electronic form containing personal information" as FIPA requires.

While FIPA's outer bounds remain to be fleshed out, developments such as those in *Griffey* indicate that courts are weighing whether to enable consumers to utilize the law to take action when companies fail to take the steps the law requires to secure PII, and to provide notice in the event of a data breach. Companies that wish to avoid liability should take heed of FIPA's requirements and consumer's rights in order to prevent future violations.

John Carlin *is co-head of the Cybersecurity & Data Protection practice and a partner at Paul, Weiss, Rifkind, Wharton & Garrison LLP's D.C. office.* **Katherine Fang** *is a law clerk at Paul, Weiss, Rifkind, Wharton & Garrison LLP's D.C. office.*



Did you suffer a data breach and what are your notice obligations?

By Alexandria Pritchett, Kamran Salour, and Edgar Vargas

Much like many aspects of life, when a business confirms it has suffered a data breach (not just an *incident* where the business would lack the statutory and potential regulatory notification obligations), the hardest part is sometimes figuring out where to begin. An effective response strategy involves a quick yet thorough assessment of key factors that affect a business' notification obligations. Implementing an appropriate response once a breach has been confirmed requires answers to fundamental questions: How did the incident or breach occur? Was the compromise contained? When did it happen? When was it discovered? What type of information was compromised? Who must be notified? When must notification be given? What constitutes adequate notice?

1. Identify the compromised information

Not all information is treated equally across the U.S. All 50 states, the District of Columbia, Guam, Puerto Rico, and the US Virgin Islands have adopted consumer notification statutes. States vary on how they define personally identifiable information (PII), and breach notification statutes may assign different requirements depending on the type of information exposed. For example, a state like Texas may clearly define PII as information that alone or in conjunction with other information identifies an individual, including an individual's: name, social security number, date of birth, or government-issued identification number; mother's maiden name; unique biometric data; and other identifiable and unique information as defined by Section 32.51, Penal Code. TX BUS & COM § 521.002(a)(1).

2. Identify Where the Impacted Individuals Reside

Because different states have different consumer notification requirements, an incident may not constitute a breach in all states.

3. Consider Industry-Specific Requirements

Additionally, some businesses must consider how federal law factors into identifying notification requirements for certain covered information. There is no omnipotent federal law that governs data breach notification requirements. Instead, several sectoral laws may impose notification obligations. Currently, there are federal laws that govern breach notification requirements in some industries such as: healthcare (*e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act), banking (*e.g.*, Gramm-Leach-Bliley Act (GLBA)), and government agen-

cies (*e.g.*, Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)).

4. Investigate How the Data Was Impacted

Businesses must consider another important wrinkle when analyzing whether notification is required under a specific statute. Most states describe a system's security breach as either the unauthorized *access* to or *acquisition* of unencrypted data containing personal information. *See, e.g.*, Conn. Gen. Stat. Ann. § 36a-701b(a)). When a state defines a breach of the security of a system to include the *acquisition* of personal information but does not include access to that information as part of the definition, then notification may not be required under that state statute. Consider New York's statute when determining whether personal information has been *acquired*: (1) the information is in the physical possession and control of an unauthorized person, (2) indications exist that the information has been downloaded, or (3) some type of evidence is found that the information was misused (*e.g.*, fraud, identity theft, etc.). N.Y. Gen. Bus. Law § 899-aa(2)(c).

Therefore, a full assessment of when and who must be notified post-breach should involve identifying the type of information compromised, whether that information falls into a category regulated by federal law, and determining how the compromised information is treated under applicable state laws.

5. Determine Who Receives Notice

Once a business determines the type of information compromised and the applicable federal and state laws, it is time to assess who must receive notice. This assessment will vary depending on the appropriate state and federal laws. There are three primary categories to consider: consumers, regulators, and credit reporting agencies.

For example, under HIPAA and HITECH, a covered entity and their business associates must notify affected consumers within 60 days and inform the United States Department of Health and Human Services (HHS). 45 C.F.R. § 164.404(b). However, if the breach affects more than 500 consumers, HIPAA requires that consumers and the HHS are notified simultaneously, in addition to notifying prominent media outlets in the relevant state or jurisdiction. 45 C.F.R. § 164.406(a); 45 C.F.R. § 164.408(b).

6. Assess Notice Requirements

Notification letters are often the first time a business communicates about a data breach to consumers, regulators, and the public.

In addition to complying with any notification requirements under state and federal data breach laws, businesses should also consider the following:

§ Personalizing the Message: The message should be tailored to the audience of the recipient. Sometimes that requires a thorough overview of the data breach. Other times, a more concise summary will suffice. Messaging an incident is a way to minimize the businesses' data breach notification obligations; messaging should be mindful of this premise.

Because different states have different data breach notification requirements, an incident may not constitute a breach in all states.

§ Avoiding Legal Opinions: Letters should be written in a concise and factual manner. Depending on the recipient, this is generally not the appropriate forum to admit or attribute fault to any parties for the data breach.

§ Streamlining the Communication Process: Businesses should consider a process for receiving and responding to consumer inquiries regarding a data breach. To prepare, businesses can create some general FAQs to assist in responding to consumers' queries. If consumers feel their concerns are not being addressed, they may seek to file a lawsuit or submit a regulatory complaint.

7. Stay Apprised of New Developments

Breach notification laws are constantly evolving, and the best way to craft an effective data breach response strategy is to create a plan that is up to date. States regularly update their breach notification requirements. Federal agencies also periodically update their breach notification requirements; for instance, the FCC recently released a notice of proposed rule-making for certain telecommunications carriers that collect certain customer proprietary network information (CPNI). Covered businesses will need to re-evaluate their data breach response plans in order to meet updated requirements. There's no better time to prepare for a data breach than now.

Alexandria Pritchett *is an associate*, **Kamran Salour** *is a partner, and* **Edgar Vargas** *is an associate at Troutman Pepper.*