Seeking Solutions:

Aligning Data Breach Notification Rules Across Borders

U.S. CHAMBER OF COMMERCE

HUNTON ANDREWS KURTH

U.S. CHAMBER OF COMMERCE

The U.S. Chamber of Commerce is the world's largest business federation representing the interest of more than 3 million business of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

HUNTON
ANDREWS KURTH

Hunton Andrews Kurth LLP is an international law firm with 1,000 lawyers serving clients in 100 countries around the world. The firm's Global Privacy and Cybersecurity practice is a leader in its field and has been ranked as a top law firm globally for privacy and cybersecurity.

I. Introduction

In an increasing number of jurisdictions around the world, lawmakers have enacted data breach notification laws that establish notice requirements in the event of a cognizable data breach. In countries that are considering enacting breach notification laws for the first time, legislatures logically would look to existing breach reporting regimes for guidance. What they will find is a global patchwork of requirements with different, and often conflicting, standards for notification. As lawmakers develop new, or amend existing, breach reporting requirements, the question of what constitutes an effective breach notification law is ripe for review and reconsideration.

There are several laudable reasons for enacting a data breach notification law. Requiring organizations to notify affected individuals about data breaches gives those who were impacted the information they need to take protective measures. Data breach reporting obligations promote accountability, transparency, and trust. At the same time, breach notification rules provide an effective means of regulating businesses' data security practices to prioritize the protection of consumer data and relevant systems.

This report highlights key differences and opportunities for convergence in existing data breach notification regimes. In some countries, for instance, a breach is notifiable only where it is likely to result in harm to affected individuals; in other countries, breach laws are triggered regardless of the potential risk or harm to individuals. Some jurisdictions require notification to the applicable regulator regardless of whether notification also is being provided to individuals; in others, regulator notification is triggered only if a specified number of individuals in the relevant jurisdiction have been affected by the incident. Despite the fact that a single security incident often has global implications, the current regulatory landscape is occupied by a mélange of data breach notification rules that differ widely based on geography and industry sector and result in variegated requirements even when applied to the same incident.

Effective breach reporting rules serve to protect affected individuals while enabling companies to operate efficiently in a global environment as responsible data stewards.

Seeking Solutions:

Given the ubiquity of data and the fact that a single incident can impact personal information about individuals from around the world, there is a need for international alignment on guiding principles and a harmonized approach for effective breach notification. Consistent reporting requirements would promote predictability and consistency for those affected by a breach. Similarly, a rationalized framework for breach reporting would help affected organizations by reducing the complexity associated with complying with varying reporting requirements across multiple jurisdictions. A streamlined approach would allow entities affected by a breach to focus their resources on the remediation of affected systems rather than devoting needless resources to precise legal compliance with the minutiae of potentially scores of different breach notification regimes globally.

This report identifies key principles to guide lawmakers who are considering enacting or amending a data breach notification law. Effective breach reporting rules serve to protect affected individuals while enabling companies to operate efficiently in a global environment as responsible data stewards. Adopting a risk-based framework while establishing clear and consistent guidelines ensures that affected individuals are notified and can focus on impactful events that reasonably may require or benefit from action on their part. It also helps regulators prioritize scarce resources on appropriately significant events.

This report proposes a breach notification framework that addresses the following fundamental questions to guide the development of an effective data breach notification law:

- What is a data breach?
- In what circumstances would notification of a data breach be required and to whom?
- When and how should notification of a data breach be provided?

The data breach notification framework outlined is designed to be replicated at scale and implemented in a culturally sensitive manner.

Framework for Effective Data Breach Notification Legislation

A framework for data breach notification legislation, or breach laws, should (1) protect affected individuals from harm resulting from a data security compromise and (2) promote responsible corporate information security practices. These principles support the adoption of risk-based, technology-neutral, and flexible requirements designed to protect individuals from real risks and focus scarce regulator resources on appropriately significant events.

Definition of Data Breach: The definition should be clear, intelligible, and sufficiently comprehensive to contemplate all types of data compromises that are of reasonable concern to individuals and that may be associated with different types of risk to individuals. In addition, the definition should be agnostic as to what security measures were in place to protect the affected personal data from compromise.

Definition of Personal Data: The definition should encompass those elements most likely to result in real risk to an individual. It should include exclusions for data that was securely altered from its original form.

Notification Harm Thresholds: Such thresholds should be included requiring notification only when there exists a reasonable likelihood of significant harm.

Timing Notification of Affected Individuals: A reasonable timing requirement reflects an appropriate and flexible timing standard for individual notification that acknowledges the practical challenges—and dangers—of imposing unnecessarily aggressive deadlines while setting reasonable expectations with a ceiling for the window of notification.

Regulator Notification: To enhance regulatory effectiveness, breach laws should require that regulators be informed of data breaches that are likely to raise considerable concern.

Law Enforcement Cooperation: In addition to addressing notification to relevant regulators, breach laws should consider the needs of law enforcement authorities in investigating an incident.

Method and Content of Notification: The permissible methods for notifying individuals should be designed to ensure that notifications make their way to affected individuals and are likely to be read, rather than lost or hidden.

Preemption: Breach laws should support uniformity and seek to align duplicative and overlapping compliance obligations by overriding or deferring to other notification laws in the same jurisdiction.

II. Current State of Data Breach Notification Regimes

a. Overview

From a global perspective, there is a cacophony of data breach notification rules that vary based on geography and industry sector. The requirements form a patchwork quilt of obligations that are not uniform even when applied to the same incident. Significant variations among many international breach notification regimes often result in conflicting standards, including with respect to the triggers for notification in the first place, which can add confusion and uncertainty.

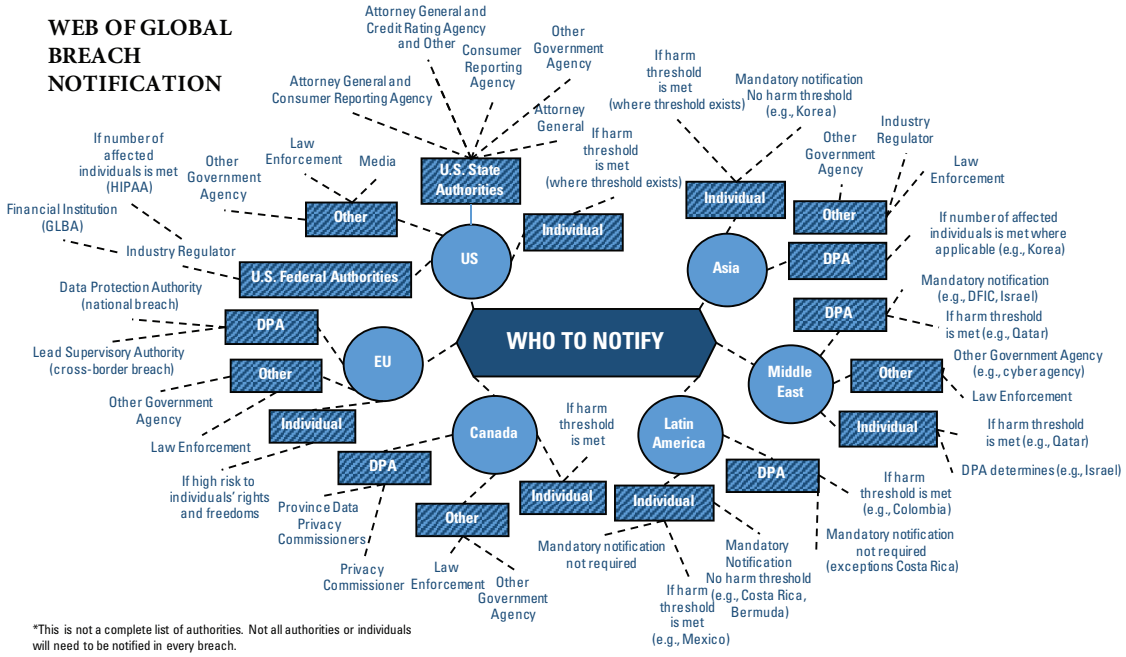
The definitions of fundamental terms such as "personal data" and "data breach" largely dictate the types of incidents that give rise to a notification obligation under the respective laws. Other provisions, such as those relating to the medium of the covered information (e.g., electronic data versus hard copy), harm thresholds, and notification timing and content requirements, differ significantly. This results in widespread variation as to whether notification is required, as well as how, when, and to whom it must be provided in a particular instance. For instance, certain breach laws limit the notification requirement to only those incidents that pose a risk of harm to affected individuals or exempt entities subject to other regulations regarding breach notification. Other breach laws require notification in the event of unauthorized access to personal data regardless of the likelihood of harm or the applicability of other similar rules. Such variation creates compliance challenges when a data breach involves multiple jurisdictions.

Significant variations among many international breach notification regimes often result in conflicting standards, including with respect to the triggers for notification in the first place, which can add confusion and uncertainty.

The varying defined terms and diverging standards for notification mean that a single event implicating multiple jurisdictions may trigger notification in some of those jurisdictions but not others. Determining whether notification is legally required pursuant to the varying global breach laws necessarily requires a fact-specific, time-consuming, and jurisdiction-by-jurisdiction analysis.

In the U.S., organizations experiencing a data breach typically must comply with the legal requirements of each jurisdiction in which an affected individual resides, rather than the law of jurisdiction in which the breach occurred or the organization is located. Outside the U.S., while residency of affected individuals is relevant in assessing the potential applicability of a breach notification law, the entity also must consider whether it is subject to the relevant legal regime.

From a practical perspective, given the differing (and frequently conflicting) notification standards to which a business may be subject in connection with a single incident, businesses often make notification decisions based less on what is required under each relevant law and more on reputational and business considerations. To the extent that notification requirements are triggered across multiple jurisdictions, organizations typically self-impose a higher standard than may be necessary by responding uniformly across impacted jurisdictions. This reality supports the need for a more harmonized breach notification standard that transcends jurisdiction-specific nuances and applies similar core principles for notification as described in this paper.



*This is not a complete list of authorities. Not all authorities or individuals will need to be notified in every breach.

Chart based on the following references:

Blackmore, Nicholas. "Mandatory Data Breach Notification Laws Spread across Asia Pacific." *Kennedys*, 3 Feb. 2018, www.kennedyslaw.com/thought-leadership/article/mandatory-data-breach-notification-laws-spread-across-asia-pacific.

Nel, Russell. "Privacy Tracker | GDPR Matchup: South Africa's Protection of Personal Information Act Related Reading: Perspective: The Vectaury Decision Is Not an Obituary for Ad Tech." *IAPP*, 5 Sept. 2017, iapp.org/news/a/gdpr-matchup-south-africas-protection-of-personal-information-act/.

"How to Notify Your DPA of a Data Breach." *IAPP*, iapp.org/resources/article/how-to-notify-your-dpa-of-a-data-breach/.

b. Examples of Current Regimes

In the last two decades, there has been a proliferation of data breach notification requirements around the world with wide variation depending on the jurisdiction. This section summarizes reporting requirements in various regions.

i. U.S.

In the U.S., although there is no overarching federal breach notification law, all 50 states plus the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have data breach notification laws. In addition, there are sector-specific breach notification requirements at both the federal level (e.g., Gramm-Leach-Bliley Act's Interagency Guidance[1] [GLB Interagency Guidance] for financial institutions and Health Information Technology for Economic and Clinical Health [HITECH] Act's Breach Notification Rule[2] in the health care context) and state level (e.g., breach notification requirements applicable to insurance providers and financial services companies). Although a number of state breach notification laws exempt organizations that are subject to the rules of a federal regulator, many state breach laws contain no such exemption and require businesses to comply with both state and federal rules.

The U.S. state breach notification laws generally define a security breach as an incident involving the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the business.

The U.S. state breach notification laws generally define a security breach as an incident involving the unauthorized acquisition of computerized data that

[1] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (Mar. 29, 2005) (codified at 12 C.F.R. pt. 30).

[2] Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,767 (Aug. 24, 2009) (codified at 45 C.F.R. pts. 160, 164). In January 2013, the U.S. Department of Health and Human Services announced the Final Omnibus HIPAA Rule, which, in part, modifies the breach notification requirements of the Interim Final Rule as of September 23, 2013. See Modifications to HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (January 25, 2013) (codified at 45 C.F.R. pts. 160, 164) (the "Breach Notification Rule").

compromises the security, confidentiality, or integrity of personal information maintained by the business. Some laws include unauthorized "access" in their definition of breach, whereby relevant personal information need not be "acquired" or exfiltrated by an unauthorized party to trigger the notification obligation. State breach laws typically define "personal information" as an individual's name in combination with certain other data elements, typically including an individual's Social Security number, driver's license number, or payment card or financial account number in combination with a required security code or password that permits access to that account. Many states have modified or are in the process of modifying the definition of personal information to include other potentially identifiable data elements, such as health or medical information, biometric information, date of birth, or an email address or username in combination with a password or security questions and answers to an online account.

As for a notification harm threshold, more than 40 of the state breach notification laws contain a harm threshold pursuant to which notification is not required unless harm (e.g., identity theft or fraud) to affected individuals has occurred or is reasonably likely to occur. In a handful of these states, additional notification (i.e., to a state regulator or law enforcement authorities) is required if an entity chooses to rely on the harm threshold.[3] With respect to regulator notification, more than 30 state breach notification laws have regulator reporting requirements. Approximately half of these are triggered only if a specified threshold number of affected residents are met.[4] The state regulator reporting requirements vary, seeking different content, formats (e.g., breach reporting form or letter), and means of delivery (e.g., online portal, email, fax, or postal mail). Some state breach notification laws require notification to multiple state agencies.

Nearly half of the state breach notification laws require notice to affected individuals within a certain number of days (e.g., 30, 45, or 60 days) of discovery of a breach, whereas others require notification "immediately," "in the most expedient time possible," or "without unreasonable delay". Approximately 10 state breach laws

[3] *See* Alaska Stat. § 45.48.090(c); Conn. Gen. Stat. § 36a-701b(b)(1); Fla. Stat. § 501.171(4)(c); S.B. 62, 93rd Leg. Sess. (S.D. January 23, 2018); Vt. Stat. Ann. § 2435(d)(1).

[4] *See* S.B. 318 (Ala. 2018); Ariz. Rev. Stat. § 18-552(B)(2)(b); Cal. Civil Code § 1798.82(f); Colo. Rev. Stat. § 6-1-716(2)(f); Del. Code Ann. tit. 6, § 12B-102(d); Fla. Stat. Ann. § 501.171(3); Haw. Rev. Stat. § 487N-2(f); Iowa Code § 715C.2(8); Mo. Rev. Stat. § 407.1500(2)(8); N.M. Stat. Ann. § 67-12C-6; N.D. Cent. Code § 51-30-02; Or. Rev. Stat. 646A.604(1)(b); R.I. Gen. Laws § 11-49.3-4(a)(2); S.C. Code Ann. § 39-1-90(K); S.B. 62, 93rd Leg. Sess. (S.D. January 23, 2018); Wash. Rev. Code § 19.255.010(15).

Seeking Solutions:

INDIVIDUAL NOTIFICATION TIMELINES

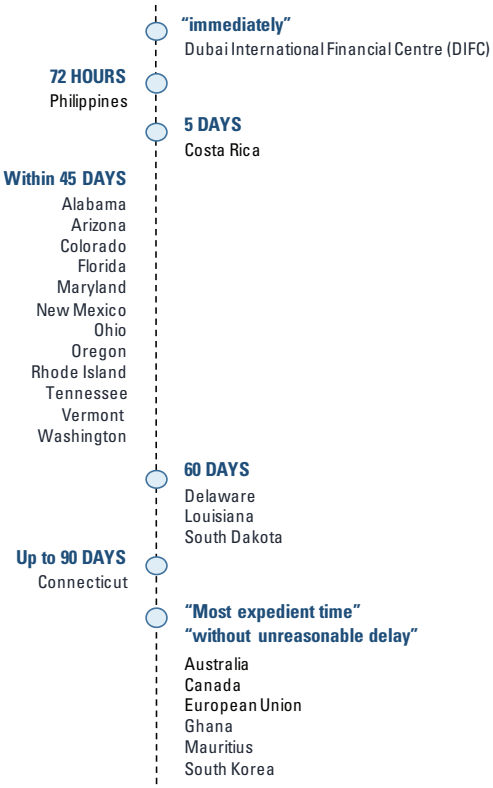


Chart based on the following reference:

"State Data Breach Notification Laws." *Foley & Lardner LLP*, 10 Sept. 2018, www.foley.com/state-data-breach-notification-laws/.

prescribe a specific number of days within which regulator notification must be provided (e.g., 10, 14, 30, 45, or 60 days of discovery), while others require regulator notice at the same time, or not later than, notification is provided to affected individuals. With respect to the substance of breach notification letters to affected residents, approximately 25 state breach laws impose specific content requirements.

At the federal level, standards for notification and respective timing and content requirements differ from those of state breach laws. For example, the HITECH Act's Breach Notification Rule defines a "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule], which compromises the security or privacy of the protected health information."[5] The term "protected health information" includes all individually identifiable health information transmitted by or maintained in electronic media or any other form or medium.[6] Under the GLB Interagency Guidance, when a financial institution becomes aware of an incident involving unauthorized access to or use of "sensitive customer information," the affected institution must promptly notify its primary federal regulator, regardless of whether the institution notifies its customers, as well as appropriate law enforcement authorities if the incident involves federal criminal

[5] Modifications to the Breach Notification Rule under HITECH Act, 78 Fed. Reg. 5638-5639, 5639 (January 25, 2013).

[6] *See* HITECH Act § 13400(12); see also 45 C.F.R. § 160.103.

violations that require immediate attention.[7] The institution also must notify relevant customers of the incident if the institution's investigation determines that misuse of sensitive customer information "has occurred or is reasonably possible."[8] As mentioned, many state breach notification laws are not preempted by federal law, adding to the complexity of compliance for affected organizations.[9]

ii. Canada

In Canada, effective November 1, 2018, the federal Personal Information Protection and Electronic Documents Act (PIPEDA) requires organizations to provide breach notification to affected individuals and the federal privacy commissioner if there is reason to believe the breach creates a "real risk of significant harm"[10] to individuals.

The relevant implementing regulations specify the content, form, and manner of breach notification and require notification as soon as feasible after determination that a breach has occurred. Breach notification in Canada historically has been governed at the provincial level with only Alberta's provincial data protection law imposing mandatory breach notification obligations across industry sectors, and certain other provinces imposing breach notification requirements for the compromise of health data.

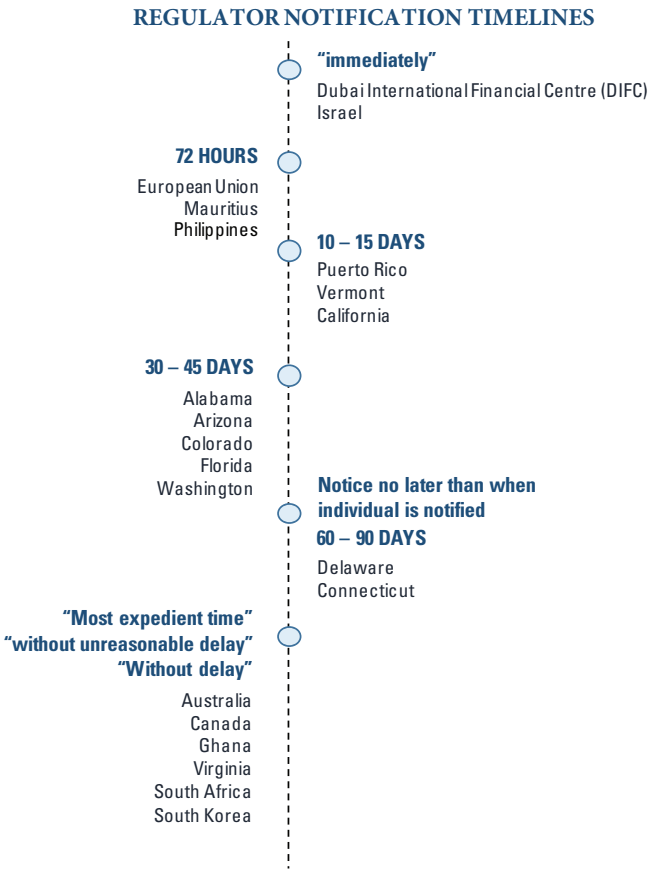


Chart based on the following reference:

Burg, Kelly. "Regulatory Watch List: Breach Notification Timelines in Proposed State Legislation." *RADAR*, 26 Feb. 2018, www.radarfirst.com/blog/regulatory-watch-list-notification-timelines-in-proposed-state-breach-notification-laws.

[7] 12 C.F.R. pt. 30, app. B, supp. A, § II.A.1; 12 C.F.R. pt. 208, app. D-2, supp. A, § II.A.1; 12 C.F.R. pt. 225, app. F, supp. A, § II.A.1; 12 C.F.R. pt. 364, app. B, supp. A, § II.A.1; 12 C.F.R. pt. 570, app. B, supp. A, § II.A.1.

[8] *Id.*

[9] In the U.S., in recognition of the need for uniform federal laws and in support of interstate commerce, the U.S. Congress often enacts legislation that preempts state law. One example of such a law is the federal Fair Credit Reporting Act. Congress currently is considering preemptive legislation in the data breach arena (e.g., H.R. 6743, known as the "Consumer Information Notification Requirement Act," passed by the U.S. House Financial Services Committee on Sept. 13, 2018, which would impose a federal, preemptive breach notification standard).

[10] Breach of Security Safeguards Regulations (PIPEDA), Ca. Gaz. Vol. 151, No. 35 (Sept. 2, 2017).

iii. European Union

In the European Union (EU), the General Data Protection Regulation (GDPR),[11] which took effect May 25, 2018, established a mandatory data breach notification requirement throughout the EU.[12] Prior to the GDPR's implementation, there was no uniform data breach notification obligation across member states, but certain member states enacted their own data breach notification rules. In some member states that had not passed breach notification laws, relevant data protection authorities issued guidance to organizations indicating that they should notify the relevant data protection authority of data breaches, such as the United Kingdom Information Commissioner's Office and the Office of the Data Protection Commissioner of Ireland.

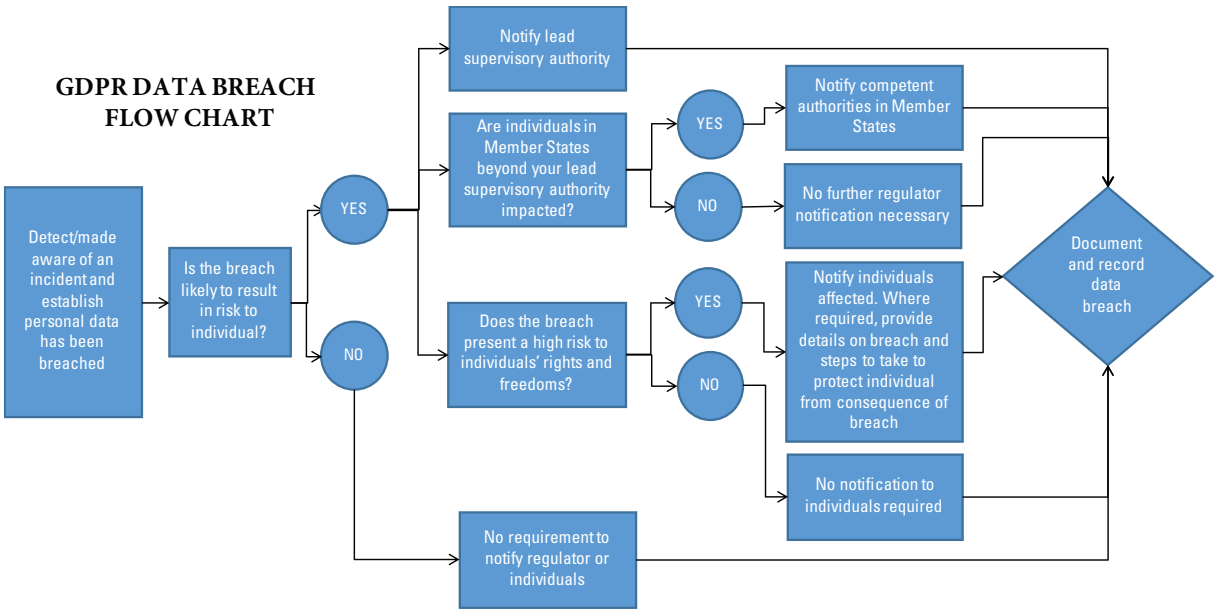
The GDPR introduced a risk-based standard for breach notification across the member states. A "personal data breach" is broadly defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed." The GDPR requires a data controller to notify the competent supervisory authority of a personal data breach and measures taken by the controller to address the breach unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.[13] A controller is required to notify affected *individuals* of a personal data breach only when the breach is likely to result in a *high risk* to the rights and freedoms of natural persons. The threshold for notifying individuals is higher than that for notifying supervisory authorities, meaning some breaches require notification to regulators but not individuals.

In addition to the GDPR's requirements, many member states have in place sector-specific laws that impose breach reporting requirements on covered organizations such as telecommunications providers. In addition, the EU Directive on the Security of Network and Information Systems (NIS Directive) requires operators of essential

[11] Regulation (EU) 2016/679 of the European Parliament and of the council of April 27, 2016, on the protection of natural persons with regard to processing personal data and the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[12] *See* GDPR Arts. 33 and 34.

[13] Such regulator notification is required without undue delay, and where feasible, not later than 72 hours after the relevant entity becomes aware of the personal data breach unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.



services and digital service providers to report to regulators those incidents that have a substantial impact.[14]

iv. Asia-Pacific

In the Asia-Pacific region, there has been a proliferation of data breach notification laws in recent years. Asia-Pacific jurisdictions that require breach notification include Australia, China, the Philippines, and South Korea. Some jurisdictions (e.g., India and South Korea[15]) have breach notification rules for specific sectors, such as financial institutions or information technology companies. As of the date

[14] The European Commission required that the member states enact national laws implementing the NIS Directive by May 9, 2018, but the majority of member states had yet to do so by the date of this writing.

[15] South Korea has both an omnibus breach notification requirement in its comprehensive data protection law (known as the Personal Information Protection Act) and a sector-specific breach notification law applicable to "telecommunications business operators." The standard for telecommunications companies is found in the Act on Promotion of Information and Communication Network Utilisation and Information Protection (IT Network Act).

of this writing, India is considering a legislative proposal for a comprehensive data protection law that would include an omnibus data breach reporting requirement. Singapore similarly is considering a mandatory breach notification requirement, which is not part of its current data protection law.

The breach notification rules in the Asia-Pacific region are not uniform and differ by country and industry sector. The notification requirement is triggered in the Philippines when an entity has a reasonable belief that personal data was acquired without authorization. Australia's breach notification law is triggered when a breach is likely to result in serious harm to an affected individual, whereas South Korea's breach notification law does not contain a harm threshold. In addition, although most Asia-Pacific jurisdictions require both individual and regulator notification when an incident triggers the applicable breach law, South Korea's omnibus breach reporting rule requires regulator notification only when 10,000 or more individuals are affected. Timing requirements for notification likewise vary by jurisdiction (e.g., regulator notification is required within 72 hours in the Philippines), while other jurisdictions (e.g., Australia) do not impose a precise deadline and instead require notification "as soon as practicable."

v. Latin America and the Caribbean

With respect to Central and Latin America, although several countries have comprehensive data protection laws, relatively few have mandatory breach notification requirements. Countries with such obligations include Mexico, which requires notification to affected individuals without delay in the event of loss, theft, or unauthorized disclosure, access, use, processing, modification, damage, or destruction to personal information that materially affects the property or moral rights of the affected data subject. Mexico's law does not require regulator notification.

In Colombia, in contrast, the law requires notification to the data protection authority regarding security breaches that pose a risk in the processing of personal information, but it does not require individual notification. In Brazil, the legislature enacted a comprehensive data protection law (which becomes effective on February 15, 2020) that includes a requirement to notify the data protection authority and, in some circumstances, affected individuals in the event of a breach. While breach notification to affected individuals or regulatory authorities is not required in Argentina, the country's data protection law obligates organizations to maintain a ledger of data breaches, which the data protection authority is entitled to inspect upon request.

Timing for notification also varies. Costa Rica requires individual notification within five business days of the entity becoming aware of a breach (defined as an "irregularity" in the processing or storage of personal data, such as loss, destruction, theft, or misuse) and requires the entity to notify the data protection authority of the breach, although there is no explicit deadline for regulator notification.

Even fewer countries in the Caribbean require breach notification. A recent example is in Bermuda, which enacted a data protection law that requires notification first to the relevant regulatory authority, and then to affected individuals, in the event of a breach of security leading to the loss or unlawful destruction or unauthorized disclosure of or access to personal information that is likely to adversely affect an individual.

vi. Africa and the Middle East

In Africa and the Middle East, relatively few jurisdictions have mandatory breach notification requirements. In Africa, both Ghana and Lesotho generally require notification as soon as reasonably practicable to affected individuals and the data protection authority where there are reasonable grounds to believe that personal data has been accessed or acquired by an unauthorized person. South Africa's comprehensive data protection law, which passed in 2014, includes a substantially similar requirement that, as of the date of this writing, had not yet become effective. Mauritius also has a comprehensive data protection law with a breach notification obligation substantially similar to the one in the GDPR.

In the Middle East, Israel, Qatar, and the Dubai International Financial Centre (DIFC) all impose mandatory breach notification obligations. Israel's breach notification law requires owners of databases designated within an "intermediate" or "high" tier of security to report data breaches to the relevant regulator, that in turn may require the database owner to notify affected data subjects. In Qatar, the data controller must notify the regulator and affected individuals if it is likely that the breach caused or will cause damage to affected individuals. In the DIFC, regulator notification is required in the event of an unauthorized intrusion into any personal data database; individual notification is not required.

Seeking Solutions:

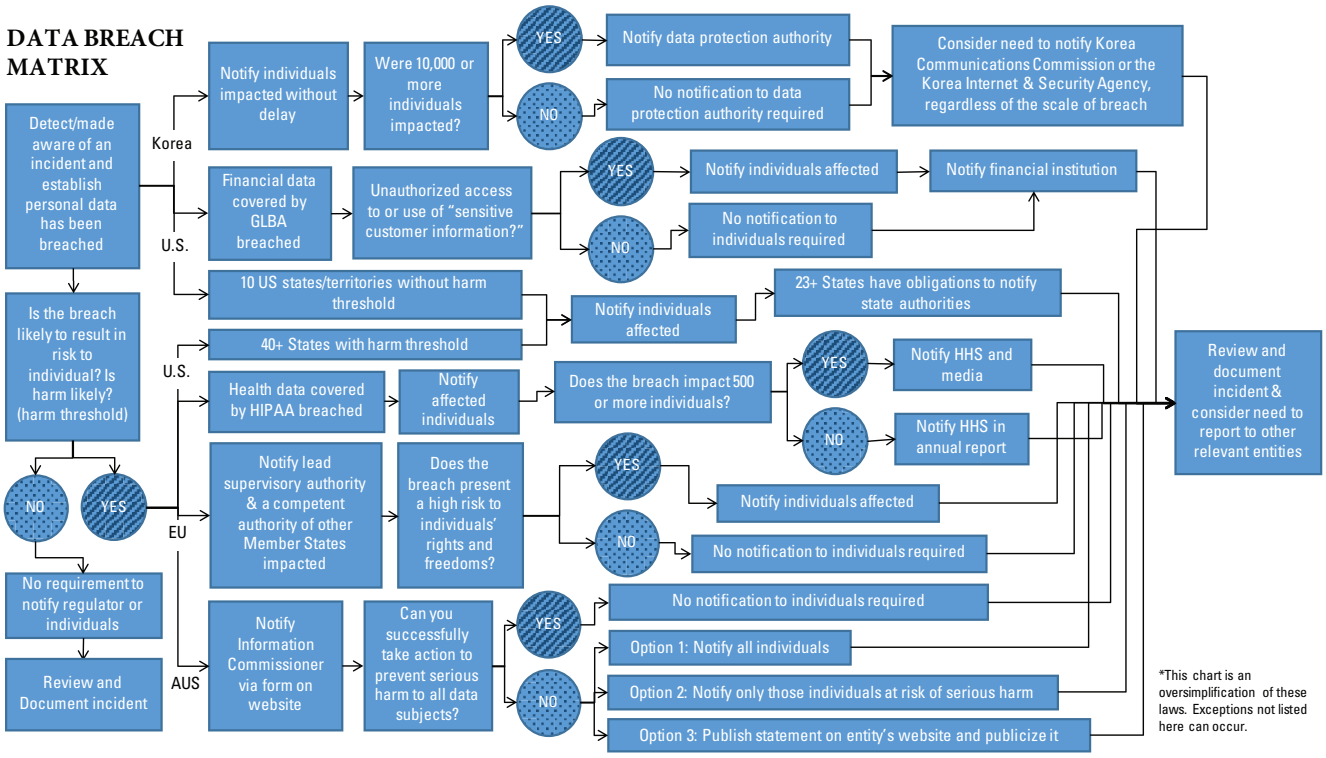


Chart based on the following references:

HHS Office of the Secretary,Office for Civil Rights. "Breach Notification Rule." *HHS.gov*, US Department of Health and Human Services, 26 July 2013, www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

"How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act." *Federal Trade Commission*, 7 Jan. 2015, www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm.

"PIPA Compliance | South Korea Personal Information Protection Act Compliance ." *Thales*, www.thalesesecurity.com/solutions/compliance/apac/south-koreas-pipa.

III. Framework for Effective Data Breach Notification Legislation

This section offers a framework for data breach notification legislation, or breach laws, that is designed to (1) protect affected individuals from harm resulting from a data security compromise and (2) promote responsible corporate information security practices. Given the disparate cultures, regulatory regimes, and legal structures around the world that influence the nature and scope of a jurisdiction's breach laws, and understanding that the laws themselves will differ based on these distinct factors, the framework provided here is intended to be used as a guide by governments in all jurisdictions that are creating or updating their breach laws. The framework is grounded in core, guiding principles that will enable localized versions of the breach laws to share common themes and objectives. This will increase predictability and consistency in the interpretation and enforcement of global breach laws, while enhancing protections for individuals. These principles support the adoption of risk-based, technology-neutral, and flexible requirements that are designed to protect individuals from real risks and focus scarce regulator resources on appropriately significant events.

These principles support the adoption of risk-based, technology-neutral, and flexible requirements that are designed to protect individuals from real risks and focus scarce regulator resources on appropriately significant events.

The framework described in this paper contemplates broad and comprehensive definitions of key terms, such as "data breach" and "personal data," that encourage businesses to think holistically about breach notification and data security and avoid focusing solely on financial harms (e.g., identity theft and fraud) that do not adequately cover the breadth of risks that individuals may face in connection with a compromise of their data. Although the framework encourages the adoption of sufficiently expansive defined terms, it envisions a harm threshold that limits the types of incidents that must be reported to regulators and affected individuals to meaningful events that reasonably may benefit from or require action on the part of the regulator or individual.

In addition to taking into account the harm threshold that tempers both the regulator and individual notification requirements, the framework recommends that a breach

law require regulator notification only if a certain number of individuals are affected by the incident. This threshold is premised on an acknowledgment that the over-reporting of data breaches is not neutral. To the contrary, it has the effect of straining the already scarce resources of regulators, which impairs their ability to protect individuals through a concerted focus on the most impactful breaches. As to timing, the framework provides that a breach law should impose reasonable deadlines for notification that ensure the timely provision of notice to affected individuals while avoiding the real risks associated with premature notification.

Here are the framework's guidelines for developing each of the fundamental components of an effective breach law.

Definitions of Key Terms

The first—and arguably most important—element of a breach law is its definitions of key terms such as "data breach" and "personal data." Clear and unambiguous definitions reduce uncertainty for organizations in determining when a situation requires them to investigate and potentially provide notification of a security issue.

i. Data breach

The definition of a "data breach" is the touchstone that establishes which types of compromises are notifiable. Below are guidelines for developing a definition of data breach:

1. The definition should be sufficiently comprehensive to contemplate all types of data compromises that are of reasonable concern to individuals (e.g., the theft, misuse, or loss of personal data) and that may be associated with different types of risk to individuals.[16] Identity theft, account fraud, and other financial risks alone are not the only threats about which individuals may be concerned.

[16] For example, theft of personal data could lead to an individual suffering discrimination, identity theft or fraud, financial loss, or reputational damage. Likewise, the loss or unauthorized alteration of critical data may place an individual's safety or health at risk or result in economic disadvantages if the data are tampered with or unavailable. In some cases, the same breach could affect the confidentiality, integrity, and/or availability of the data. For instance, the accidental loss of a laptop could compromise the confidentiality and availability of personal data stored on the device to the extent that the data is neither encrypted nor backed up or copied. Similarly, an incident involving accidental or unauthorized alterations to personal data maintained in a company database could compromise both the integrity and availability of the data to the extent that the original state of the database cannot be restored.

A broad definition should be tempered for notification purposes by a harm threshold as discussed later in the text.

2. The definition should be written in plain and intelligible language, free from legal jargon. This would allow entities to focus on the general nature of a compromise and its potential ramifications in determining whether a data breach occurred, rather than requiring them to inconsequentially assess whether specific types of actions took place or make sense of ambiguous legalistic terms. Breach laws that complicate the definition of a data breach force businesses unnecessarily to grapple with nuanced technicalities, such as distinguishing between "unauthorized acquisition or acquisition without valid authorization"[17] or interpreting when "unlawful access" has occurred.

Clear and unambiguous definitions reduce uncertainty for organizations in determining when a situation requires them to investigate and potentially provide notification of a security issue.

3. Unlike many existing breach notification laws that predicate notification upon occurrence of a "breach of the security of a system," the definition should not require a breakdown in security or a failure to implement safeguards as a prerequisite to the occurrence of a notifiable breach. Rather, the definition should be agnostic as to what and whether security measures were in place to protect the affected personal data from compromise.[18] Such prerequisites often can be difficult to understand in practice and lead to confusion when determining whether a reportable data breach occurred. Indeed, many security breaches occur despite the fact that there were strong (or any) security measures in place.

4. To assist entities in understanding when a breach has occurred, the breach law (or supporting guidance) should provide illustrative examples of events

[17] *See, e.g.*, N.Y. Gen. Bus. Law § 899-AA(c). ("Breach of the security of the system shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business.")

[18] An exception is when the data that is suspected of compromise is rendered unreadable (i.e., via tokenization or encryption) so that there is no significant risk of harm.

or factors that would suggest a compromise has occurred. This reduces uncertainty in identifying a potentially notifiable data breach. For example, such guidance should clarify that anomalous activities on systems or networks, alerts from security monitoring tools, or detection of cybersecurity vulnerabilities alone are not sufficient to constitute a notifiable compromise.

Based on the foregoing guidelines, a data breach might be defined as "a compromise to the confidentiality, integrity, or availability of personal data maintained by the organization." Upon identification of a data breach, a company would conduct an investigation to determine whether the incident triggers a notification obligation. A data breach would be notifiable only if it meets the relevant harm threshold discussed here.

ii. Personal data

The second key term to define is "personal data." The scope of covered information is critical because it effectively determines the types of harm from which the breach law will protect individuals. For example, a breach notification law should include in its definition of personal data those elements most likely to be used by criminals to commit identity theft or financial fraud. It also should include other information concerning an individual (e.g., an individual's biometric information), which if compromised could also result in real risk to an individual (e.g., physical safety).

Breach laws should apply to information that is personally identifiable, whether alone or in combination and association with data elements held by the entity. Some guidelines for developing a definition of personal data include:

1. The definition of personal data should be tempered by a harm threshold with respect to notification obligations (as discussed in the next section).

2. The definition should reflect the reality that, even when information alone does not directly identify an individual, such information often can be easily combined or associated with other data elements to reveal an individual's identity. Technological advances and the ability to combine disparate pieces of data can lead to the identification of a data subject even when the individual elements of data alone do not identify a person.[19] For example, in the EU,

[19] *See* Federal Trade Commission (FTC) report, *Protecting Consumer Privacy in an Era of Rapid Change* (dated March 2012) at 20.

Recital 30 to the GDPR asserts that "natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers, or other identifiers such as radio frequency identification tags. This may leave traces which, in particular, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

3. Similarly, the U.S. Federal Trade Commission believes that "[i]n many cases, persistent identifiers, such as device identifiers, MAC addresses, static IP addresses, and retail loyalty card numbers" amount to personally identifiable information.[20] These policy positions recognize that certain types of data (e.g., medical data, government-issued identifiers, financial data, and payment card details) can alone be used to cause harm, while other types of data require being combined or supplemented with additional data to facilitate identity theft or other harm. Both forms of data potentially should be subject to notification obligations, subject to harm thresholds (as discussed later). A broader definition of personal data with notification based on a harm threshold supports efforts to harmonize breach notification requirements at the global level by reducing uncertainty and promoting consistency as to the scope of data covered by breach laws, while avoiding the need to continuously amend the definition to address changes in technology and contemplate evolving data collection practices.

4. Given the broad range of personal data that potentially would be covered by breach laws, the definition of personal data should envision exclusions for data that was securely altered from its original form. Specifically, breach laws should include a safe harbor for personal data that is encrypted, exempting an entity from providing notification of a breach of encrypted data to the extent the encryption was not compromised. The breach law also should include exceptions for personal data that was adequately de-identified,[21] pseudonymized (e.g., through hashing, masking, or other pseudonymization techniques), or truncated and for information that is publicly available. To

[20] *See* S. Waterman, FTC's Ramirez: *New Tech's Complexity Leaves Privacy Basics Unchanged* (dated August 23, 2016), Fedscoop, *available at* https://www.fedscoop.com/edith-ramirez-ftc-aspen-institute-august-2016/.

[21] The breach law should provide clear guidance as to what constitutes "de-identified" data.

promote a future-proofed and adaptable standard, the exclusions should be technology neutral and avoid being prescriptive as to the requisite types or levels of encryption, pseudonymization, or de-identification methods. In offering an exception for encrypted or pseudonymized data, breach laws should call for the data handler to ensure that the data is adequately protected such that it is reasonably indecipherable and inaccessible to an unauthorized party. This incentivizes businesses to take steps to ensure that the personal data is encrypted or otherwise protected using an industry-standard methodology, the methodology is applied properly to protect the data, and the relevant decryption key or pseudonymization methodology remains secure.

Notification Harm Thresholds

An effective breach law promotes responsible data protection practices that help keep individuals' data safe by hinging the notification trigger on the potential for harm or risk to individuals. Tempering a notification requirement with a harm threshold helps limit the number and frequency of events that trigger notification, which helps avoid the undesirable and dangerous effects of over-notification such as inundating regulators and individuals with notices of breaches, which neither protects individuals from real threats nor provides regulators or affected individuals with useful information.

The harm threshold should take into account both the severity and likelihood of harm to individuals, requiring notification only when there exists a reasonable likelihood of significant harm.

On the other hand, a breach law that results in the under-disclosure of harmful breaches puts individuals at risk. Breach laws should promote safety and transparency, warning individuals of actual risks and providing them with information necessary to take steps to reduce the possibility of harm. They also should help individuals make more informed and safer consumer choices by shining a light on companies that mishandle information or fail to employ reasonable safeguards to protect data.

With this balance of interests in mind, breach laws should require notification only when an entity determines that a breach resulted or is reasonably likely to result in a material risk of harm to the affected individuals. The harm threshold should take into

account both the severity and likelihood of harm to individuals, requiring notification only when there exists a reasonable likelihood of significant harm as a result of the data breach. Notice obligations should not be triggered when the likelihood of harm to individuals is merely theoretical, minimal, or remote. Breach laws also should provide examples of the types of harms (e.g., financial, safety, consumer rights, and social well-being) that are more likely to meet the threshold, focusing on those that present real threats and concrete injuries that are of the greatest concern to individuals and for which action may be necessary. Such harms may include those that potentially cause actual economic or social disadvantage, such as identity theft, financial fraud, physical harm, or discrimination. The threshold should not recognize harms that are more subjective, abstract, or idiosyncratic to a small minority of concerned individuals, such as when a breach results only in a loss of the individual's control over less sensitive data or a violation of contractual commitments concerning the processing of the relevant data.

An appropriate harm threshold obligates organizations to consider the type, sensitivity, confidentiality, and volume of personal data compromised by a breach in determining whether notification is required. There are several factors that entities should consider in this analysis. As a rule of thumb, the more sensitive the data, the higher the risk of potential harm to individuals. The confidentiality of the affected data also matters when considering the risk threshold. For example, an incident involving unauthorized access to or disclosure of publicly available information or information that was already known by the recipient generally does not lead to a level of risk that requires notification. The permanence of the consequences (e.g., short- or long-term effects) also should be taken into account.

In addition to protecting individuals by enabling them to focus on notifications regarding incidents that present a real risk of harm and for which they can take steps to protect themselves, a harm threshold further protects individuals by providing businesses with an incentive to act quickly to remediate an issue. In certain cases, the more quickly a business responds to and remediates an incident, the more likely it will be that the entity can rely on a breach law's harm threshold.[22]

[22] For example, a business may reduce the likelihood of harm or misuse of the personal data if the business remotely deletes the data before it is viewed by an unauthorized party on a compromised device, or immediately identifies and takes action against an employee who inappropriately accessed personal data before the employee is able to use the data. In the event of an inadvertent disclosure of personal data, an appropriate remedial measure may include receiving assurances from a trusted (but inadvertent) recipient that the recipient will either return or securely destroy the data.

Seeking Solutions:

As an accountability mechanism, breach laws could require organizations to document internally security breaches for which notification is not required because the harm threshold is not met. In this regard, relevant laws may require entities to maintain logs of data breaches containing a brief description of each incident. This approach provides entities with discretion in assessing the risk of harm and also makes them accountable for their assessments by documenting the relevant incidents. Breach laws may also require that entities retain relevant documentation for a specified time period (e.g., three years) in case a regulator wants to review the company's history of data breaches.

Timing of Notification to Affected Individuals

Another essential component of breach laws is the timing requirement for providing notice to affected individuals. Identifying an appropriate timing obligation is a crucial challenge for lawmakers seeking to balance the risk associated with inappropriate delays against rushed notifications. On the one hand, a delayed notice could prevent affected individuals from receiving actionable information about the risk to their data and steps they may take to protect it. Alternatively, a rushed notification increases the likelihood that organizations will not have sufficient information about the nature and scope of the issue and will provide notice prematurely. This will have negative results for both the affected individuals and the relevant organization. An appropriate and reasonable time frame for notification balances the risks that may result from notification delays (such as potentially hindering individuals from taking steps to protect their information) against those that may result from premature notification (such as the dissemination of misinformation, causing unnecessary alarm to affected individuals or causing individuals to take unnecessary actions that may inconvenience them (such as canceling a credit card), and potentially exposing additional data to risk of compromise if the notification is made before the entity has restored the security and integrity of its systems).

A reasonable timing requirement also recognizes the increasing pressure organizations face to provide timely notification of breaches that arises outside of the legal and regulatory context. As is apparent in recent breaches, regulators, affected individuals, the media, and the public have come to expect that organizations will notify stakeholders more quickly than in the past. Given the nature of today's media, social media, and blogosphere, businesses experiencing data breaches face several difficult decisions immediately after discovery, starting with balancing their

knowledge of the facts (or lack thereof) with the need to make a public statement before a leak occurs. As a result, some companies self-impose more aggressive timing requirements. The decision to notify early is driven by market forces and the risk of reputational fallout that may result from later notification, regardless of the negative impact to individuals who might be notified but who are not actually affected or who receive inaccurate information as a result of the speed with which uninformed notification was issued.

For these reasons, breach laws should adopt a somewhat flexible timing standard for individual notification that acknowledges the practical challenges—and dangers—of imposing unnecessarily aggressive deadlines while setting reasonable expectations with a ceiling for the window of notification. In taking this approach, breach laws can require that notice be provided in the most expedient time possible and without unreasonable delay but not later than a specified number of days (e.g., 30 or 45 days) after the entity becomes aware of a data breach. This requirement suggests that the time frame to notify would begin when the entity either (1) determines that a breach has occurred or (2) is notified (e.g., by law enforcement or a service provider) that a breach occurred.

What is understood in the first few days of a breach investigation is often dramaticcly different from what is learned in the weeks and months to follow.

A key compliance challenge is understanding when the clock starts ticking. (i.e., when an entity "determines" or "becomes aware of" a breach). What is understood in the first few days of a breach investigation is often dramatically different from what is learned in the weeks and months to follow. To ensure that businesses act expeditiously upon learning of a potential security breach, the breach law can specify that organizations are expected to take reasonable steps to establish whether a data breach in fact occurred. If, through this initial investigation the company confirms with a reasonable degree of certainty that a breach took place, then it will be deemed to have "determined" that there has been a breach, rather than when it first received notice of a potential issue. Importantly, a forensic investigation should not be expected to prove a negative (i.e., that a breach is unlikely to have occurred or that harm is unlikely to have resulted).

Breach laws should allow entities experiencing data breaches to delay notification for legitimate purposes, including if law enforcement authorities request a delay, such as

where notification would impede a criminal investigation or pose a risk to national security. Breach laws also may allow for regulatory approval of a short (e.g., 15 day) extension of time to delay notification to determine the scope of the incident or restore the integrity or security of the compromised systems. If vulnerable systems are not sufficiently patched prior to notification, there is a possibility of copycat hackers seeking to take advantage of known system vulnerabilities, further compounding the initial system compromise. The regulator should have the authority to extend the delay even further under extenuating circumstances.

Regulator Notification

Regulators play a crucial role in monitoring compliance with breach laws and providing individuals with resources for mitigating potential harm arising from a data breach. To enhance regulatory effectiveness, breach laws should require that regulators be informed of data breaches that are likely to raise considerable concern. Breach laws should contain limitations, however, to ensure that regulators are not overwhelmed with notifications by being made aware of every incident, large and small. Such over-notification dilutes regulatory resources that are needed to manage truly impactful breaches. The most straightforward way of drawing a line in this regard is to mandate notification to the relevant regulator if a breach triggers a notification obligation to a specified number of affected individuals (e.g., 1,000). The size threshold for regulator notification should be aimed at alerting regulators of reasonably significant data breaches.

An expedited regulator notification requirement forces companies to expend their resources on preparing notifications to regulators within the first few days, which is often the most critical period in the investigation.

While it is important to equip regulators with information needed to respond to individuals' questions and identify compliance issues in a timely manner, the timing requirements should be reasonable. The law should require notification to regulators not later than the time of notification to affected individuals. A requirement to notify regulators within hours or even days of discovering a breach is unrealistic and unsustainable. At that point in an entity's investigation, there frequently is insufficient information to understand the nature or scope of the issue—or even whether there is a system vulnerability that needs immediate

attention. An expedited regulator notification requirement forces companies to expend their resources on preparing notifications to regulators within the first few days, which is often the most critical period in the investigation. Furthermore, the organization likely will have very little information to provide to the regulator so early in the investigation.

In the event multiple regulators have concurrent jurisdiction over an entity, the breach law should contemplate reporting notifiable data breaches to a single regulator, which should have the responsibility of sharing the notification with other relevant regulators as appropriate. The ability to notify a single regulator encourages efficiency and transparency, while seeking to avoid redundancy for both sides. It avoids multiple regulators assessing the same issue and the affected entity having to expend resources preparing redundant notifications. The law should establish transparency mechanisms that contemplate information sharing among relevant regulators so that if a regulator believes it has a material interest in the breach, the regulator can be notified and collaborate in the response to the issue. The criteria for determining which regulator to notify should be based on operational and jurisdictional ties and designed to prevent forum shopping.

Law Enforcement Notification and Cooperation

In addition to addressing notification to relevant regulators, breach laws should consider the needs of law enforcement authorities in investigating an incident. Also, it is important to encourage businesses to share threat information with law enforcement without the fear of adverse regulatory action.

Method and Content of Notification

The method and content of the notification to both individuals and regulators are important details that should be addressed in a breach law. The permissible methods for notifying individuals should be designed to ensure that notifications make their way to affected individuals and are likely to be read, rather than lost or hidden. Many breach notification laws, for example, allow entities to provide notice by postal mail, email, or telephone. It also is necessary for a breach law to allow organizations to provide individuals with public notice in the event that the entity does not have sufficient or up-to-date contact information for the affected individuals or when it would require unreasonable efforts and resources to communicate individually with

them. The public communication, commonly referred to as "substitute notice" under the U.S. state breach notification laws, should be a method of public notification likely to reach the affected individuals.

Many U.S. state breach laws allow organizations to provide "substitute notification" if (1) providing notification to affected individuals will cost more than a threshold amount (e.g., $250,000); (2) more than a threshold number of individuals are affected (e.g., 500,000); or (3) the organization does not have sufficient contact information to provide direct notification to affected individuals. The substitute notification criteria also should permit entities to provide public notification when time is of the essence and individual notification letters will cause a delay in notifying the affected population. Breach laws could contain prescribed methods for providing substitute notification. For instance, in the U.S., substitute notification under the state breach laws typically consists of (1) a conspicuous posting on the relevant website, which often involves posting a banner above the fold on the website; (2) notification to major statewide media, such as through a press release to a newswire service; and (3) email notice if email addresses of the affected individuals are available to the organization. Alternatively, breach laws could require that the notice meet a certain standard, such as informing individuals in an "equally effective manner" as individual communications. This latter approach, which was adopted in the GDPR, leaves it up to the relevant entity to determine how to sufficiently notify the group impacted.

The permissible methods for notifying individuals should be designed to ensure that notifications make their way to affected individuals and are likely to be read, rather than lost or hidden.

With respect to content, breach laws should specify what information about the breach needs to be disclosed to affected individuals. Breach notification laws with too many specific content requirements result in breach notices that are long, complicated, and difficult to read and understand. This reduces the likelihood that recipients of the notice will comprehend the situation and steps they should take to protect themselves and ultimately reduces the effectiveness of the notification requirement.

In contrast, too few content requirements increase the risk that businesses will send brief and meaningless disclosures that will neither shed sufficient light on the incident and its impact on the affected individuals' personal data nor equip the individuals

with useful information on how to protect themselves. Breach laws should strike a balance with respect to content and require the notifications to disclose important information about the breach that may help affected individuals protect themselves or hold the business accountable. This information includes the nature of the breach and personal data affected, when the breach occurred, steps the business is taking to protect the affected population and prevent similar breaches from occurring, and contact information in case the individual has questions or concerns. Breach laws should allow affected entities discretion to determine what additional information may be helpful to the affected individuals, including choosing whether to offer free identity protection and credit monitoring services to the affected individuals in jurisdictions where those types of services are available.

Preemption

As breach notification laws continue to be enacted around the world, businesses routinely are forced to navigate a crowded landscape of varying—and sometimes conflicting—notification obligations. For this reason, it is increasingly important to address preemption issues with respect to other breach notification requirements in the same jurisdiction. There often are multiple breach laws applicable to certain types of entities within the same jurisdiction. Some jurisdictions enact breach notification laws at the federal, state, provincial, and local levels, requiring entities subject to these laws to comply with all of them. Moreover, jurisdictions also often have sector-specific rules that impose mandatory or voluntary notification requirements on covered entities, such as those in the financial, health care, insurance, digital infrastructure, transport, or energy sectors.

Breach laws should support uniformity and seek to align duplicative and overlapping compliance obligations by overriding or deferring to other notification laws in the same jurisdiction.

Breach laws should support uniformity and seek to align duplicative and overlapping compliance obligations by overriding or deferring to other notification laws in the same jurisdiction. For example, if permissible in a given jurisdiction, the breach law should override breach notification requirements from lower jurisdictions, such as federal preemption over state or provincial breach notification laws. Likewise, the breach law should defer to laws from higher jurisdictions or applicable sector-

specific breach laws by excusing entities from compliance with the breach law if the entity is subject to one of these other sources of notification obligations. In offering preemption, the law should provide a clear exemption and avoid imposing standards that are difficult to apply or are overly subjective. Such provisions could include those that excuse notification only where the other law provides greater protection or at least as thorough disclosure requirements, or only in situations in which the entity provides notification in accordance with the other law.

IV. Conclusion

Data breach notification laws play a vital role in ensuring that organizations protect the personal information they collect and process about individuals. While it is unrealistic to expect complete uniformity across the globe, the divergence among current breach notification standards is suboptimal because it serves to diminish the effectiveness of these requirements. Specifically, the existing landscape is a patchwork of obligations that reduces consistency and predictability for individuals affected by a breach and diverts organizations' resources in the wake of an event from the critical task of breach remediation focused on protecting individuals to managing the needlessly complex notification regimes of multiple jurisdictions. Harmonized global notification standards will ease this burden by simplifying and streamlining organizations' notification obligations, allowing them to focus on protecting individuals across the globe who may be affected by a data breach.

Harmonized global notification standards will ease this burden by simplifying and streamlining organizations' notification obligations, allowing them to focus on protecting individuals across the globe who may be affected by a data breach.

U.S. CHAMBER OF COMMERCE

1615 H Street, NW • Washington, DC 20062-2000
www.uschamber.com