The Sedona Conference Draft Incident Response Guide, Second Edition (April 2023)

The Sedona Conference Draft Incident Response Guide, Second Edition (April 2023)

Drafting Team Members:

Matt Meade (Drafting Team Leader)
Katherine Booth
Cameron Carr
Bob Cattanach
Anya Korolyov
Warren Kruse
Rohan Massey
Joe Pochron
Christian Schröder
Jake Simpson
Nichole Sterling
Joe Swanson
David Moncure (Steering Committee Liaison)

FOREWORD

The intent of the drafting team, which includes privacy and data protection lawyers from many different backgrounds, is to provide a comprehensive but practical guide to help practitioners deal with the multitude of legal, technical, and policy issues that arise whenever an incident occurs. The challenge of preparing any type of guide in such a rapidly evolving area of the law is that it is likely to be outdated, at least to some extent, by the time it is published, or soon thereafter. Nevertheless, the drafters believe that the value of this *Incident Response Guide* ("*Guide*") is not so much in being a definitive compendium of the law in this area, but rather to inform the process that an organization will likely engage in when it adopts the *Guide* for its own use.

The goal, therefore, is to provide those practicing in this space with not only a high-level overview of the key legal requirements that are relevant when an incident occurs, but with enough detail that the *Guide* can be employed largely as a single-source reference to guide the user through the various legal and operational steps necessary to respond to an incident. We address the foundational legal principles of breach notification requirements, principally by presenting those requirements grouped according to the types of obligations that U.S. jurisdictions typically impose, including subcategories for details such as the timing, content, and recipients for breach notifications. The reader may also want to keep in mind the nature of the incident and other more specific obligations that may exist depending on the industry sector involved, particularly health care and financial, as well as the requirements of other international jurisdictions, including the European Union with the advent of its General Data Protection Regulation (GDPR)[1] and more recently enacted and amended laws, such as those in Brazil, China, and Singapore.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard

In our globally intertwined digital economy, incidents will increasingly involve international data, and organizations will need to be alert to the potential that the laws of other jurisdictions may apply in an incident, including if it impacts the data collected in, or of residents of, other countries. The requirements in international jurisdictions will frequently be different from U.S. requirements – and their potential application should not be an afterthought in an organization's incident response. While this *Guide* does not purport to provide a comprehensive summary of international requirements, it tries to identify areas where international considerations should be top-of-mind and provides some examples where aspects of incident response in other key jurisdictions differ from those of the U.S.

As noted in the body of the document, the target audience for this *Guide* is small- to medium-sized organizations, which we expect will not have unlimited resources to devote to incident responses. With this in mind, we have provided sample notification letters that can be used according to different jurisdictional requirements, as well as a very basic Model Incident Response Plan.

It goes without saying that any attempt to provide a document of this nature is by definition a compromise. This *Guide* attempts to strike a balance between being reasonably complete, but at the same time, not so voluminous and legal-authority laden that it is not practical to use during the exigencies of an incident response. As will become evident to

---

Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119/1) *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents [hereinafter GDPR, which shall additionally be understood to encompass and refer to the UK GDPR].

the reader, one of the principal values of this document will be to assist practitioners in the *process* of preparing for an incident response, especially including key leaders in the company as part of the incident response team, which, based on our experience, promotes cross-functional ownership of the pre-incident planning that will be indispensable when it comes time to respond to an actual breach.

TABLE OF CONTENTS

Guide by adding discussion of the following three areas: (1) the evolution and emergence of different types of incidents including ransomware; (2) international incident response; and

(3) key legislative changes since the First Edition was published in 2020.

I. INTRODUCTION

In today's connected world, compromise of ~~electronically stored information (ESI)~~data is inevitable—even for the most prepared organization. An effective and efficient response is critical to expediting recovery and minimizing the resulting harm to the organization and other interested parties, especially affected consumers. The best time to plan such a response is before an incident occurs.

This *Incident Response Guide* ("*Guide*") is intended to help organizations prepare and implement an incident response plan and, more generally, to understand the information that drives the development of such a plan. It has been created by thought leaders in the industry, including privacy counsel from Fortune 500 companies, government attorneys, technical security practitioners, and attorneys from several~~ of the nation's most~~ prominent law firms. It reflects both the practical lessons learned and legal experience gained by the drafters from direct experience responding to incidents, from representation of affected clients, and from the promulgation of rules and guidelines on national and international levels, and is intended to provide general guidance on the topic.

This *Guide* is designed as a reference tool only and is not a substitute for applying independent analysis and good legal judgment in light of the needs of the organization. The reader should note that this *Guide* is up-to-date only as of the date of publication. This is a rapidly changing area of law, so care should be taken to understand and comply with the most current requirements. Nothing contained in this *Guide* is intended to establish a legal standard or a yardstick against which to measure compliance with legal obligations. A reader should neither assume that following this *Guide* will insulate it from potential liability, nor that failure to adhere to this *Guide* will give rise to liability. Rather, the purpose is to identify in detail issues that should be considered when addressing the

preparation and implementation of an incident response that is suitable to his or her organization.

While this Guide was drafted with small to medium-sized organizations ~~in mind~~, it is anticipated that the breadth of topics covered and the chronological sequence of the material will prove a useful reference for even the most experienced cybersecurity lawyer ~~and~~an sophisticated organization.

II. **PRE-INCIDENT PLANNING**

A. Identifying and Mapping Data and Legal Obligations

The foundation for any Incident Response Plan ("IRP") requires careful advance planning. The first step for the organization is to identify what format of data (digital, paper, and other tangible data) it has, and where that data is located.

Tangible data is typically located in offices, filing cabinets, and at remote storage locations, while digital data is more widely dispersed, in on-premises servers, servers located in the cloud, and on hard drives, discs, and flash drives. It is also constantly flowing into, through, and from a variety of physical and logical "locations." Because legal obligations differ depending on data type (e.g., trade secrets, confidential information, personally identifiable information (PII), protected health information (PHI), and payment card information (PCI)), data maps that identify data type as well as data location ~~facilitate~~and flow of data through the company are critical to the effective analysis of and compliance with legal obligations and aid in overall speed of response.

Once the organization's data is mapped, the organization will need to identify the legal and contractual obligations that apply to the data. An index of legal obligations should include both regulatory requirements as well as contractual undertakings that may apply to various data types, including at the locations where they exist or based on how the data was collected. This can help assess legal obligations both in the ordinary course of business~~, as well as~~ and when an incident occurs. The organization's information governance efforts typically form the cornerstone of this process.

Basic data governance considerations will focus on collection, security, use, retention, transfer, and secure destruction of data at end of life. In the statutory and regulatory realm, data security requirements may include

specific requirements, like encryption of PHI under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), or more general data security requirements based on reasonableness or industry standard practices. Contractual undertakings may adopt these data security requirements by reference, or impose additional obligations. The exercise of identifying the legal and contractual obligations that apply to an organization's data should also consider requirements under applicable laws in jurisdictions outside the United States that the organization anticipates may apply. For example, the extraterritorial reach of non-U.S. laws vary from requiring processing or an establishment in the jurisdiction to a business nexus relationship or the intentional offering of your business products or services in the foreign country to simply collecting personal data from individuals in the country or citizens of the country no matter where in the world they might be. Enforceability questions aside, the point here is that an organization must consider as part of any data mapping exercise where and how it is acquiring personal data to assess the applicability of the non-U.S. laws appropriately before a cyber incident. Performing this assessment in the aftermath of a personal data breach is an exercise that will frequently cause companies to miss notification deadlines and can lead to regulatory inquiries that might be avoided with the types of improved compliance that result from understanding in advance the applicable laws, their relevant definitions and notification triggers, the steps necessary to notify the regulator(s), and the types of information necessary for individual notices.

Irrespective of the origin of a security requirement, there should be a process for assigning responsibility for data security by function and position, assessing and tracking compliance, and conducting periodic audits.

B. Supply Chain Security

Digitization is increasingly pervasive. Data that is captured at remote locations is transmitted and processed at various central hubs and increasingly stored off-premises, where it can be accessed later for analytic, reporting, or other business purposes. Sensors now capture data at every turn, especially via controllers embedded within equipment that operate at facilities, as well as the entire facility itself. Given the ubiquity of data and increasing subcontracting and outsourcing of functions, it is common for third parties to have access to the organization's data, systems, or networks to perform routine activities, including maintenance and trouble-shooting. Organizations also routinely share data with third parties, including suppliers, contractors, consultants, auditors, and law firms, collectively "Vendors." Additionally, please see the "Third-party Incidents" section for additional information on these types of incidents.

An organization should conduct due diligence on the security practices of any proposed Vendor that will have access to its data in order to assess whether that Vendor has the policies and procedures in place to appropriately protect the data that will be entrusted to the Vendor, as well as make risk allocation decisions that should be reflected in the language of the contract with that Vendor. Organization-specific due diligence checklists for vendor assessment can be an efficient tool, and may include the following questions:

- Does the Vendor have security certifications such as International Standards Organization (ISO) 27001?
- Does the Vendor follow a National Institute of Standards and Technology (NIST) or another comparable cybersecurity framework?

- Does the Vendor have adequate insurance, including cyber liability coverage?
- What is the Vendor's history of data security events?
- Will the Vendor permit security audits or provide copies of its external security audit reports?
- What due diligence does the Vendor conduct for its own employees, subcontractors, suppliers, and other third parties, especially those that might have access to the organization's data?
- What access controls and related data security measures does the Vendor employ?
- What are the Vendor's encryption practices, at rest and in transit?
- If the Vendor will house the organization's data, where will it be located and how and where will it be transferred, and how much notice will the organization receive if it is to be relocated?
- What are the Vendor's backup and recovery plans?
- Does the Vendor have an IRP?

A due diligence checklist should be regularly updated to reflect changes in legal and regulatory requirements in the United States and elsewhere, the nature of evolving security threats, and standard industry practices. As both national and international cybersecurity laws and standards evolve, the requirements to record due diligence efforts will become expected practice and likely a statutory requirement.

Vendors that pass due-diligence screening should be contractually required to comply with the organization's security policies, guidelines, and practices, and to assist the organization with reasonable investigation requests if an incident occurs. Ideally, the Vendor agreement should include

information-sharing and notice requirements, including when the Vendor must notify the organization of its own data incidents, and changes to its security, data location, or regulatory jurisdiction(s). Unfortunately, this may not always be possible with many of the larger cloud Vendors, whose bargaining power often allows them to offer services on a "take it or leave it" basis, so the organization must factor in the consequences of this concession into their overall security approach.

Vendor access to the organization's networks and other secure assets should be limited to tasks necessary to complete its obligations. Certain types of data (confidential or privileged information, intellectual property, sensitive personal information, and protected health information) should be encrypted, and the Vendor's access to, ability to transfer to or from, and, if necessary, retention of any encrypted data should reflect this protection. A Vendor should be able to access the organization's data and systems only after appropriate training and acknowledgement of its commitment to the organization's security practices. The Vendor's actual access should be logged and auditable, with any irregularities or concerns promptly addressed. Depending on the sensitivity of the information involved, retaining a consultant to validate training and security practices may be a prudent investment. If a Vendor holds the data of the organization, the Vendor (and any Vendor subcontractors) should be legally obligated (by contract, law, professional responsibility, or otherwise) to keep the data secure to at least the same standard as the organization ~~will~~would be held under the laws of applicable jurisdictions inside and outside the United States. It is important to note the more prescriptive an organization is with respect to a Vendor's security measures, the more likely the organization may be seen as the controller of the data held by the Vendor, potentially introducing some additional compliance risk to the organization if the Vendor might

otherwise have been considered the controller. The relative risks and benefits associated with ensuring Vendors maintain appropriate security measures, and whether the organization or its Vendor is considered the controller of data, is beyond the scope of this *Guide*. Suffice it to say that, as a general statement, careful consideration should be given to Vendor arrangements as part of the organization's overall privacy risk management, including with reference to the laws of jurisdictions outside the United States.

Other contractual provisions to consider include limits on subcontractors and other third parties; restrictions on the use of data except for the purposes of the organization; audit rights; notice in case of a Vendor data incident; indemnification; carve-outs from limitation of liability and waiver of consequential damages; data return and destruction; and periodic or ongoing oversight and monitoring.

The organization's Vendor management practices should ensure that Vendor access is terminated for individuals when there are changes in Vendor personnel, and in its entirety upon completion of the agreement. Finally, post-termination data access and assistance should be addressed (for those instances where, post-term, the Vendor's assistance is required to mitigate or manage incidents or regulatory requirements such as investigations), as any unauthorized access may give rise to a cybersecurity event.

C. Exercising the IRP and Response Process Lifecycle

Once an IRP is established, organizations should treat the IRP as a living document and test the efficacy of the IRP and associated response procedures. Testing an IRP is crucial for organizations as it helps to identify and address any weaknesses or gaps in the plan before an actual incident occurs. By testing the plan, an organization can evaluate the effectiveness of its response procedures, identify any areas that need improvement, and refine the plan accordingly. Testing

also helps to ensure that all stakeholders understand their roles and responsibilities during a cyber incident, and that they can work together efficiently and effectively to mitigate the effects of an incident.

There are several ways an organization can test its incident response plan. One approach is to conduct a tabletop exercise, which involves bringing together key stakeholders from across the organization to walk through the incident response plan step-by-step. This exercise can help identify any gaps or weaknesses in the plan and allow stakeholders to discuss and refine their roles and responsibilities. A tabletop exercise can also help stakeholders to understand how the plan would be executed in practice and highlight the importance of a team-centered, collaborative approach to incident response..

Another way to test the incident response plan is to conduct a simulation exercise. This type of exercise involves simulating a cyber incident to evaluate the effectiveness of the response plan. This can be done in a controlled environment with a predetermined scenario, or in a more realistic environment with a simulated attack. A simulation exercise can help identify any shortcomings in the plan, and provide stakeholders with the opportunity to practice their roles and responsibilities in a real-world scenario

Lastly, an organization can conduct a full-scale test of the incident response plan. This type of test involves simulating a real cyber incident and testing the response procedures in real-time. This type of test can be complex and time-consuming, but it provides the most realistic evaluation of the IRP. By testing the plan in this way, an organization can identify any shortcomings in the plan and ensure that stakeholders are prepared to respond effectively in the event of an actual cyber incident.

Organizations should exercise the IRP at both the executive and technical levels because both levels play a critical role in incident response. The executive level is responsible for

making strategic decisions during an incident, while the technical level is responsible for implementing the response plan and mitigating the effects of the incident.

At the executive level, exercising the IRP helps ensure that decision-makers have a clear understanding of their roles and responsibilities during an incident. It also helps to identify any gaps or weaknesses in the plan from a high-level perspective, such as ensuring that the IRP aligns with the organization's overall business continuity plan, and that communication channels are established between different departments and stakeholders.

At the technical level, exercising the IRP helps ensure that technical staff are familiar with their roles and responsibilities, and that they have the technical skills and knowledge needed to respond effectively to a cyber incident. Technical exercises can also help identify any issues related to the configuration of hardware and software, and ensure that technical staff are familiar with the tools and technologies needed to respond to an incident.

Exercising the IRP at both levels is important because it ensures that all stakeholders are prepared to respond effectively to a cyber incident. It also helps to identify any gaps or weaknesses in the plan, allowing organizations to refine the plan and improve their incident response capabilities. Additionally, it helps to ensure that all stakeholders understand their roles and responsibilities, and that they can work together effectively to mitigate the effects of a cyber incident.

III. **THE INCIDENT RESPONSE PLAN**

The IRP provides the standard procedures and protocols for responding to and recovering from an incident. To promote maximum visibility and commitment within the organization, the core components of the IRP should be developed collectively by the members of an Incident Response Team ("IRT"), rather than simply assigned to the Information Technology (IT) department or an outside resource to draft.

The first step in any IRP is to apply agreed-upon criteria that define when an event should be considered only an IT-related incident (e.g., malware infection or detection of routine port scans by external parties) and when the event actually triggers the IRP. The IRP should also identify the responsibilities of each IRT member at the time the incident is first discovered, including how the team leader is designated for each expected type of incident. In addition, the IRP should describe how the team should be modified as a situation evolves and define the criteria for escalations. Basic protocols should include the logging of all critical events, commencing with how the organization learned of the incident, how and when the IRT was notified, as well as the why, what, and how for all responses, particularly escalations to more senior members of the management team and the organization's board of directors.

The IRP should define severity levels with business and legal-impact-based criteria. Clear and consistent communications are one of the most essential pillars of any IRP. The IRP should specify how information should be communicated once an incident is discovered, who should communicate it, and how those communications are coordinated. Protocols should also be established to ensure compliance with reporting mechanisms, which may also include a compliance hotline.

There is no one-size-fits-all IRP. To provide some framework for smaller and even some medium-sized organizations, see the Model Incident Response Plan at Appendix A, *infra*. The IRP should be scaled in sophistication and scope to the nature of the organization. Larger organizations may have business units with their own plans because of regulatory or other considerations (e.g., financial services subsidiary, health care services, and foreign regulatory requirements). In those instances where a business unit may have its own plan, careful thought must be given as to how that plan will interconnect with the organization's crisis management plan, and the overall management structure for coordinating incident responses.

The use of counsel in responding to an incident is an important consideration. Counsel is likely to be most familiar with the legal consequences attendant to an incident, such as reporting obligations. Involving legal counsel should never be an afterthought, and the IRP should include protocols for promptly notifying relevant legal counsel about incidents. Counsel's involvement in communications regarding the incident may also affect the ability to protect those communications by the attorney-client privilege and/or the work-product doctrine or other applicable legal privileges or professional secrecy obligations in jurisdictions outside the United States—which is itself a topic for more comprehensive discussion. To be clear, however, the mere presence of counsel as part of the process does not necessarily equate to qualifying any communication as privileged.

With regard to this latter point, communications and other written materials generated as a result of an incident often contain frank assessments regarding the organization's preparedness, vulnerabilities, and potential liability. Accordingly, those materials may be demanded in future litigation or enforcement proceedings. Whether those communications and other written materials will be shielded

from disclosure is a complex issue that involves a number of factors, one of which is whether counsel was an essential party to the communications. Further, the law on this issue in the data breach context is still developing. For a more thorough treatment of this issue, please consult The Sedona Conference *Commentary on Application of Attorney-Client Privilege and Work Product Protection to Documents and Communications Generated in the Data Security Context*.[2] If an incident involves foreign data, foreign servers, or otherwise involves jurisdictions outside the United States, or gives rise to litigation or regulatory risk in such jurisdictions, the privilege laws of those other jurisdictions may also be relevant to consider. Navigating legal risk and protecting legal privilege, generally and across multiple jurisdictions is, a complex issue that requires fact-specific (and possibly multi-jurisdictional) advice. For the purposes of this *Guide*, ~~suffice~~ it is enough to say that counsel ~~is~~, including foreign counsel where appropriate, are likely to play a significant role in responding to any incident.

Additionally, the IRP should provide clear guidance on the preservation of evidentiary material. Preserving evidence is an essential part of an IRP during a cyber incident. This is because digital evidence can help identify the source of the attack, the method used, and the scope of the damage caused. Without proper evidence preservation, it can be difficult to determine what happened during the incident and how to prevent future attacks.

Another reason why preserving evidence is important during a cyber incident is that it allows for a more effective

---

[2] . The Sedona Conference, *Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents and Communications Generated in the Data Security Context*, 21 SEDONA CONF. J. 1 (forthcoming 2020), available at https://thesedonaconference.org/publication/Commentary_on_Application_of_Attorney-Client_Privilege_and_Work-Product_Protection_to_Documents_and_Communications_Generated_in_the_Cybersecurity_Context.

response. The preservation of evidence helps to ensure that the IRT has access to all relevant information needed to investigate and respond to the incident. This includes identifying the systems and data affected by the incident, the extent of the damage caused, and any potential security vulnerabilities that were exploited. Armed with this information, the IRT can make informed decisions and take the necessary steps to mitigate the effects of the incident and prevent future attacks.

Lastly, preserving evidence helps to maintain the integrity of the investigation. It is important to follow established procedures and guidelines for preserving evidence to ensure that it is not tampered with or compromised in any way. This is important not only for legal reasons but also to ensure that the investigation is thorough and accurate. By preserving evidence in a methodical and systematic way, the IRT can build a strong case and ultimately help protect the organization from further harm.

When a security incident does occur, the IRP should contain guidance to the IRT on how to perform emergency segmentation. Emergency segmentation is a crucial component of an IRP that involves isolating and restricting access to critical systems and data in the event of a security incident. This strategy helps to prevent the spread of malware, limit the impact of the attack, and prevent unauthorized access to sensitive information. Emergency segmentation involves creating separate network segments that can be quickly implemented to contain the attack and prevent further damage.

One reason why an organization would implement emergency segmentation is to minimize the risk of data loss or theft. By segmenting the network, critical data and systems can be protected from unauthorized access, ensuring that confidential information remains secure. This approach can also prevent the spread of malware and reduce the damage caused by the attack.

Finally, emergency segmentation is an essential part of an incident response plan as it can help organizations to minimize downtime and maintain business continuity. By quickly isolating affected systems, the organization can limit the impact of the attack, allowing critical business functions to continue operating. This strategy can help to mitigate the financial and reputational damage caused by the incident and enable the organization to resume normal operations as quickly as possible.

IV. **EXECUTING THE INCIDENT RESPONSE PLAN**

A. Initial Assessment of the Incident ("C-I-A")

The IRP is triggered when a "threat actor"[3] initiates an action that disrupts the organization's cyber infrastructure[4] by compromising the:

- **C**onfidentiality or privacy of information in the organization's care;
- **I**ntegrity of the organization's data or computing/communications systems; or
- **A**vailability of the organization's data or computing/communications systems by authorized users.

The organization then becomes aware of the disruption—often after a significant amount of time has elapsed. Typically, this awareness will originate from:

- the organization's IT or security personnel noticing or being alerted to suspicious or anomalous system or user behaviors;
- a user within the organization noticing a system anomaly, unusual user behavior, or data flaw; or
- the organization being contacted by a third party such as law enforcement or a regulator, a client or customer, a Vendor, a member of the press (social

[3] . Threat actors are human or human-directed, and generally fall into classes such as: insider, whether negligent or malicious; unsophisticated "script kiddies"; socially motivated hacktivists; criminals; competitors; or state-sponsored actors.

[4] . Cyber infrastructure consists of computing and communications systems including those with data and data-processing capability, web presence, etc., whether owned and operated by the organization or by others for the organization.

media or conventional press), or even the ~~malicious~~threat actor itself.

The IT group typically will conduct a scoping investigation of the disruption and attempt to determine its cause, time frame, and which systems or information are at risk. If the disruption is minor, and the risk of harm is determined to be low, the IT group may simply document the situation, repair the disruption, and bring systems back to normal operations. Depending on the severity and cause, the group may inform the full IRT and even senior management. Typically, the thresholds between minor disruptions and disruptions requiring escalation are predetermined as part of a comprehensive written information security plan or the IRP. Typically, the IRT establishes a maximum time period for the IT group to determine if the incident is minor and needs no escalation, prior to the incident defaulting to a more serious status.

B. Activating the Incident Response Team

The incident should be escalated to the IRT if the disruption is not minor and threatens continued operations, or the risk of harm is determined to exceed organizational comfort levels (often by referring to the Enterprise Risk Management protocols or policies). The incident should also be escalated to the IRT if, as indicated earlier, the IT group has been unable to characterize the incident as minor within a pre-set default period of time, or if such escalation is otherwise legally required.

An essential step in the IRP is to identify, individually, each member of the IRT. The IRT should include both internal and external resources that are reasonably likely to be involved in responding to an incident. At a minimum, the IRT should include representatives from the following business areas to the extent they are staffed internally by the organization (if the incident has international scope, then those representatives

should be able to cover all relevant jurisdictions that may be impacted):

- ☐ IT
- ☐ Cybersecurity
- ☐ Legal
- ☐ Compliance
- ☐ Privacy
- ☐ Human Resources
- ☐ Finance
- ☐ Risk Management / Operational Risk
- ☐ Communications / Public Relations / Investor Relations
- ☐ Physical Security
- ☐ Law Enforcement Liaison
- ☐ Supporting external resources (e.g., outside counsel, forensic experts, law enforcement contacts, and crisis management)

Each IRT designee should have a designated backup, with 24x7 contact information available for both the designees and the backups, to ensure that the unanticipated—but inevitable—absence of one key IRT member does not stall or hamstring the process.

As indicated in Section III, each IRT member has predetermined responsibilities. Using the "C-I-A" analysis above, for example, the IT group determines preliminarily what (if any) data has been compromised ("C"), whether systems or data integrity have been affected ("I"), and whether the availability of the organization's data or computing/communications systems has been affected ("A") to assess, at least initially, the scope of the problem. It may also be possible to gain some insight into the identity of the threat actor, the target of and motivation for the attack, the extent of

the attack or breach, and whether it can be quickly contained and mitigated or more significant effort will be required.[5]

C. First Steps of Incident Response and Escalations

The IRP should define data events in terms of severity levels and specify which severity levels require referral to the full IRT. The first point of contact on the IRT should be controlled according to the IRP. That person convenes the IRT per the procedures defined by the IRP. Having counsel (inside or outside, including non-U.S. counsel where appropriate) integrally involved in directing these initial steps will help ensure that the IRT is cognizant of its legal obligations including its legal obligations under the laws of jurisdictions if the incident has an international aspect. Counsel's involvement may also assist the organization in later asserting that the process—and any communications made as part of that process—should be protected under the attorney-client privilege or the work-product doctrine, or pursuant to other legal privileges that may exist under the laws of jurisdictions outside the United States, as noted earlier in Section III.

The IRT should recognize that the facts will be incomplete. Nevertheless, the IRP can provide a checklist or decision-analysis guide that will direct the IRT to take preliminarily responsive actions based on the facts available, as well as provide a framework for identifying what additional facts need to be obtained in order to proceed. The framework should include guidance on the importance of preserving evidentiary material required for an investigation, and how the action of preservation will allow for additional facts to be uncovered. Additionally, this framework should include guidance to the IRT on what evidence needs to be preserved, how to preserve the evidence, and in what format.

[5] . This information should be conveyed immediately to the IRT, consistent with the IRP.

As the investigation unfolds, and more facts are divulged, the process should continue under the instruction of counsel as much as reasonably possible to ensure that the organization complies with:

- regulatory and other legally required reporting requirements under any applicable laws;
- insurance policy requirements;
- contractual-reporting or information-sharing requirements;
- legal-hold requirements and obligations to preserve evidence;
- insider trading protocols; and
- internal policy.

In particular, the IRT should be aware of possible time-sensitive requirements and be prepared to assess at regular intervals whether the facts known at that juncture are sufficient to "start the clock" on any of them, including, in particular, breach-notification requirements (both domestic and foreign) or notices to insurance carriers. The IRP should include communication protocols dictating how and to whom information is communicated once an incident occurs and provide clear guidance to the IRT on what circumstances may trigger external communications and escalation to the C-suite and, if necessary, any Board committees (e.g., Audit or Risk), if not the full Board of Directors.

D. Evolution of the Incident Response

At the beginning of any incident, necessary information is unavoidably incomplete. After activation of the IRT, next steps include initial assessment of the incident's cause and scope, its severity and potential consequences, whether there may be ongoing vulnerabilities or continuing risks, and the status of system security. Once these are determined, the first round of

communication to key decision makers in the organization can commence.

Sometimes the cadence for these initial steps, especially the process of communicating the initial assessment, may be measured in several hours, depending on the situation. For more complicated incidents—especially if it is suspected that the organization's information may have been exfiltrated—the process required to obtain a reasonably accurate assessment may take several weeks, if not months. Just as with the initial response, as more facts become available, legal counsel should remain integrally involved in the direction and evolution of the response as the legal consequences associated with those additional facts are assessed. Legal advice regarding regulatory-reporting obligations, contractual requirements, litigation exposure or regulatory investigation risk, and compliance with internal management protocols will be a critical consideration during the execution of the IRP. Organizations should recognize that inevitably there will be a tension between the desire to protect the communication of legally sensitive information on the one hand, and the importance of transparent and open communication among the key players on the other. One of the more difficult decisions to be made will be the extent to which counsel should be involved in the process of generating or evaluating information that could potentially trigger legal consequences, and the extent to which that involvement enhances the ability to claim attorney-client privilege ~~or~~, work product, or other applicable legal privileges, which ~~is~~are by no means guaranteed merely by counsel's involvement. Indeed, some international jurisdictions, especially civil law jurisdictions (such as France or Germany), have limited or non-existent privilege doctrines when compared to common law jurisdictions. Even common law jurisdictions can vary significantly with respect to the scope of privileges. Counterbalancing that consideration is the need to disseminate

critical information throughout the IRT as quickly and efficiently as possible. Unstructured dissemination risks forfeiting privilege ~~and~~, work-product, and other applicable disclosure protections, because such communications may later be determined not to qualify for protection.

To be clear, not all communications with counsel qualify for protection, even under expansive U.S. applications; only those communications necessary for counsel to provide legal advice, or prepare for litigation, will be protected. The intent to seek legal advice should be used to determine which communications should initially be directed to counsel, and counsel (U.S. and otherwise, as applicable) should be consulted to determine the appropriate communication and privilege approach for the incident.

In addition to applicable U.S. and foreign legal requirements, operational concerns need to be considered. Once the initial security aspects of the incident have been assessed, the IRT will face enormous pressure to alert key stakeholders, and potentially respond to inquiries from the media or public discourse on social media. The pressure to "get out ahead" of the story on the one hand, and "get it right" on the other, invariably creates tensions. The ubiquitous nature of social media can challenge even the most thoughtful and disciplined communication plan. Social media is a powerful tool and, if handled correctly, can provide an enormously helpful channel for messaging; but if handled incorrectly, it can also result in misinformation and mistrust, which will be extremely difficult to overcome.

E. Communications Required Because of Third-Party Relationships or Contracts

The organization may also have contractual or relationship obligations to alert other interested parties and stakeholders. The IRP should catalogue potential parties that may have to be alerted to the incident, including:

- employees;
- contractors;
- clients or customers;
- vendors; and
- lenders, banks, and other financial institutions.

For large organizations or large IRTs, the importance of clearly defining who is the "voice" of the IRT for communications to senior management will be essential to avoid confusing, duplicative, or unclear communications. This is particularly true for significant incidents where the investigation and remediation are factually complex, where the stakes for the organization are quite high, and where the nature of the incident brings particular urgency to finding a resolution.

IV. INCIDENT RESPONSE FOR VARIOUS INCIDENT TYPES

The next section in this paper seeks to apply the principles described above, particularly in Section III, to four recurring fact patterns that have become more common since the publication of the First Edition: ransomware; business email compromise; incidents caused by insiders; and third-party compromises. These four fact patterns are by no means the only instances giving rise to data security incidents, but are common occurrences. In addition, the discussion of the four fact patterns below is not meant to be exhaustive for any one of those fact patterns. Rather, each discussion is intended to highlight the unique circumstances and incident response considerations that may be presented by any of these fact patterns.

Readers of this Guide are encouraged to consider the unique circumstances that may present themselves for any particular

incident and to work with their internal subject matter experts and outside advisers, as needed, to navigate those circumstances.

One inescapable conclusion, however, is that incident response—regardless of the type of incident—functions best as a multi-disciplinary, team approach that draws on security experts, application owners, administrators, finance, legal, communications, and risk functions on the inside of the organization. And, as shown in the preceding sections and in the discussion that follows, the outside advisers called upon to assist may include insurance professionals, counsel, digital forensics and incident response, public relations, data mining firms, and ransom negotiators.[6]

Ransomware

Additional considerations may arise when responding to a ransomware attack. Ransomware commonly presents as a violation of data or system Availability but can also impact Confidentiality as ransomware threat actors' tactics have shifted. Ransomware can generally be broken down into three categories:

- **Single Extortion** – Involves threat actors deploying a variant of encrypting malware designed to lock files and

[6] Where an organization has a cyber-insurance or other potentially applicable policy, it should work with its insurance professionals from the outset of the investigation to evaluate whether to make a claim. This process will likely entail seeking insurer approval for hiring the outside advisers listed above.

render data unusable by the victim. Recovery from single extortion can be achieved by paying for the decryption tool or by recovering from available backups.

- **Double Extortion** – Involves threat actors deploying encrypting malware AND exfiltrating potentially sensitive data, adding another lever to cajole victims into paying the ransom demand. Recovery from a double extortion attack becomes more complex and generally requires additional parties to be engaged (e.g., Threat Actor Negotiation firm) to reach a settlement for both the decryption tool (if backups do not exist) and to negotiate for the deletion of the stolen data.
- **Triple Extortion** – While not materially different from a double extortion attempt, some threat groups have been known to mine the exfiltrated data from the victim environment to communicate with customers, vendors, and partners of the victim via email or phone to place additional pressure on the victim organization. The recovery process is largely unchanged from double extortion; however, the advent of triple extortion tactics does drive the need for a Crisis Communication firm to be engaged throughout the process.

a. High Level Response Process

Due to the high impact of ransomware, incident response teams will be under a large amount of pressure to resolve the incident and restore the environment back to working order. Incident response teams will likely be inundated with various tasks and workstreams that all need to be executed simultaneously. One often overlooked position within an incident response team that could help with the execution of the incident response plan is a Project Management role

designed to keep disparate teams focused throughout the incident lifecycle. Prior to an incident occurring, IRPs should provide a framework to track workstreams and to nominate the position of a Project Manager. As noted in other sections, the organization will want to consider what legal privileges it intends to apply to various aspects of the incident response and ensure that any Project Management structure appropriately protects applicable legal privileges. For example, the investigation of an incident is usually done by legal counsel under attorney-client, work product or other privileges.

Sample Response Framework:

Scope	**Contain**	**Investigate**	**Recover**
Assess impact and severity	Contain incident and eradicate malicious software	Conduct a root cause analysis	Restore services and resume operations
Determine critical organizational functions requiring immediate attention	Cease any unauthorized data transfers from the environment	Determine what data left the environment or was accessed without authorization	Pay or No Pay?
Determine		Determine	

staffing requirements and talent gaps that may exist to support a long running engagement		notification obligations (if any)	

Additionally, incident response plans should directly call out or reference Business Continuity/Disaster Recovery (BC/DR) plans to provide guidance on the restoration order and system level dependencies of critical applications or functions to an organization. Such guidance will speed up the recovery process and prevent confusion from the incident response team when it becomes time to restore functionality. Recovery processes should not occur without proper preservation of evidentiary material occurring prior to restoration.

b. Pay or No Pay

If recovery from backups is not feasible, or if an organization is facing a double or triple extortion threat, the primary decision point becomes "Pay or No Pay?". Payment of a ransom demand does not automatically lead to the restoration of an environment, nor will it guarantee deletion of the exfiltrated data (in cases of double extortion). When payment is made, the threat actors will usually supply a decryption tool to undo the encryption process. These tools usually:

- Are of lower quality and can take several days to decrypt large sets of data;

- Could potentially hold additional malware designed to reinfect the environment; and

- Might not work on certain files or applications.

If decryption of the data is successful, it is possible the original encryption process corrupted data and systems rendering them unusable even after paying the ransom demand. If payment is made for stolen data (in the case of double extortion), there is no guarantee the threat actors did not make a copy of the stolen data with a plan to post or sell the data after settlement. Additionally, payment of a ransom could lead to an organization facing unintended regulatory issues as some ransomware actors and threat groups are sanctioned by various regulatory bodies depending on the locale of the victim organization. Organizations considering a payment to a threat actor will need to ensure compliance with any laws or sanctions relating to treat actor payments in all jurisdictions relevant to their business operations, including outside the U.S. Such decision points should be discussed thoroughly with counsel.

Communications During a Ransomware Incident

Communications during a ransomware incident need to be tightly controlled and should be developed in conjunction with counsel and a crisis communications firm. Due to the catastrophic nature of most ransomware attacks that involve encrypting malware, victims will likely need to communicate both internally and externally to key stakeholders, staff, and customers alike. Internal communications should be crafted to prevent unauthorized communication with the threat actors if ransom demands are displayed within view (e.g., ransom notes on employee desktop devices) and should limit sharing of key incident details outside of formal incident communication mechanisms. External communications to customers, vendors, or other stakeholders should also be crafted, especially in cases of triple extortion.

One often overlooked facet of communication is victim communication directly with the threat actor. In the case of ransomware, most threat actors will provide a mechanism to facilitate direct communication. Using a third party to engage in direct communication with the threat actor can be useful in some situations. For instance, a victim organization may be able to glean additional intelligence that can be useful throughout the response process such as:

- Ransom demand amount
- Proof of file decryption
- In the cases of double extortion
    - Proof of data exfiltration
    - Data exfiltration amount
- How the threat actors were able to get in and commonalities in the types of documents that the threat actor provides as proof of exfiltration

The decision whether to have a specialist engage in direct communication with the threat actor should be made early in the response process. Victim organizations should look to procure the services of a specialist threat actor negotiation firm to conduct such discussions.

The response process will vary depending on the nature and severity of the incident but can be strengthened by incorporating specific ransomware response playbooks or sections within an organization's incident response plan. Additionally, organizations should consult with counsel and other outside experts in the event of an actual incident occurring.

A. Business Email Compromise

Another common incident type is the "business email compromise." In this Guide, "BEC" will refer to any scheme in

which a third party attempts to gain access to one or more email accounts within an organization. That access may be obtained through the third party harvesting a user's login credentials, such as where a user's credentials have been compromised in another incident and that user employs the same credentials for his or her work email. Alternatively, access to the user's email may occur through a credential-harvesting scheme where the third party sends a legitimate-looking email to the user that asks him or her to provide their credentials. There are many other ways in which a third party may attempt to access a user's email account, such as through other forms of social engineering.

These schemes have become ubiquitous. Indeed, losses stemming from BEC schemes are believed to be several billion dollars.[7] In that regard, a common aim of a BEC scheme is to use access to the compromised email account to monitor the organization's processes and cadence for wire payments so as to set in motion a wire diversion. For instance, in a wire diversion, a third party with access to the email of an organization's treasurer or other finance employee may use that access to monitor the account and learn that vendors are always paid on certain days and only after a certain authorization is obtained. Armed with that knowledge, the third party may create a separate fraudulent email account with an address that is nearly identical to that of the person who must approve wire payments. The third party then sends an email purporting to be from the person who approves wire

[7] See, e.g., FBI Alert No. I-050422-PSA, Business Email Compromise: The $43 Billion Scam (May 4, 2022), ic3.gov/Media/Y2022/PSA220504 (last visited Apr. 4, 2023); FBI Alert No. I-040620-PSA, Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion (Apr. 6, 2020), ic3.gov/Media/Y2020/PSA200406 (last visited Apr. 3, 2023).

payments but changes the wire instructions or directs that a previously unknown vendor be paid. In reality, the third party (or an accomplice) controls the account into which those funds will be paid. In today's world, where even small or medium-sized organizations may be processing several or more wires a day, it can be very difficult to identify and thwart such a scheme. There are many derivations of this scheme, many of which have as their aim the diversion of funds from an organization. Underlying every scenario, however, is the unauthorized access to a user's email account, which in this case permitted the third party's illicit monitoring and intelligence gathering that preceded the wire diversion.

To carry out these schemes, the third party not only obtains access to a user's business email, but that third party often creates one or more mailbox rules designed to thwart detection. For example, the third party with access to the email account may not want the real user to see incoming emails from a certain legitimate sender. So, the third party may create a mailbox rule that automatically moves all incoming emails from that designated sender to the junk or trash folder so that the mailbox's user does not see those emails.

Although the aim of most BEC schemes is to facilitate wire diversion, there may be other aims as well. For instance, the third party with access to the mailbox may seek to perpetuate the scheme—and find other victims—by sending purportedly legitimate emails from the user's mailbox to all of his or her contacts. In reality, those emails, although they appear to come from the user, are sent by the third party from within the mailbox and may seek to harvest the credentials of other unsuspecting recipients or elicit payments from those recipients.

Another potential component of a BEC scheme is that the third party may collect the contents of the mailbox, such as where the mailbox contains sensitive information. For example, consider a human relations professional's mailbox, which may contain sensitive information for the organization's employees. A third party with unauthorized access to a user's mailbox may obtain some or all of the contents of that mailbox. This can occur by the third party forwarding selected emails, setting up rules to do so in an automated fashion, or "synching" the mailbox in order to download the entirety of it. If the third party has accessed or acquired any of this data through the BEC, the organization may have notification obligations, such as under various statutes, regulations, and/or contracts.

Given these many features of BEC schemes, an organization that falls victim to such a scheme should consider the following questions and potential action items as part of its response to the incident:

- Whose mailbox has been compromised and what are his or her job functions? Has the incident been confined to just one mailbox or are other users potentially at risk? Has any unauthorized access been terminated?

- With that access, could the third party move to other parts of the organization's networks or systems, such as where the email system may be integrated with other applications? Even if not integrated, if the user employed the same login credentials for those other applications as he or she did for email, the organization will need to determine whether the third party used those credentials to access the other applications.

Answering these questions will likely involve working with a digital forensics and incident response firm, preferably engaged through in-house or outside counsel so as to maximize the application of the attorney-client privilege and other potential privileges and protections.

In addition to giving careful and prompt attention to the questions listed above, the organization will want to immediately consider whether any wire diversions have occurred as a result of the scheme. The organization's Finance function should immediately evaluate all recent wire transfers and other payments. If any of those transfers appears to be fraudulent, the organization or its counsel should contact the organization's bank and law enforcement immediately. Ideally, the organization will have a preexisting relationship with one or more agents through the local field office, which will facilitate getting prompt assistance. If no such relationship exists, the organization can contact the FBI through the local field office or at ic3.gov and the Secret Service through the local field office or one of its Cyber Fraud Task Forces (CFTFs). Because diverted wires often end up leaving the country, federal law enforcement assistance—as opposed to working with local police—is likely most effective. In all instances, however, time is of the essence, as law enforcement's ability to identify and freeze diverted funds wanes by the day.

As noted above, because a BEC necessarily involves a third party accessing a mailbox without authorization, the organization should consider whether any notification obligations are triggered by that access. To assess this, the organization will likely need to engage with a digital forensics and incident response expert. The forensics expert should analyze all available evidence to determine whether the third party accessed contents of the mailbox or acquired any of those contents, such as through forwarding emails, setting up

mailbox rules, or downloading the entirety of the mailbox. The organization should consider the nature of the mailbox user's job functions. In some cases, the data at risk may be so large that a data mining firm is needed to ingest the data and analyze it in an automated fashion to identify whether PII or other sensitive information was present in the mailbox and therefore at risk. The organization will want to work with counsel to oversee this work, ensure the work is subject to applicable legal privileges, and analyze potential notice obligations set by statute, regulation, or contract. As part of this analysis, the organization should consider if any court orders in pending litigation require notice of any kind. An organization that has a central repository of contracts and has inventoried their notice obligations may be better positioned to efficiently analyze those potential notification obligations.

Insider Threats

The term "insider threat" refers to the potential for an individual who has or had authorized access to an organization's critical assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.[8] An insider threat can be a current or former employee of an organization, a contractor or vendor, a visitor to the organization, or anyone who would have or had access to the critical assets of an organization.

The statistics surrounding insider threat incidents are staggering; a 44 percent increase since 2020 in reported incidents, with credential theft by insiders almost doubling in that same time. The average annual cost to remediate an

[8] Common Sense Guide to Mitigating Insider Threats, Carnegie Mellon Software Engineering Institute, 2022, Seventh Edition.

insider threat incident was $6.6 million. The average time to contain an insider threat incident was 85 days, with only 12 percent of incidents contained under 30 days. Not surprising, those organizations that were able to contain the incident under 30 days experienced the least costs related to this type of incident, which stemmed from business disruption and technology enhancement or upgrades.[9] All of this points to the importance of planning for insider threats and responding to them in a timely manner.

An insider threat incident can take many forms, however the primary examples of insider threat incidents are:

- Intellectual Property Theft
- Information Technology Sabotage
- Fraud
- Misuse of Authorized Access
- Unintentional Incidents
- National Security Espionage
- Workplace Violence

Each type of insider threat incident is unique in terms of the fact pattern, and organizations should organize their response plans accordingly. It is common for complex insider threat incidents to require not only incident response, but also monitoring and surveillance, investigation, containment, and remediation, and beyond.

There are three main types of insider threat actors: malicious, unintentional, and compromised. The majority of insider threat incidents are from unintentional actors who have access to an organization's critical assets and, through some form of negligence, negatively impacted the organization. Malicious

[9] 2022 Cost of Insider Threats Global Report, the Ponemon Institute, 2022.

actors are those actors that use their access to inflict harm on the organization. There are a variety of stressors and concerning behaviors that may occur that can cause an employee to become a malicious threat actor. Organizations should familiarize themselves with those indicators and incorporate that into their insider threat framework. Compromised actors are actors that may be compromised from an outside influence, very often a nation-state that is leveraging the insider threat actor for some form of espionage or intellectual property theft.

An organization that is looking to build a response plan around insider threat incidents should refer to Section III of this paper, as well as Appendix A. Aside from a response plan, an organization should also consider adopting a broader insider threat framework that not only addresses incident response, but other relevant domains. In general, a mature insider threat program should address all of the following:

- Governance & risk
- Monitoring
- Asset Protection
- Incident Response
- Personnel & Physical Security
- Education & Awareness

Since an insider threat incident will require involvement and response from various stakeholders within an organization, current response plans that exist for information or physical security can be integrated into an organization's insider threat response plan. Additionally, as part of that process, a decision will need to be made within the organization if, given the type of insider threat assessment, law enforcement needs to be notified as well.

Third-Party Compromises

Third-party cyber incidents have been a significant cyber-security risk for organizations in recent years, and it is likely that this trend will continue in the future. The increasing complexity of supply chains and the reliance on third-party vendors and suppliers to provide critical services and support has made organizations more vulnerable to cyber threats originating through third-party sources.

Third-party cyber incidents refer to cyber-security incidents that originate through external parties that have been granted some level of access to an organization's data or information systems. These parties can include vendors, suppliers, partners, contractors, and other third-party service providers. Third-party cyber incidents can occur in various forms and are not too different from direct cyber incidents; examples include data breaches, malware attacks, supply chain attacks, and social engineering attacks all of which result in the exposure of sensitive information for individuals and businesses. However, a third-party incident is more complicated than a direct cyber-attack in that it, by definition, involves multiple organizations. As such, these incidents often are composed of multiple threats or even multiple attackers. A third-party incident is often complex, and as such may have several features to it that would be incidents unto themselves. For example,

- A third-party incident may result in a data breach of sensitive information either held by the organization or by a partner organization that was also impacted.
- A third-party incident may feature malicious requests to the organization's systems that would otherwise be authorized when coming from the partner organization (such as fake orders, requests for customer information, etc.).

- A third-party service may allow malware into the organization's environment, facilitating the detected incident, or future incidents if it remains a persistent threat.
- Attackers might be able to mimic members of a penetrated partner organization, allowing the attackers to bypass both technical and social safeguards to convince the organization's personnel to grant them information or access they should not have.

If an organization experiences a third-party cyber incident, it is important to take the following steps unique to third-party compromises (these are in addition to the steps identified earlier in this Guide regarding incident response generally).

- Promptly notify the third-party vendor or supplier, if the organization learned of the incident, to ensure they take appropriate action to contain the incident and prevent it from spreading further.
- With counsel, conduct a thorough assessment of the incident to determine the scope and impact of the incident. Find out what type of data was compromised, how the attack occurred, and what steps the vendor is taking to address the issue. Determine whether the cyber attack poses a risk to the organization. If the vendor has access to sensitive data, such as customer information or intellectual property, the attack could potentially impact the organization as well.
- Review and update third-party contracts to ensure that they include robust cyber-security requirements and obligations and consider conducting regular audits and assessments of third-party vendors to ensure compliance.

- Depending on the severity of the cyber attack, the organization may want to consider taking legal action against the vendor. This could include filing a complaint with a regulatory agency or initiating litigation against the vendor.

The specific actions an organization takes will depend on the nature and severity of the incident, the information compromised, as well as any legal or regulatory requirements. Therefore, organizations should consult with legal and cyber-security experts to ensure they are taking appropriate and effective measures to address the incident, and to protect legal privileges that may apply to the incident response.

V. KEY COLLATERAL ISSUES

A. When and How to Engage Law Enforcement

In many cases, a data breach will involve actions by someone—whether inside or outside the organization—that could be considered a violation of U.S. federal or state law, or the laws of another nation or jurisdiction. One of ~~three~~four circumstances will typically lead to the involvement of law enforcement:

- There is a legal requirement under any applicable law[10] to report the matter to law enforcement authorities.
- A contractual obligation requires reporting to law enforcement authorities.[11]
- Reporting the matter to law enforcement is discretionary, with the affected organization retaining some latitude to decide whether reporting the incident seems, overall, to be consistent with the organization's best interests.
- The first notice that an organization has of a potential breach is outreach from a law enforcement authority, contacting the victim

[10] For example, in Canada, private sector privacy laws do not explicitly require that incidents be reported to claw enforcement, there is a general requirement under the federal privacy statute to report incidents to any third party that may help reduce the risk of harm to the affected individuals, which could potentially include law enforcement or government agencies depending on the circumstances. See, e.g.: *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 10.2, <https://canlii.ca/t/7vwj#sec10.2>, retrieved on 2023-04-19.

[11] For example, France now requires cyber-attack complaints to be filed to "competent authorities" within 72-hours if victims wish to seek reimbursement under their cyber insurance policy. This new reporting obligation was introduced by article L12-10-1 of the French Insurance Code.

organization to inform them of activity that law enforcement has discovered.

There are a number of factors to consider in determining whether and how to engage law enforcement, including:

- the nature of the data that was potentially compromised;
- the need for assistance of law enforcement in investigating or mitigating the incident;
- the potential level of involvement from law enforcement in investigating the incident and the level of requests for evidence or audit logs;
- the need to mitigate any exposure under sanctions or similar regimes;
- the country and/or state of residence of any persons whose information is implicated in the incident;
- whether any specific regulatory scheme or statutory framework applies to the particular data or business operations at issue; and
- the locations where the organization is headquartered, has operations, or does business.

There can be a policy dimension to the decision on whether to engage law enforcement that is tied to the organization's culture. Some organizations voluntarily notify law enforcement out of a sense that good corporate citizenship obligates them to pass along information that might help authorities investigate crimes or even prevent other organizations from falling victim to the same crimes. Other organizations may be skeptical of triggering government involvement and less inclined to see advantages in passing information on to law enforcement entities. Although these intangible factors tend to be matters of organizational culture and policy, rather than strictly legal questions, it is important that organizations consider these decisions at a level of

management commensurate with the potential consequences. Senior leadership will want to consider shareholder expectations, the reactions of customers and business partners, past public relations and public policy positions, or other factors that are unique to the organization.

Some organizations may be concerned that notifying law enforcement could trigger an investigation into their own information security practices and are therefore hesitant to make that outreach. The best approach to this issue is to establish, either directly or through outside counsel, a relationship with key law enforcement entities in advance of an incident, so that any reporting to law enforcement can occur within the context of a relationship built on some measure of trust, enabling the organization to consider more objectively whether the fear of heightened investigative scrutiny is well-founded in any particular instance.

Any checklist an organization might prepare regarding the decision whether to report to law enforcement should include:

- whether the organization could be exposed to legal liability for failing to report the incident (for example, when failure to report could constitute an independent violation of law);
- whether there is specific benefit to notifying law enforcement, such as when an incident involves breach of PII of victims in states where breach laws provide for a delay of notification if law enforcement determines that notification will impede a criminal investigation;
- the potential benefit to law enforcement and to other victims;[12]

[12] . A single organization rarely has the insight to be able to adequately assess whether the cyber activity affecting them is part of a larger effort by organized crime, terrorists, or others who use malicious cyber activity as a means of financing their own operations (such as terrorist attacks, political

- whether a law enforcement investigation could disrupt business operations;[13] and
- the philosophy of the organization.

At a minimum, organizations should identify in advance which federal and state laws require notification to governmental entities in the event of a breach. Critical to that assessment will be whether an organization has customer, employee, or other data that, if compromised, would trigger a requirement to notify a state attorney general or similar regulatory entity. The nature of the incident may influence whether federal, state, and/or local law enforcement is likely to have interest in the incident.

1. Employee Theft

For example, if the incident involves a terminated employee who stole property (such as a laptop computer) that results in a data compromise (the laptop contains sensitive personal information), state or local law enforcement agencies may be best suited to investigate the theft as a local law enforcement matter and aid in recovery of the information.

~~2. Other Employee Misconduct~~

~~Employee actions can also combine criminal activity with computer security threats in different ways. For example, employees may use the organization's computing resources for unauthorized activity on the internet, such as sale of illegal drugs, human trafficking, or downloading of child pornography. Because of the nature of the websites and the communities of interest who engage in these activities on the~~

destabilization, illegal arms trade, or other matters that affect the security of individuals and nations around the world).

[13] . Here, it should be noted that many law enforcement agencies are committed to carrying out investigations in a manner that causes as little disruption as possible to the organization.

~~internet, these activities can also increase the risk that malicious code will be imported into the organization's computer systems—which might result in the risk of downloading ransomware, or of giving an external hacker access to sensitive PII or intellectual property on the organization's network. In some cases, the illegal activity will lead to discovery of the breach; in others, discovery of the malicious code is what causes the organization to realize that this illegal activity is taking place. In such cases that involve a mix of a data security incident and serious criminal activity, the organization should report the matter to the appropriate law enforcement authorities, as failure to do so could result in independent civil liability or criminal charges for the organization. The organization can expect to become involved in a criminal investigation of what actions were taken on the organization's networks and by whom.~~

2. ~~3.~~ External Hacking

In incidents involving external hacking into an organization's network, federal law enforcement may be better suited to handle the matter than state or local authorities. First, state and local law enforcement agencies vary greatly in their capacity to respond to cyber incidents. Some have well-resourced and sophisticated components dedicated to computer crimes, while others have few, if any, resources available to handle these types of investigations. Second, in many instances, the hacking activity will constitute a violation of federal law, such as the Computer Fraud and Abuse Act. Consequently, the malicious activity is likely to fall within the jurisdiction of, and be of interest to, federal law enforcement agencies.

The U.S. Federal Bureau of Investigation (FBI) and U.S. Secret Service Electronic Crimes Task Force generally lead federal law enforcement investigations of cyber crimes. If nothing else, these federal agencies can help direct an

organization to state or local law enforcement if the matter does not meet the federal agencies' thresholds. Interacting with the FBI and U.S. Secret Service is described in more detail below.

There are a number of guidelines to consult for reporting cyber crimes The FBI and Department of Homeland Security (which includes the U.S. Secret Service) have issued unified guidance to state, local, tribal, and territorial law enforcement agencies on how to report potential cyber crimes to the federal government.[14] The FBI works through its Cyber Division and its Cyber Task Forces, located in each of its 56 field offices.[15]

Organizations should also be cognizant of reporting to law enforcement authorities outside the U.S., as multinational cooperation on cyber crime continues to increase. For example, Europol has become increasingly involved in investigation of cyber crimes through its European Cybercrime Centre (EC3), which was established in 2013 with a stated purpose to "strengthen the law enforcement response to cyber-crime in the EU and thus to help protect European citizens, businesses and governments from online crime."[16]

---

[14] . FED. BUREAU OF INVESTIGATION, LAW ENFORCEMENT CYBER INCIDENT REPORTING (2017), *available at* https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf/view.

[15] . Anecdotally, the FBI has been more than willing to meet with organizations to help them understand the threat landscape even before any potential incident, and when appropriate conduct post-incident assessments (e.g., obtaining the internet protocol (IP) address of the financial account to which fraudulent transfers of funds have been directed). However, as a practical matter, absent extraordinary circumstances, the FBI typically lacks the resources to pursue aggressively the swelling tide of "run-of-the-mill" data breaches and related schemes, including "business email compromise," which are addressed above in IV.B."

[16] . *European Cybercrime Centre—EC3*, EUROPOL, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (last visited Dec. 2, 2019).

In addition to multinational efforts such as Europol, most nations have some form of national law enforcement effort against cyber crime, and many nations also have subordinate local or regional law enforcement efforts directed against cyber crime. Organizations with a substantial business presence outside the U.S. should ensure they are familiar with the law enforcement entities that may have jurisdiction of cyber-related criminal activity that affects the organization's activities in those countries or regions.[17] Some jurisdictions may mandate notification to specific CERT teams under statute.[18]

At the beginning of an incident, it is often difficult to tell whether a criminal prosecution is likely to result. For that reason, it is important that the organization carry out its investigation in a manner that preserves the chain of custody for any evidence that may later be relied upon in court. This is important for potential civil litigation as well. Technology professionals who are assisting with the incident response should be particularly careful to avoid taking actions that might obscure the evidence of any unauthorized actions taken on the network. This will typically include preservation of

[17] For example, in Canada, the Royal Canadian Mounted Police (RCMP) has taken a leadership role in coordinating law enforcement efforts in response to cybercrimes across Canada, in collaboration with regional police forces and public service agencies such as the Canadian Centre for Cyber Security (CCCS) and the Canadian Anti-Fraud Centre (CAFC).

[18] For example, in India, pursuant to the introduction of Section 70B IT Act which introduces the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013. Rule 12 of the CERT-In Rules sets out that any individual, organization, or corporate entity affected by certain cybersecurity incidents should report the same to CERT-In 'as early as possible'. The accompanying directors establish that service providers, intermediaries, data centers, bodies corporate, and government organizations must mandatorily report certain cyber incidents within six hours of awareness.

system log files and full and precise imaging of system components. The scope of this work can be both painstaking and complex, depending on the nature of the organization's technology architecture and the type of incident.

Preserving this evidence and preserving the chain of custody that allows it to be admissible in court frequently requires a specialized set of experience and skills that may be beyond the expertise of in-house computer security professionals. Organizations that do not have personnel specifically trained in this kind of activity—and perhaps even those that do—should strongly consider engaging outside consultants who have experience in performing this work. Most often, the organization will want to engage those consultants through counsel, so that the work is better positioned to be carried out within the scope of the attorney-client privilege ~~and/or~~, the work-product doctrine, or other legal protections from disclosure, and preferably engage them well before an incident occurs through pre-negotiated Master Services Agreements.

The critical point that organizations should remember is that these considerations need to be built into the IRP for the very first moment that a suspected incident is identified; once network actions have been taken (including remedial actions like isolating infected servers or devices), it is often already too late to preserve the evidence in a form that would be admissible in court.

For example, in many traditional networks, disconnecting power from a server will not be an appropriate means of preserving evidence. In some situations, it may be appropriate for the server or other hardware to remain powered on but the network connection severed (by unplugging an Ethernet cord or turning off wireless connectivity to that device). Certain standard response actions for certain specified events might be set forth in the IRP; nonstandard events will require more careful thought before taking responsive action.

This is merely one example, however, as cloud computing, third-party data hosting, use of service-oriented architectures, automated data aging, handling and storing backup data, and many other factors will affect the specific actions that are most appropriate in a particular case. For these reasons, it is essential that the organization rely on the advice of skilled technology professionals who have specific expertise in preservation of systems and data for forensic investigation purposes, whether those professionals are employees of the organization or hired as outside consultants.

B. Notice to Insurance Carriers

The notice required by an organization's insurance carrier should be set forth in the organization's insurance policy and carefully followed. The same applies to any separate policies that may apply to an organization's subsidiaries.

C. Alternative Communications Channels

In the event of a significant cybersecurity incident or intrusion, as with other emergency situations, it is essential to have reliable communication channels available to keep key players and essential stakeholders informed, and to lead and manage the incident response. In some cases, this may require alternative (and secure) communications channels. As with other incident response preparations, alternative communications channels should be planned and provisioned in advance to handle situations where corporate communications systems have been completely disrupted.

Assuming that the disruption of communications is limited to the organization's systems, and that third-party provider systems are still functioning, national telecommunication companies and internet service providers will be able to provide alternative communications channels for voice, text, and email. Organizations that cannot sustain a loss of internal communication systems without risking material compromise

to their ability to function should, at a minimum, explore advance arrangements for standby communications channels for their mission-critical functions. Secure emergency online portals, such as systems provided by "ERMS Emergency Notification and Mass Communication," can also be used as standby methods to broadcast information to users or selected groups and to share documents among a specific group of people.

With any alternative communications channels, there are certain caveats to be observed:

- Careful thought must be given to ensuring the security of the devices used by persons authorized to access the alternative communications channels.

  Personal cellphones or home phones may be a possibility, but if phone numbers for those devices were available on the organization's network at the time of an intrusion (as is often the case), it may be prudent, at least at the outset, to assume that those devices may have been compromised as well.

  The more advisable course may be to maintain a stock of emergency cellphones, tablets, and laptops, preinstalled with appropriate security (e.g., two-factor authentication), for distribution as appropriate in the event of an emergency, especially for use by members of the IRT and senior management of the target organization.

- Preexisting email addresses and phone numbers should not be used (or permitted) to access the alternative communications channels. Instead, alternative email addresses (for example, name@xxxx.yyyy.com) and non-office phone numbers, all previously unused, should be issued for use with devices permitted to access the alternative communications channels.

In addition, the new (emergency) email addresses and phone numbers should *not* be kept online in any form (e.g., listed in the official IRP) to prevent that information from falling into the hands of the attackers. Instead, a hard-copy list (such as a wallet card) should be distributed only to members of the IRT and the organization's senior management who are expected to use the alternative communications channels.

- Consider face-to-face "in-person" meetings and communications as part of the alternative communications channels, and make arrangements for an emergency room or "war room," which can accommodate the IRT and senior management, for fact review, analysis, and decision-making.

  Situating an emergency room in one of the organization's offices may be sufficiently secure, but it may be more prudent to plan an alternative location in a different building. As with emergency email addresses and phone numbers, the alternative location should be revealed only to those who need to know.

- To ensure that the capabilities of alternative communications channels are maximized, it is also essential to document and periodically review relevant processes. This should include regular maintenance (and when changes are made, redistribution) of the off-line list of emergency email addresses and phone numbers, as well as documentation in the IRP of how to use the emergency tools and how to contact critical resources like forensic consultants, external counsel, public relations consultants, law

enforcement authorities, insurance companies, and key external stakeholders.

- Finally, to avoid alerting the threat actors that alternative communications channels have been activated, it may be appropriate to continue selective use of preexisting communications channels by some personnel with nonsensitive information (and possibly with "misinformation").

D. Terminating Unauthorized Access

Various studies have consistently shown that a significant percentage of cyber incidents have been caused by trusted insiders. In many cases, those studies conclude that insiders are responsible for over half of all incidents, through a combination of carelessness or risky behavior with unintended consequences, and deliberate incidents, such as theft of information, impairment of computer equipment and systems, or otherwise.

All computer and network access should be terminated as soon as possible for employees who no longer work for an organization, particularly in instances in which an employee has been fired or laid off. When an employee is being fired or laid off, the best practice is to revoke systems access immediately prior to notifying the employee of the administrative action about to be taken; this prevents the employee from being able to take retaliatory action on the network in response to the employer's action.

It is also essential for organizations with suspected malware to carefully and quickly examine whether there may be any unauthorized access that is persisting on the network. It is not uncommon for sophisticated hackers to leave backdoors that are not readily identifiable; an organization may believe it has closed the vulnerability, not recognizing that additional code remains elsewhere in the network or in devices that can be used as a launching point for further unauthorized access.

Unfortunately, it may not be apparent at the time that incident response begins whether the incident was caused by an advanced persistent threat (a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time, rather than causing immediate damage to the network or organization) or other sophisticated actor. Consequently, this risk is another reason why organizations should consider engaging external consultants who specialize in remediating cyber incidents to work with in-house computer security personnel to ensure that network security has been restored against both known and less obvious threats.

E. Engaging Outside Vendors

1. Pre-engaged Vendors

The IRP that was prepared and tested in advance should include consideration of outside Vendors for several purposes: computer forensics (to determine the nature and scope of an incident and the degree of ongoing vulnerability); continuous monitoring (some organizations will choose to contract with outside Vendors to provide ongoing security monitoring of their networks); breach notification (some Vendors are well-practiced in providing multi-jurisdictional incident notifications to victims; an organization with complex, multi-jurisdictional PII of customers or employees may wish to consider using a consultant to streamline and facilitate the process of breach notification, to include written notification and customer call center services); and crisis communications or media relations (depending on the nature of the incident, public relations can be a key factor in successfully navigating a breach~~)~~. Organizations with cyber insurance should carefully review their policies, as the selection of Vendors may be limited to pre-approved Vendors, or in some instances dictated, by their insurers. If an organization has any preferred Vendors that require insurer approval, it should

obtain approval at the time of policy placement or renewal, or otherwise in advance of a cyber incident.

2. Considerations in the Use of Vendors

Whether to use Vendors can be a particularly difficult decision for small and mid-sized organizations whose business model does not include a large standing budget for incident response. The decision is a particularly difficult one in the early days of an incident, when there are still limited facts about what might have happened and the organization is struggling with the question of whether its own IT services staff (whether in-house or provided by a Vendor) can handle the incident investigation on its own. For smaller organizations in particular, there can be a tendency to first try to handle the investigation in-house, due to concerns that the cost of hiring an external computer security consultant will be unduly damaging to the organization's overall budget and fiscal health. Organizations with cyber insurance should carefully review their policies, as they may have coverage available for various types of Vendors.

3. Cost and Resource Issues for Vendors

In their preparedness efforts, small and mid-sized organizations concerned about these matters should have specific conversations with cybersecurity consultants about their rates and services. Like the organizations they serve, consulting firms come in a variety of sizes. Mid-sized and smaller organizations that are considering incident response planning should not be deterred by concerns that large consulting firms have a business model that falls outside of their price range, as both large and small firms are able to provide sophisticated services across a wide range of price points to meet the needs of organizations that are faced with actual or potential cybersecurity incidents. Organizations with cyber insurance may also benefit from any pre-established

arrangements for discounted rates from certain consultants through their insurer and should consult with their insurer as appropriate.

4. Attorney-Client Privilege and Technical Consultants

As noted earlier, consideration should be given to having legal counsel engage technical consultants to facilitate the provision of legal analysis and advice, and potentially protect that process by the attorney-client privilege ~~and/or~~, the work-product doctrine, or other disclosure protections. This topic is addressed in relation to U.S. laws in greater detail in The Sedona Conference *Commentary on Application of Attorney-Client Privilege and Work Product Protection to Documents and Communications Generated in the Data Security Context*,[19] but among the issues to consider here are the language of the engagement letter with the technical consultant and whether counsel will be the intermediary between the consultant and the organization, and whether to engage different incident response consultants than are used for ongoing or pre-incident services.

The rules about legal privilege may also be different in jurisdictions outside the U.S.[20] As such, additional consideration should be given to the privilege rules in applicable jurisdictions for incidents that have an international aspect or may result in legal or regulatory proceedings outside the United States.

[19] . *Commentary on Application of Attorney-Client Privilege and Work Product Protection to Documents and Communications Generated in the Data Security Context*, *supra* note 2.

[20] For example, in Canada, legal counsel's engagement of consultants may be subject to solicitor-client privilege and/or litigation privilege.

5. Engaging Technical Consultants at the Time of Breach

If there is no pre-arrangement with technical consultants, organizations that experience an incident should consult with in-house or outside counsel on the value and feasibility of bringing in technical consultants. Many law firms have existing relationships with consultants whose services they can engage or recommend, and many consultants are available on extremely short notice to respond to an incident, even if there haven't been previous discussions with the organization that is affected by the incident. As organizations increasingly purchase some form of insurance coverage for cybersecurity incidents, those carriers frequently have pre-approved panels of legal counsel and technical consultants available for immediate assistance.

F. Credit Monitoring and Identity Theft Considerations

Credit monitoring has been part of the data-breach landscape for many years, most often through voluntary action by the organization that suffered the breach, or as part of a consent decree with a regulator (such as the Federal Trade Commission (FTC)) or settlement among parties to litigation.

For the reasons discussed in detail below, however, organizations should carefully evaluate the decision to offer—and if so, to what extent—credit monitoring to impacted individuals in connection with a data breach. ~~At~~Offering credit monitoring and identity theft protection services can be viewed by courts as the organization following best practices and taking steps to mitigate any potential harms from the incident. It may also reduce legal risk by mitigating potential harm to individuals as a result of an incident. On the other hand, at least one court, the Seventh Circuit, has interpreted an offer of credit monitoring in a credit card breach as a sign that the risk was real, not "ephemeral," and, therefore, qualified as a concrete injury:

> It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk *is so ephemeral that it can safely be disregarded.* These credit-monitoring services come at a price that is more than *de minimis*. For instance, Experian offers credit monitoring for $4.95 a month for the first month, and then $19.95 per month thereafter. See https://www.experian.com/consumer-products/credit-monitoring.html. *That easily qualifies as a concrete injury.*[21]

The clear message from *Neiman Marcus* is that offering credit monitoring is a factor that the court will consider in connection with establishing standing. Overall, the potential risks and benefits associated with offering or not offering credit monitoring services and identity theft protection is a complex question. The law continues to evolve, and the relevant considerations may vary from jurisdiction to jurisdiction or internationally. Organizations should consult local and international counsel as applicable for current advice on the risks and benefits of offering identity theft protection and credit monitoring services in response to an incident.

Second, credit monitoring only partially addresses the consequences of the potential theft of personal information. Some commentators have opined that it gives "consumers limited help with a very small percentage of the crimes that can be inflicted on them."[22] "Breached companies . . . like to

[21] . Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015) (emphasis added).

[22] . Brian Krebs, *Are Credit Monitoring Services Worth It?*, KREBS ON SECURITY (Mar. 19, 2014),

offer it as a good [public relations] move even though it does absolutely nothing to compensate for the fact that a criminal stole credit card mag stripe account data."[23] A spokesman for the Privacy Rights Clearinghouse recently stated: "Fraudulent use of a stolen card number won't show up on a credit report because they don't show individual charges. And credit reports don't show debit card information at all."[24]

Third, offering credit monitoring when, for example, the breach involves medical data such as diagnoses, doctors' notes, and x-rays absent Social Security numbers, may arouse suspicion among those impacted that the breach is more comprehensive than the breached organization has disclosed in its notice. For example, if the breach notice informs the consumer that no Social Security numbers were accessed or subject to unauthorized use as a result of the incident, a recipient naturally might wonder why he or she is being offered credit monitoring. Credit monitoring will not tell you if someone has "hijacked your identity for nonfinancial purposes, i.e., to get a new driver's license, passport, or other identity document."[25] Moreover, credit monitoring will not tell you if someone is using your medical information to get free medical care or medication.

Consideration should also be given to whether credit monitoring is required under U.S. laws or laws of jurisdictions outside the United States. A number of states have adopted a

---

SECURITY (Mar. 19, 2014), https://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it (quoting Avivah Litan, fraud analyst at Gartner, Inc.).

23 . *Id.*

24 . Gregory Karp, *Why Credit Monitoring Will Not Help You After a Data Breach*, CHI. TRIB. (Aug. 15, 2014, 8:00 PM), http://www.chicagotribune.com/business/chi-why-credit-monitoring-will-not-help-you-after-a-data-breach-20140815-story.html.

25 . Krebs, *supra* note 13 (quoting Avivah Litan, fraud analyst at Gartner, Inc.).

stricter approach to offering credit monitoring. In 2014, California amended its breach notification law as follows:

> 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, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).[26]

California's amended law states that identity theft protection services should be used for breaches involving Social Security numbers, driver's license numbers, or California identification card numbers. Noticeably excluded from the types of personal information where identity theft protection should be offered are breaches involving: account numbers or credit or debit card numbers, in combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information; health insurance information; and information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.[27]

In 2015, Connecticut followed California and passed a law affirmatively requiring: "appropriate identity theft prevention services and, if applicable, identity theft mitigation services" for at least one year, and, later, effective October 1, 2018,

---

[26] . CAL. CIV. CODE § 1798.82(d)(2)(G).

[27] . *Id.* § 1798.82(h).

extended that obligation to twenty-four months.[28] It is important to note that the Connecticut law, like California, **does not require** credit monitoring in all cases, but instead requires "appropriate identity theft prevention services."[29] Connecticut's former Attorney General George Jepsen stated the following, in connection with the announcement of the 2015 version of the Connecticut law:

> The bill also calls for companies who experience breaches to provide no less than one year [as of October 1, 2018, twenty-four months] of identity theft prevention services. This requirement sets a floor for the duration of the protection and *does not state explicitly what features the free protection must include.* I continue to have enforcement authority to seek more than one year's protection—and to seek broader kinds of protection—where circumstances warrant. Indeed, in matters involving breaches of highly sensitive information, like Social Security numbers, my practice has been to demand two years of protections. I intend to continue to that practice.[30]

The clear message from the Connecticut law, and one which appears to be gaining additional traction in this space, is that organizations should not necessarily rely solely on credit monitoring and need to determine what identity theft

---

28 . CONN. GEN. STAT. § 36a-701b(b)(2)(B).

29 . *Id*.

30 . George Jepsen, *Statement from [former] AG Jepsen on Final Passage of Data Breach Notification and Consumer Protection Legislation*, STATE OF CONN. OFFICE OF THE ATTORNEY GEN. (June 2, 2015), https://portal.ct.gov/AG/Press-Releases-Archived/2015-Press-Releases/Statement-from-AG-Jepsen-on-Final-Passage-of-Data-Breach-Notification-and-Consumer-Protection-Legisl (emphasis added).

prevention service would be appropriate under the circumstances.

Many jurisdictions outside of the US do not permit the use of credit monitoring solutions for data subjects. Some alternative products may be available to those jurisdictions such as dark web monitoring or identify theft protection packages.

It should be noted, however, that breach notification laws across jurisdictions change frequently, and organizations should be sure to include a review of potentially applicable credit monitoring and identity theft protection requirements in their incident response. in accordance with the advice of counsel, including counsel in jurisdictions outside the United States if the incident has an international aspect Regardless of whether the credit monitoring services are voluntarily offered or required, organizations should consider incorporating into their IRPs a budget line to cover the cost of providing credit monitoring services to affected persons. If, however, credit monitoring is not appropriate, then the significant cost of the service can be reallocated to enhanced employee training, cyber enhancements, and the completion of a thorough risk assessment of cyber vulnerabilities.

G. PCI-Related Considerations

In May of 2018, the Payment Card Industry Security Standards Council promulgated Version 3.2.1 of the Data Security Standard ("PCI DSS" or "Standard") with requirements regarding actions to take in the event of a breach of payment card-related information. Not all provisions are listed here, but, for those subject to PCI DSS, there are key provisions worth mentioning. For instance, the Standard reminds entities handling payment card industry information of the importance of adhering to PCI DSS Requirement 12.10: "Implement an incident response plan. Be prepared to respond

immediately to a system breach."[31] The guidance for Requirement 12.10 goes on to state, "Without a thorough security incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as new legal liabilities."[32] Requirement 12.10.2 requires that the plan be reviewed and tested at least annually.[33]

The PCI DSS requirements are widely accepted as industry-standard best practices. Under fact patterns where they apply, they are likely to be viewed as setting a baseline for reasonableness in the handling of payment card information. Consequently, organizations and their counsel should take particular care to assess whether an organization's handling of payment card information complies with them.

---

[31] . PAYMENT CARD INDUS. SEC. STANDARDS COUNCIL, DATA SECURITY STANDARD 113 (Ver. 3.2.1 May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1510781420590.

[32] . *Id*.

[33] . *Id.* Seemingly implicit in these standards is the assumption that organizations will be able, within their own systems, to isolate or mitigate a breach without causing loss of evidence; have protocols for notifying business partners, such as payment card brands, merchant banks, and others whose notification is required by contract or law; and have a process for engaging a Payment Card Industry Forensics Investigator ("PFI") prior to any occurrence, so that the PFI can be notified immediately upon recognition of a breach. Importantly, the PFI must be on a PCI-DSS-approved list, and—to ensure independence—cannot be already providing PCI services to the organization experiencing the breach.

VI. **BASIC NOTIFICATION REQUIREMENTS**

A. Introduction

In most cases, the determination of whether a data breach has occurred and whether notice is required will depend upon the dictates of applicable state data breach notification laws. In turn, the applicability of state data breach notification laws will depend upon the residency of the individuals impacted by the data incident, and not, as one might think, the organization's state and/or country or other jurisdiction of incorporation or principal place of business.

Once the organization has determined the residency of all impacted individuals, then it can determine which state data breach notification laws apply and whether, after investigation, the facts of the incident support a conclusion that a data breach has occurred as defined by state law. If the data incident does rise to the level of a data breach, then several questions follow:

- Is notification required?
- To whom must notification be made?
- When must notification be made?
- What must be included in the notification?

The next section offers guidance in answering these questions and navigating key notice logistics. Although providing similarly comprehensive guidance for jurisdictions outside the U.S. is beyond the scope of this *Guide*, this section does highlight some considerations in key jurisdictions outside the U.S. for the purpose of illustrating the need to keep foreign legal requirements top-of-mind when dealing with incidents that have an international aspect. In reviewing the guidance offered below, please note that the summary and overview of state notice requirements is only current as of the date of this publication. Given the recent regularity with which state legislators and (derivatively) regulators have been amending

data breach notification laws, organizations should consult legal counsel in the appropriate jurisdictions and scrutinize the relevant state statutes and state websites for information regarding any changes or amendments to the requirements and rules discussed below.

B. *Has a Breach of Personally Identifiable Information Occurred that Requires Notification?*

In evaluating whether a breach (as defined by law) has occurred that requires notification, an important threshold consideration is whether the incident involves PII as defined by applicable state law, or "personal data" as defined by the GDPR or similar comprehensive privacy or data protection laws. The definition of PII varies among states and continues to evolve. For instance, biometric data is treated as PII in some states, but not in others. And some states treat a credit card number as PII, while others do so only if the credit card number is accessed or acquired in combination with the PIN, access code, expiration date, or security code (i.e., CVV). Further, some states exclude from the definition of PII social security numbers that have been truncated or partially redacted (i.e., only the last 4 digits are visible). These are just a few examples of the variances in the definition of PII across state laws. Accordingly, when analyzing whether a "breach" has occurred that requires notification, it is imperative to evaluate the current definition of PII in each applicable jurisdiction.

After evaluating whether protected PII has been impacted by the data incident, the next question to answer is whether the protected PII has been "breached," as defined by relevant law. Not surprisingly, the definition of "breach" varies state by state and similarly continues to evolve. That said, most states define a "breach" *generally* as the unauthorized *acquisition* of protected PII. However, several states and Puerto Rico consider the and some include unauthorized access to (versus

[34] See Ala. Code § 8-38-2(1); Alaska Stat. § 45.48.090(1); Ariz. Rev. Stat. § 18-551(1); Ark. Code Ann. § 4-110-103(1); Cal. Civ. Code § 1798.82(g);

~~the full-scale acquisition of) protected PII alone sufficient to constitute a "breach."[26] And, yet, another small handful of states include~~unencrypted computerized data containing PII in their "breach" definition (in addition to the unauthorized acquisition of) the unauthorized use, illegal use, or unauthorized release of protected PII.[35] Therefore, once it is determined that protected PII has been impacted by the data incident, analysis must be performed to assess whether the facts and forensic findings of the data incident establish, or at least indicate, that the protected PII was accessed, acquired, used, or released without authorization, and whether such

§ 18-551(1); Ark. Code Ann. § 4-110-103(1); Cal. Civ. Code § 1798.82(g); Colo. Rev. Stat. § 6-1-716(1)(h); Conn. Gen. Stat. § 36a-701b(a)(1); Del. Code Ann. tit. 6, § 12B-101(1); D.C. Code § 28-3851(1); Ga. Code Ann. § 10-1-911(1) (applies only to Information Brokers and Data Collectors); Haw. Rev. Stat. § 487N-1; Idaho Code § 28-51-104(2); 815 Ill. Comp. Stat. 530/5; Ind. Code § 24-4.9-2-2(a); Iowa Code § 715C.1(1); Kan. Stat. Ann. § 50-7a01(h); Ky. Rev. Stat. Ann. § 365.732(1)(a); La. Stat. Ann. § 51:3073(2); Me. Rev. Stat. Ann. tit. 10, § 1347(1); Md. Code Ann., Com. Law § 14-3504(a); Mass. Gen. Laws ch. 93H, § 1(a); Mich. Comp. Laws § 445.63(b); Minn. Stat. § 325E.61(1)(d); Miss. Code Ann. § 75-24-29(2)(a); Mo. Ann. Stat. § 407.1500(1)(1); Mont. Code Ann. § 30-14-1704(4)(a); Neb. Rev. Stat. § 87-802(1); Nev. Rev. Stat. Ann. § 603A.020; N.H. Rev. Stat. Ann. § 359-C:19(V); N.M. Stat. Ann. § 57-12C-2(D); N.C. Gen. Stat. § 75-61(14); N.D. Cent. Code § 51-30-01(1); Ohio Rev. Code Ann. § 1349.19(A)(1); Okla. Stat. tit. 24, § 162(1); Or. Rev. Stat. § 646A.602(1); 73 Pa. Stat. § 2302; 11 R.I. Gen. Laws § 11-49.3-3(a)(1); S.C. Code Ann. § 39-1-90(D)(1); S.D. Codified Laws § 22-40-19(1); Tenn. Code Ann. § 47-18-2107(a)(1); Tex. Bus. & Com. Code Ann. § 521.053(a); Utah Code Ann. § 13-44-102(1); Vt. Stat. Ann. tit. 9, § 2430(13)(A); Va. Code Ann. § 18.2-186.6(A); Wash. Rev. Code § 19.255.005(1) and § 19.255.010(1)(2) (eff. 3/1/2020); W. Va. Code § 46A-2A-101(1), (6); Wis. Stat. § 134.98(2); Wyo. Stat. Ann. § 40-12-501(a)(i).

[35] . See Conn. Gen. Stat. § 36a-701b(a)(1); Fla. Stat. § 501.171(1)(a); N.J. Stat. Ann. § 56:8-161; N.Y. Gen. Bus. Law § 899-aa(1)(c); P.R. Laws Ann. tit. 10, § 4051(c); 11 R.I. Gen. Laws § 11-49.3-3(a)(1). *See also* MASS. GEN. LAWS ch. 93H, § 1(a); ME. REV. STAT. ANN. tit. 10, § 1347(1); N.C. GEN. STAT. § 75-61(14); P.R. LAWS ANN. tit. 10, § 4051(c).

access, acquisition, use, or release triggers a "breach" under relevant state law.

After establishing unauthorized access or acquisition, the majority of states require the "breach" analysis to be taken one step further—to assess whether the unauthorized access or acquisition has compromised the security, confidentiality, or integrity of the protected PII. In these states, a "breach" only occurs where there has been the unauthorized access or acquisition of protected PII *that compromises* the security, confidentiality, or integrity of that PII.[36] If the facts indicate there has been no compromise to the security, confidentiality, or integrity of the PII resulting from the unauthorized access or acquisition, then it is possible to conclude no "breach" has occurred;[37] however, such a conclusion necessitates caution

---

[36] . *See* ALASKA STAT. § 45.48.090(1); ARIZ. REV. STAT. § 18-551(1); ARK. CODE ANN. § 4-110-103(1); CAL. CIV. CODE § 1798.82(g); COLO. REV. STAT. § 6-1-716(1)(h); DEL. CODE ANN. tit. 6, § 12B-101(1); D.C. CODE § 28-3851(1); GA. CODE ANN. § 10-1-911(1) (applies only to Information Brokers and Data Collectors); IDAHO CODE § 28-51-104(2); 815 ILL. COMP. STAT. 530/5; IND. CODE § 24-4.9-2-2(a); IOWA CODE § 715C.1(1); KAN. STAT. ANN. § 50-7a01(h); KY. REV. STAT. ANN. § 365.732(1)(a); LA. STAT. ANN. § 51:3073(2); ME. REV. STAT. ANN. tit. 10, § 1347(1); MD. CODE ANN., COM. LAW § 14-3504(a); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.63(b); MINN. STAT. § 325E.61(1)(d); MO. ANN. STAT. § 407.1500(1)(1); MONT. CODE ANN. § 30-14-1704(4)(a); NEB. REV. STAT. § 87-802(1), (5); NEV. REV. STAT. ANN. § 603A.020; N.H. REV. STAT. ANN. § 359-C:19(V); N.J. STAT. ANN. § 56:8-161; N.M. STAT. ANN. § 57-12C-2(D); N.Y. GEN. BUS. LAW § 899-aa(1)(c); OHIO REV. CODE ANN. § 1349.19(A)(1); OKLA. STAT. tit. 24, § 162(1); OR. REV. STAT. § 646A.602(1); 73 PA. CONS. STAT. § 2302; P.R. LAWS ANN. tit. 10, § 4051(c); 11 R.I. GEN. LAWS § 11-49.3-3(a)(1); S.C. CODE ANN. § 39-1-90(D)(1); S.D. CODIFIED LAWS § 22-40-19(1); TENN. CODE ANN. § 47-18-2107(a)(1); TEX. BUS. & COM. CODE ANN. § 521.053(a); UTAH CODE ANN. § 13-44-102(1); VT. STAT. ANN. tit. 9, § 2430(12)(A); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(1)—(2); W. VA. CODE § 46A-2A-101(1), (6); WYO. STAT. ANN. § 40-12-501(a)(i).

[37] . There are a few states—namely, Alabama, Connecticut, Florida, Hawaii, Mississippi, North Carolina, and Wisconsin—that do not require an evaluation of "compromise" (as a concept separate from "harm" as

and close scrutiny of the facts, because in many instances the mere fact that there was *unauthorized* access to or acquisition of the protected PII means necessarily the security, confidentiality, or integrity of that PII has been arguably compromised.

But analysis must not stop there. Even though an investigation may have revealed facts that suggest a data "breach" has likely occurred, several common exceptions may apply that could place the data incident squarely outside the definition of a data breach and/or that obviate the need for notification under the law. These include: there is no reasonable likelihood of harm; the personal information impacted was encrypted; and the data breach was the result of the good-faith access or acquisition by an employee or agent of the organization. Each of these is discussed in greater detail below. Finally, other exceptions may apply depending on the specific state law or the type of organization (e.g., if the organization has an internal policy; if the organization is a financial institution; if the organization is an insurance company; or if the organization falls under the purview of the Gramm-Leach-Bliley Act (GLBA) or HIPAA)).

1. Risk to Individual's Rights and Freedoms is Unlikely

Under the GDPR, personal data breaches are reportable to the regulator where there is likely to be a risk to individual's rights and freedom.[38] The personal data breach is reportable to

discussed in the following section), but instead deem unauthorized access to or acquisition of the protected PII alone sufficient to constitute a "breach"—barring other exceptions (as discussed in the following sections). *See* ALA. CODE § 8-38-2(1); CONN. GEN. STAT. § 36a-701b(a)(1); FLA. STAT. § 501.171(1)(a); HAW. REV. STAT. § 487N-1; MISS. CODE ANN. § 75-24-29(2)(a); N.C. GEN. STAT. § 75-61(14); WIS. STAT. § 134.98(2).

38 GDPR, supra note 1 and 2, Art. 33 (1).

affected individuals where it is likely to result in a *high* risk to the rights and freedoms of individuals.[39] The only exception is therefore where there it is unlikely that there is a risk to individual's rights and freedoms presented from the breach.

The European Data Protection Board ("EDPB") has issued a number guidance notes on how to interpret this threshold. The EDPB suggests that immediately upon becoming aware of a breach, the data controller should assess the risk that could result from the incident. The examples given of damage which may result in a high risk to the rights and freedoms of individuals are discrimination, identity theft or fraud, financial loss and damage to reputation. The EDPB also states that where the breach involves personal data revealing racial or ethnic origin, political opinion, religion or philosophical beliefs, trade union membership, genetic data, data concerning health or sex life, criminal offenses or convictions, the likelihood of any such risk to data subjects is likely to be higher.

Generally, the more sensitive the personal data or the broader the combination of personal data categories, the higher the risk of harm will be to the individuals affected; however, consideration must also be given to the specific circumstances and the potential consequences of the personal data breach. An individual instance of personal data which are not sensitive, when combined could cause significant harm, for example when able to be used for the purposes of identity theft.[40]

For other international jurisdictions, there may be no risk of harm threshold and notification requirements may be automatically triggered without any risk of harm analysis, for example in India, South Korea, Turkey, and some African jurisdictions.

39 GDPR, supra note 1 and 2, Art. 34 (1).

40 See European Data Protection Board Guidelines 9/2022 on personal data breach notification under GDPR Version 2.0 28 March 2023.

1. No Reasonable Likelihood of Harm Exists

In many states, notification may be avoided if, *after investigation*, the organization has established or has a reasonable basis to conclude that there is no reasonable likelihood that harm to the impacted individuals has resulted or will result from the breach. Thirty-six states recognize some form of this exception[41] (*see* Table VI.B.1(A) immediately below).

Table VI.B.1(A):
"No Reasonable Likelihood of Harm" Exception

States recognizing the no-reasonable-likelihood-of-harm exception	Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan,

[41] . *See* ALA. CODE § 8-38-5(a); ALASKA STAT. § 45.48.010(c); ARIZ. REV. STAT. § 18-552(J); ARK. CODE ANN. § 4-110-105(d); COLO. REV. STAT. § 6-1-716(2)(a); CONN. GEN. STAT. § 36a-701b(b)(1); DEL. CODE ANN. tit. 6, § 12B-102(a); FLA. STAT. § 501.171(4)(c); HAW. REV. STAT. § 487N-1; IDAHO CODE § 28-51-105(1); IND. CODE § 24-4.9-3-1(a); IOWA CODE § 715C.2(6); KAN. STAT. ANN. § 50-7a01(h); KY. Rev. Stat. Ann. § 365.732(2); LA. STAT. ANN. § 51:3074(I); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MD. CODE ANN., COM. LAW § 14-3504(b)(1)—(2); MICH. COMP. LAWS § 445.72(1); MISS. CODE ANN. § 75-24-29(3); MO. ANN. STAT. § 407.1500(2)(5); Mont. Code. Ann. § 30-14-704(4)(A); N.C. GEN. STAT. § 75-61(14); NEB. REV. STAT. § 87-803(1); Nev. Rev. Stat. Ann. § 603A.020; N.H. REV. STAT. ANN. § 359-C:20(I)(a); N.J. STAT. ANN. § 56:8-163(a); N.C. GEN. STAT. § 75-61(14); N.M. Stat. Ann. § 57-12C-2(D); OKLA. STAT. tit. 24, § 163(A)—(B); OR. REV. STAT. § 646A.604(7); 73 PA. CONS. STAT. § 2302; 11 R.I. GEN. LAWS § 11-49.3-4(a)(1); S.C. CODE ANN. § 39-1-90(A); S.D. CODIFIED LAWS § 22-40-20; Tenn Code Ann. §47-18-2107(a)(1); UTAH CODE ANN. § 13-44-202(1)(a)—(b); VT. STAT. ANN. tit. 9, § 2435(d); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(1); W. VA. CODE § 46A-2A-102(a)—(b); WIS. STAT. § 134.98(2)(cm)(1); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

	Mississippi, Missouri, Nebraska, New Hampshire, New Jersey, New York, North Carolina, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming

As discussed in greater detail below, what constitutes "reasonable likelihood of harm" varies from state to state, with some states offering greater guidance and others offering none (*see* Table VI.B.1(B): Varying Degrees of Specificity Regarding the Meaning of "Reasonable Likelihood of Harm").

On one end of the spectrum, ten states offer little to no guidance on the meaning of "reasonable likelihood of harm": Alabama, Alaska, Arkansas, Connecticut, Louisiana, Mississippi, Oregon, Pennsylvania, South Dakota, and Washington.[42] These states provide only generally that notification is *not* required if, after reasonable investigation, the organization determines "there is not a reasonable likelihood of harm" to the impacted individuals. As the determination of whether there is reasonable likelihood of harm to the impacted individuals in these ten states is left to the organization, such a determination should be made on a case-by-case basis within the context of the facts of the incident and the findings of the forensic investigation. Notably, in the case of Connecticut, the organization must make such determination in consultation with relevant local, state, or federal law enforcement.

Other states offer more clarity as it relates to the "no harm" exception. For example, Florida, Hawaii, Indiana, Kansas, Massachusetts, Michigan, Missouri, New Mexico, North

[42] . *See* ALA. CODE § 8-38-5(a); ALASKA STAT. § 45.48.010(c); ARK. CODE ANN. § 4-110-105(d); CONN. GEN. STAT. § 36a-701b(b)(1); LA. STAT. ANN. § 51:3074(I); MISS. CODE ANN. § 75-24-29(3); OR. REV. STAT. § 646A.604(8); 73 PA. CONS. STAT. § 2302; S.D. CODIFIED LAWS § 22-40-20; WASH. REV. CODE § 19.255.010(1-2).

Carolina, Oklahoma, Rhode Island, South Carolina, Utah, Vermont, Virginia, West Virginia, and Wisconsin define "harm" in terms of identity theft, fraud, financial harm, or other illegal use.[43] In these fifteen states, notification is not required if, after reasonable investigation, the organization determines the breach has not resulted or is not reasonably likely to result in identity theft, fraud, or other illegal use. Arizona, Iowa, and Florida, tie "harm" to economic loss.[44] In these three states, a data incident only rises to the level of an actionable "breach" if it "materially" compromises the security or confidentiality of the personal information *and* is reasonably likely to cause economic loss or financial harm to an individual.

Eleven other states use a slightly different metric. In Colorado, Delaware, Idaho, Maine, Maryland, Nebraska, New Hampshire, New Jersey, New York, Vermont, and Wyoming, the "no harm" exception is generally defined by the actual or potential misuse of the personal information.[45] In these eleven states, notice is *not* required if, after reasonable investigation, the organization simply determines that the misuse of the

[43] . FLA. STAT. § 501.171(4)(c); HAW. REV. STAT. § 487N-1; IND. CODE § 24-4.9-3-1(a); KAN. STAT. ANN. § 50-7a01(h); MICH. COMP. LAWS § 445.72(1); MO. ANN. STAT. § 407.1500(2)(5); N.M. STAT. ANN. § 57-12C-6(C); N.C. GEN. STAT. § 75-61(14); OKLA. STAT. tit. 24, § 163(A)(B); 11 R.I. GEN. LAWS § 11-49.3-4(a)(1); S.C. CODE ANN. § 39-1-90(A); UTAH CODE ANN. § 13-44-202(1)(a)—(b); VT. STAT. ANN. tit. 9, § 2435(d); VA. CODE ANN. § 18.2-186.6(B); W. VA. CODE § 46A-2A-102(a)—(b); WIS. STAT. § 134.98(2)(cm).

[44] . ARIZ. REV. STAT. § 18-552(J); FLA. STAT. § 501.171(4)(c); IOWA CODE § 715C.2(6).

[45] . COLO. REV. STAT. § 6-1-716(2)(a); DEL. CODE ANN. tit. 6, § 12B-102(a); IDAHO CODE § 28-51-105(1); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MD. CODE ANN., COM. LAW § 14-3504(b)(2); NEB. REV. STAT. § 87-803(1); N.H. REV. STAT. ANN. § 359-C:20(I)(a); N.J. STAT. ANN. § 56:8-163(a); N.Y. GEN. BUS. LAW § 899-aa (1)(c), (2)(a); VT. STAT. ANN. tit. 9, § 2435(d); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

personal information has not occurred and/or is not reasonably likely to occur.

Table VI.B.1(B): Varying Degrees of Specificity Regarding the Meaning of "Reasonable Likelihood of Harm"

Meaning of "Reasonable Likelihood of Harm"	**States**
Reasonable likelihood of harm = **not defined**, explained, or qualified	Alabama, Alaska, Arkansas, Connecticut, Louisiana, Mississippi, Oregon, Pennsylvania, South Dakota, Washington[46]
Reasonable likelihood of harm = reasonably likely the personal information has been or will be **misused**	Colorado, Delaware, Idaho, Maine, Maryland, Nebraska, New Hampshire, New Jersey, New York, Vermont, Wyoming[47]

[46] . *See* ALA. CODE § 8-38-5(a); ALASKA STAT. § 45.48.010(c); ARK. CODE ANN. § 4-110-105(d); CONN. GEN. STAT. § 36a-701b(b)(1); LA. STAT. ANN. § 51:3074(I); MISS. CODE ANN. § 75-24-29(3); OR. REV. STAT. § 646A.604(7); 73 PA. CONS. STAT. § 2302; S.D. CODIFIED LAWS § 22-40-20; WASH. REV. CODE § 19.255.010(-2).

[47] . COLO. REV. STAT. § 6-1-716(2)(a); DEL. CODE ANN. tit. 6, § 12B-102(a); IDAHO CODE § 28-51-105(1); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MD. CODE ANN., COM. LAW § 14-3504(b)(2); NEB. REV. STAT. § 87-803(1); N.H. REV. STAT. ANN. § 359-C:20(I)(a); N.J. STAT. ANN. § 56:8-163(a); VT. STAT. ANN. tit. 9, § 2435(d); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

Meaning of "Reasonable Likelihood of Harm"	States
Reasonable likelihood of harm = reasonably likely to result in **identity theft, fraud**, **financial harm**, or other **illegal use** of the personal information	Florida, Hawaii, Indiana, Kansas, Massachusetts, Michigan, Missouri, New Mexico, New York, North Carolina, Oklahoma, Rhode Island, South Carolina, Utah, Vermont, Virginia, West Virginia, Wisconsin[48]
Reasonable likelihood of harm = reasonably likely to cause substantial **economic loss** or **financial harm** to the individual	Arizona, Florida, Iowa[49]

As always, careful scrutiny should be paid to each applicable state law and the nuances that may exist among state laws regarding this exception, especially if the incident impacts residents in more than one state.

If, after investigation, the organization determines there is no reasonable likelihood of harm and, consistent with that conclusion, decides not to notify impacted individuals, twelve states require the organization to document that determination and maintain that written record for three to five years,

48 . FLA. STAT. § 501.171(4)(c); HAW. REV. STAT. § 487N-1; IND. CODE § 24-4.9-3-1(a); KAN. STAT. ANN. § 50-7a01(h); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.72(1); MO. ANN. STAT. § 407.1500(2)(5); N.M. STAT. ANN. § 57-12C-6(C); N.Y. GEN. BUS. LAW § 899-aa (1)(c), (2)(a); N.C. GEN. STAT. § 75-61(14); N.Y. Gen. Bus. Law § 899-aa(2)(a); OKLA. STAT. tit. 24, § 163(A)(B); 11 R.I. GEN. LAWS § 11-49.3-4(a)(1); S.C. CODE ANN. § 39-1-90(A); UTAH CODE ANN. § 13-44-202(1)(a)—(b); VT. STAT. ANN. tit. 9, § 2435(d); VA. CODE ANN. § 18.2-186.6(B); W. VA. CODE § 46A-2A-102(a)—(b); WIS. STAT. § 134.98(2)(cm).

49 . ARIZ. REV. STAT. § 18-552(J); FLA. STAT. § 501.171(4)(c); IOWA CODE § 715C.2(6).

depending on the state (*see* Table VI.B.1(C) immediately below).

Table VI.B.1(C): States Requiring Documentation of "No Reasonable Likelihood of Harm" Determination

States Requiring Documentation	Length of Document Retention
Maryland, South Dakota	3 years[50]
Alabama, Alaska, Arkansas, Florida, Iowa, Louisiana, Missouri, New Jersey, New York, Oregon	5 years[51]

Some states, however, require more than internal documentation when this exception applies. For example, in Connecticut and Florida, the organization must actually "consult with" "relevant federal, state, and local agencies responsible for law enforcement" in arriving at the conclusion that the breach is not likely to result in harm to the impacted individuals.[52] In Alaska, South Dakota, and Vermont, even though an organization need not notify impacted individuals, the organization must nevertheless notify the state attorney general in writing of its determination that there is no reasonable likelihood of harm to the impacted individuals.[53] In Florida, after consultation with law enforcement, the organization is to notify the Florida Department of Legal

50 . *See* MD. CODE ANN., COM. LAW § 14-3504(b)(4); S.D. CODIFIED LAWS § 22-40-20.

51 . *See* ALA. CODE § 8-38-5(f); ALASKA STAT. § 45.48.010(c); ARK. CODE ANN. § 4-110-105(g(1)); FLA. STAT. § 501.171(4)(c); IOWA CODE § 715C.2(6); LA. STAT. ANN. § 51:3074(I); MO. ANN. STAT. § 407.1500(2)(5); N.J. STAT. ANN. § 56:8-163(a); N.Y. GEN. BUS. LAW § 899-aa (1)(c), (2)(a); OR. REV. STAT. § 646A.604(7).

52 . CONN. GEN. STAT. § 36a-701b(b)(1); FLA. STAT. § 501.171(4)(c); OR. REV. STAT. § 646A.604(7) ("may" consult, not required).

53 . ALASKA STAT. § 45.48.010(c); S.D. CODIFIED LAWS § 22-40-20; VT. STAT. ANN. tit. 9, § 2435(d).

Affairs of the "no harm" determination in writing within thirty days of making the determination.[54] Importantly, the notification and consultation required by these very few states may not be considered part of the public record and may not be open to inspection by the public, even upon request.

While it is beyond the scope of this publication generally to address every foreign notification requirement, the ~~European Union's General Data Protection Regulation (~~GDPR~~)~~[44]'s[55] breach notification requirements merit mention here, especially for those entities subject to the jurisdiction of both the U.S. and the EU and due to the proliferation of laws worldwide modeled on the GDPR. Article 33 of the GDPR requires notification to the supervisory authority of a data breach "*unless* the personal data breach is *unlikely to result in a risk to the rights and freedoms of natural persons*."[56] Article 34, the counterpart to Article 33 with regard to the notification obligations to individuals, requires notification of a data breach to the data subjects whose information was compromised *only* "[w]hen the personal data breach is *likely to result in a high risk* to the rights and freedoms of natural persons."[57]

Briefly summarized for comparative context, the GDPR uses different substantive standards for triggering notifications, to some extent incorporating the U.S. standard of "no likely risk of harm" exception followed in many states. The important distinction, however, is that Article 33 establishes a *presumption of harm,* which would have to be rebutted in order *not* to trigger notification to supervisory authorities under Article 33, whereas Article 34 allows for a more traditional risk-of-harm analysis *before* notification obligations to the individual are triggered. In addition, in contrast to U.S. state

54 . FLA. STAT. § 501.171(4)(c).

55 . GDPR, *supra* note 1.

56 . *Id.*, Art. 33(1).

57 . *Id.*, Art. 34(1).

data breach notification statutes, which prioritize and place greater importance on notification to the impacted individuals, GDPR, with its presumption of harm and shorter notification window (discussed below) applicable for notification to regulators, appears to prioritize and place greater importance on notification to the supervisory authority than impacted individuals. Indeed, notification to impacted individuals is only required if the data breach is likely to result in a "high risk" to the rights and freedoms of the impacted individuals and to assist those individuals in taking mitigating steps to protect themselves in the event of a breach.

As a further example, in Canada, mandatory breach notification requirements are governed by a federal privacy statute, the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"),[58] which applies to private-sector organizations across Canada and potentially abroad, when those organizations collect, use or disclose personal information of Canadians in the course of a commercial activity. However, where a province has adopted its own substantially similar law to PIPEDA, the provincial private sector breach notification requirements will apply instead, which is currently the case in Alberta[59] and Quebec.[60]

Unless an exception applies, under PIPEDA organizations must notify the federal Office of the Privacy Commissioner of Canada ("**OPC**")[61] and affected individuals if there is "any breach of security safeguards involving personal information under [the organization's] control" that creates a "real risk of

58 S.C. 2000, c. 5. Notably, significant PIPEDA reform (Bill C-27) is currently in Second Reading before the Canadian Parliament and is expected to be passed in late 2023 or 2024.

59 Personal Information Protection Act, SA 2003, c P-6.5.

60 Act respecting the protection of personal information in the private sector, CQLR c P-39.1

61 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 10.1(1), <https://canlii.ca/t/7vwj#sec10.1>, retrieved on 2023-04-19.

significant harm" ("**RROSH**") to the individual.[62] PIPEDA defines "significant harm" as including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property, and provides that the sensitivity of the personal information involved and the probability that the personal information has been, is being or will be misused, are factors relevant to determining RROSH.[63] The determination of whether there is RROSH must be made on a case-by-case basis.

Under the privacy statute in Alberta, organizations must notify the province's privacy commissioner in the event of any "loss of or unauthorized access to or disclosure of the personal information" if there is a RROSH.[64] Under the privacy statute in Quebec, organizations must notify the province's privacy commissioner and affected individuals if there is "access", "use", "communication" or "loss" of personal information not authorized by law or any other breach of the protection of personal information, if the incident presents a "risk of serious injury," which is currently understood to be the same threshold as RROSH.[65] Other international jurisdictions seem to prioritize notification to individuals, such as Mexico and South Korea, where regulatory notification may not be required even when individual notice is required.

2. The Personal Information Was Encrypted

62 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 10.1(3), <https://canlii.ca/t/7vwj#sec10.1>, retrieved on 2023-04-19.

63 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, ss 10.1(7)-(8), <https://canlii.ca/t/7vwj#sec10.1>, retrieved on 2023-04-19.

64 Personal Information Protection Act, SA 2003, c P-6.5, s 34.1, <https://canlii.ca/t/81qp#sec34.1>, retrieved on 2023-04-19.

65 Act respecting the protection of personal information in the private sector, CQLR c P-39.1, s 3.5, <https://canlii.ca/t/xpm#sec3.5>, retrieved on 2023-04-19.

Because of advancements in encryption technology, virtually all U.S. jurisdictions now generally distinguish between encrypted and unencrypted personal information when defining what constitutes a "data breach" requiring notification.[66]

If personal information (or some element of personal information) was "encrypted" when breached, depending on the state law, then: (a) such encrypted personal information is excluded from the definition of triggering personal information; (b) the data incident falls outside the definition of a "data breach;" *or* (c) the data incident is exempted from any disclosure obligation. Although varying definitions exist, encryption generally refers to the use of a security technology

---

66 . *See* ALA. CODE § 8-38-2(6)(b)(2); ALASKA STAT. § 45.48.090(7); ARIZ. REV. STAT. §18-551(1)(a),(3); ARK. CODE ANN. § 4-110-103(7); CAL. CIV. CODE § 1798.82(a); COLO. REV. STAT. § 6-1-716(1)(d), (g)(I)(A), (h); CONN. GEN. STAT. § 36a-701b(a); DEL. CODE ANN. tit. 6, § 12B-101(1); D.C. CODE § 28-3851(1); FLA. STAT. § 501.171(1)(g)(2); GA. CODE ANN. § 10-1-911(6); HAW. REV. STAT. § 487N-1; IDAHO CODE § 28-51-104(5); 815 ILL. COMP. STAT. 530/5; IND. CODE § 24-4.9-2-2(b)(2); IOWA CODE § 715C.1(11); KAN. STAT. ANN. § 50-7a01(b), (g)—(h); KY. REV. STAT. ANN. § 365.732(1)(a); LA. STAT. ANN. § 51:3073(4); ME. REV. STAT. ANN. tit. 10, § 1347(6); MD. CODE ANN., COM. LAW § 14-3501(c), (e)(1)(i); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.72(1); MINN. STAT. § 325E.61(1)(a)(e); MISS. CODE ANN. § 75-24-29(2)(a); MO. ANN. STAT. § 407.1500(1)(9); MONT. CODE ANN. § 30-14-1704(1); NEB. REV. STAT. § 87-802(1), (5); NEV. REV. STAT. ANN. § 603A.040; N.H. REV. STAT. ANN. § 359-C:19(IV)(a); N.J. STAT. ANN. § 56:8-161(10); N.M. STAT. ANN. § 57-12C-2(C)(1), (D); N.Y. GEN. BUS. LAW § 899-aa(1)(b); N.C. GEN. STAT. § 75-61(14); N.D. CENT. CODE § 51-30-01(1); OHIO REV. CODE ANN. § 1349.19(A)(7); OKLA. STAT. tit. 24, § 162(1), (3), (6); OR. REV. STAT. § 646A.602(11)(a); 73 PA. CONS. STAT. § 2302; P.R. LAWS ANN. tit. 10, § 4051(a); 11 R.I. GEN. LAWS § 11-49.3-3(a)(1), (8); S.C. CODE ANN. § 39-1-90(A), (D); S.D. CODIFIED LAWS § 22-40-19(1)—(2); TENN. CODE ANN. § 47-18-2107(a)(1), (2); TEX. BUS. & COM. CODE ANN. §§ 521.002(a)(2), 521.053(a); UTAH CODE ANN. § 13-44-102(4); VT. STAT. ANN. tit. 9, § 2430(5); VA. CODE ANN. § 18.2-186.6(A-C); WASH. REV. CODE § 19.255.010(1)—(2); W. VA. CODE § 46A-2A-101(1),(3),(6); WIS. STAT. § 134.98(1)(b); WYO. STAT. ANN. § 40-12-501(a)(vii).

or methodology that renders electronic data unusable, unreadable, or indecipherable without the use of a confidential process or key. Although all states differentiate between encrypted and unencrypted data, their treatment of such encrypted or unencrypted data may differ and, therefore, the relevant state statute should be consulted when evaluating whether notice is required in instances where encrypted data has been impacted by a data incident. Importantly, in many states, encrypted data is not considered "encrypted" or exempted from notice if the decryption key was or is reasonably believed to have been accessed or acquired during the breach.

Importantly, for incidents involving data of individuals located in jurisdictions outside the U.S., consideration should be given to whether a similar distinction between encrypted and unencrypted personal information exists under the laws of those other jurisdictions. For example, in Canada, there is no express distinction in privacy statutes between encrypted and unencrypted personal information when considering an organization's notification obligations.

The GDPR does not draw a specific distinction between encrypted or non-encrypted data in relation to the reporting obligations to data protection authorities, although use of encryption and pseudonymization (as discussed below) can be a factor in choosing not to notify affected individuals. It is worth noting the distinction drawn between anonymized and pseudonymized personal data under the GDPR. Fully anonymized data - data which has been anonymized such that it cannot become identifiable personal data in any circumstance (i.e., it cannot be combined with an identifier or key) - is no longer considered to be personal data under the GDPR, and therefore would not be subject to the reporting requirements. Pseudonymized personal data under the GDPR by contrast is personal data which has been made

unidentifiable on its own but can become identifiable personal data when combined with other information (regardless of where this other information is held). Therefore, if a breach relates to the disclosure of pseudonymized personal data, the data breach reporting obligations to data protection authorities may still come into effect, for example if there is a possibility that the threat actor also had access to the relevant key. The EDPB has stated that whilst pseudonymization can reduce the likelihood of individuals being identified in the event of a breach, pseudonymization techniques alone cannot be regarded as making the data unintelligible in the event of a breach.[67]

3. The "Good Faith" Exception for Employees and Agents

Almost all states and the District of Columbia (D.C.) have an exception for the "good faith" access to, or acquisition of, personal information by employees or agents of the organization.[68] Generally, under this exception, facts that

67 See European Data Protection Board Guidelines 9/2022 on personal data breach notification under GDPR Version 2.0 28 March 2023.

68 . *See* ALA. CODE § 8-38-2(1)(a); ALASKA STAT. § 45.48.050; ARIZ. REV. STAT. § 18-551(1)(b); ARK. CODE ANN. § 4-110-103(1)(B); CAL. CIV. CODE § 1798.82(g); COLO. REV. STAT. § 6-1-716(1)(h); DEL. CODE ANN. tit. 6, § 12B-101(1); D.C. CODE § 28-3851(1); FLA. STAT. § 501.171(1)(a); GA. CODE ANN. § 10-1-911(1); HAW. REV. STAT. § 487N-1; IDAHO CODE § 28-51-104(2); 815 ILL. COMP. STAT. 530/5; IND. CODE § 24-4.9-2-2(b)(1); IOWA CODE § 715C.1(1); KAN. STAT. ANN. § 50-7a01(h); KY. REV. STAT. ANN. § 365.732(1)(a); LA. STAT. ANN. § 51:3073(2); ME. REV. STAT. ANN. tit. 10, § 1347(1); MD. CODE ANN., COM. LAW § 14-3504(a)(2); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.63(3)(b); MINN. STAT. § 325E.61(1)(d); MO. ANN. STAT. § 407.1500(1)(1); MONT. CODE ANN. § 30-14-1704(4)(a); NEB. REV. STAT. § 87-802(1); NEV. REV. STAT. ANN. § 603A.020; N.H. REV. STAT. ANN. § 359-C:19(V); N.J. STAT. ANN. § 56:8-161(10);); N.M. STAT. ANN. § 57-12C-2(D); N.Y. GEN. BUS. LAW § 899-aa(1)(c); N.C. GEN. STAT. § 75-61(14); N.D. CENT. CODE § 51-30-01(1); OHIO REV. CODE ANN. § 1349.19(A)(1); OKLA. STAT. tit. 24, § 162(1); OR. REV. STAT. § 646A.602(1)(b); 73 PA. CONS. STAT. § 2302; P.R. LAWS ANN. tit. 10, § 4051(c); 11 R.I. GEN. LAWS § 11-49.3-3(a)(1);

might otherwise cause the organization to conclude that a "data breach" has occurred are neutralized if an investigation reveals that the "breach" was the result of "good faith"—though unauthorized—access to or acquisition of personal information by an employee or agent of the organization. However, in most instances, this exception only applies if: (1) the personal information was not used for a purpose unrelated to the organization's business, and (2) the employee or agent does not make a further willful unauthorized disclosure.

As noted above, consideration should be given to whether a similar exception for "good faith" access to, or acquisition of, personal information exists in other jurisdictions where impacted individuals may be located. For example, in Canada, there is no "good faith" exception for employees. However, whether or not the access to, or acquisition of, personal information was in good faith may be considered as part of the RROSH analysis.

C. Notice Logistics: Audience, Timing, and Content

In the event an exception does not apply, and/or the organization otherwise decides notification is required, the organization must undertake several determinations to ensure that logistics-related requirements, such as audience, timing, and content, have been satisfied under the applicable data breach notification laws. These logistics-related considerations include: (1) to whom notice must be provided (e.g., individuals, state attorneys general, etc.); (2) whether notice must be provided within a specific period of time (e.g., thirty

S.C. CODE ANN. § 39-1-90(D)(1); S.D. CODIFIED LAWS § 22-40-19(1); TENN. CODE ANN. § 47-18-2107(a)(1); TEX. BUS. & COM. CODE ANN. § 521.053(a); UTAH CODE ANN. § 13-44-102(1)(b); VT. STAT. ANN. tit. 9, § 2430(8)(B); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.005(1); W. VA. CODE § 46A-2A-101(1); WIS. STAT. § 134.98(2)(cm)(2); WYO. STAT. ANN. § 40-12-501(a)(i).

days) and in a specific sequence; and (3) the method and content required for the notice (or notices, if more than one is required). These logistics-related requirements are important aspects of notice—aspects that most state regulators scrutinize with exacting detail. Violation of certain notice-related requirements can result in fines or consumer lawsuits. As such, and especially given state law variations and nuances, organizations should consult the specific language of the applicable state statute(s) and take care in complying with each of these aspects.

1. To Whom Notice Must Be Provided

Generally, there are three groups to whom notice may be required: (1) the individuals who had their personal information accessed or acquired without authorization during the breach; (2) state or other government regulators; and/or (3) credit or consumer reporting agencies.

Depending on the circumstances of the breach, other third parties—such as Vendors, credit card companies, and insurers—may also require notification; however, notification to these other third parties is generally necessitated not by applicable law, but instead by contract. [69] This section discusses notice obligations only as provided by relevant state law. It is important to note, though, that when a data incident occurs, as with the organization's investigation into the incident and

[69] . Depending on the applicable state law, third-party vendors and third-party data brokers, collectors, processors, or aggregators (collectively "third-party vendors") may have notification obligations to the entity that maintains, owns, or licenses the personal information if the third-party vendors suffer a data incident or breach that impacts the personal information of the owner or licensor (or the owner or licensor's customers or employees). If you are a third-party vendor, and you suffer a data incident or breach, you should consult the applicable state statutes to assess whether you have a statutory obligation to notify the data owner or licensor of a data incident or breach (beyond any contractual obligations you may have).

resulting notice obligations, the organization should consider whether and when it should notify these equally important other third parties. And to the extent contracts exist governing the organization's relationship with these other third parties, it is recommended that these contracts be pulled and closely reviewed at the outset of any data incident.[70]

- Notice to Individuals

  Regardless of the number of state residents impacted, all states require the organization to provide notice to *any* individual impacted by the breach. As discussed in greater detail below, the timing and content of the notice to the impacted individuals varies by state.

- Notice to Regulators

  Unlike notice to individuals, whether the organization must also provide notice to its state or other regulators varies by state and may depend upon the number of state residents impacted by the breach and/or whether the organization is a specially regulated entity. This section will focus on organizations that are *not* specially regulated (e.g., entities that are not financial institutions, or covered entities under HIPAA, etc.). Organizations that are specially regulated should refer to the specific state statutes, as well as any applicable federal statutes, to assess whether and when notice to state and/or federal regulators is required.

With regard to organizations that are not specially regulated, the following thirty-two U.S. states and territories

[70] . A contracts management process that collects metadata on notice requirements contained in Vendor and other third-party agreements can accelerate the review process at the time of an incident.

have laws with requirements regarding notification to regulators: Alabama, Arizona, California, Colorado, Connecticut, Florida, Hawaii, Illinois, Indiana, Iowa, Louisiana, Maine, Maryland, Massachusetts, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Oregon, Rhode Island, South Carolina, South Dakota, Texas, Vermont, Virginia, Washington, and Puerto Rico[71] (*see also* Table VI.C.1(A): U.S. Jurisdictions Requiring Notice to Regulators).

As detailed in Table VI.C.1(A) below, depending on the laws of the jurisdiction(s) implicated by the breach, relevant regulators to whom notice may be required may include: (1) the state attorney general's office; (2) the consumer affairs or consumer protection divisions; and/or (3) the state police.

Of the U.S. states and territories requiring notice to relevant regulators, fourteen require notice to the relevant regulator *regardless* of how many residents have been impacted by the breach[72] (*see* Table VI.C.1(A): U.S. Jurisdictions Requiring

---

[71] . ALA. CODE § 8-38-6; ARIZ. REV. STAT. § 18-552(B)(2)(b); CAL. CIV. CODE § 1798.82(f); COLO. REV. STAT. § 6-1-716(2)(f); CONN. GEN. STAT. § 36a-701b(b)(2); FLA. STAT. § 501.171(3)(a); HAW. REV. STAT. § 487N-2(f); IND. CODE § 24-4.9-3-1(c); IOWA CODE § 715C.2(8); LA. ADMIN. CODE tit. 16, § 701.A; ME. REV. STAT. ANN. tit. 10, § 1348(5); MD. CODE ANN., COM. LAW § 14-3504(h); MASS. GEN. LAWS ch. 93H, § 3(b); MO. ANN. STAT. § 407.1500(2)(8); MONT. CODE ANN. § 30-14-1704(8); NEB. REV. STAT. § 87-803; N.H. REV. STAT. ANN. § 359-C:20(I)(b); N.J. STAT. ANN. § 56:8-163(12)(c); N.M. STAT. ANN. § 57-12C-10); N.Y. GEN. BUS. LAW § 899-aa(8)(a); N.C. GEN. STAT. § 75-65(e1); N.D. CENT. CODE § 51-30-02; OR. REV. STAT. § 646A.604(1)(b); P.R. LAWS ANN. tit. 10, § 4052; 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(K); S.D. CODIFIED LAWS § 22-40-20; VT. STAT. ANN. tit. 9, § 2435(b)(3); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(2)(7).

[72] . CONN. GEN. STAT. § 36a-701b(b)(2); IND. CODE § 24-4.9-3-1(c); LA. ADMIN. CODE tit. 16, § 701.A; ME. REV. STAT. ANN. tit. 10, § 1348(5); MD. CODE ANN., COM. LAW § 14-3504(h); MASS. GEN. LAWS ch. 93H, § 3(b); MONT. CODE ANN. § 30-14-1704(8); NEB. REV. STAT. § 87-803(2); N.H. REV. STAT. ANN. § 359-C:20(I)(b); N.J. STAT. ANN. § 56:8-163(12)(c); N.Y. GEN. BUS. LAW

Notice to Regulators). The other eighteen, however, require notice to the relevant regulator *only if* a certain minimum number of residents have been impacted by the data breach (*see* Table VI.C.1(A): U.S. Jurisdictions Requiring Notice to Regulators). These minimum thresholds range from 250 residents to 1000 or more residents.[73]

Table VI.C.1(A):
U.S. Jurisdictions Requiring Notice to Regulators

§ 899-aa(8)(a); N.C. GEN. STAT. § 75-65(e1); P.R. LAWS ANN. tit. 10, § 4052; VT. STAT. ANN. tit. 9, § 2435(b)(3).

[73] . Ala. Code § 8-38-6(a); ARIZ. REV. STAT. § 18-552(B)(2)(b); CAL. CIV. CODE § 1798.82(f); COLO. REV. STAT. § 6-1-716(2)(f); FLA. STAT. § 501.171(3)(a); HAW. REV. STAT. § 487N-2(f); IOWA CODE § 715C.2(8); MO. ANN. STAT. § 407.1500(2)(8); N.D. CENT. CODE § 51-30-02; OR. REV. STAT. § 646A.604(1)(b); 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(K); S.D. Codified Laws § 22-40-20; VA. CODE ANN. § 18.2-186.6(E); WASH. REV. CODE § 19.255.010(15).

U.S. Jurisdiction	Minimum Threshold Required	To Whom Regulator Notice Must Be Made
Alabama[74]	1000+ residents	Office of the Attorney General
Arizona[75]	1000+ residents	Office of the Attorney General
California[76]	500+ residents	Office of the Attorney General
Colorado[77]	500+ residents	Office of the Attorney General
Connecticut[78]	No minimum / 1+ resident	Office of the Attorney General
Florida[79]	500+ residents	Department of Legal Affairs of the Office of Attorney General
Hawaii[80]	1,000+ residents	Office of Consumer Protection
Illinois[81]	500+ residents	Office of Attorney General
Indiana[82]	No minimum / 1+ resident	Office of the Attorney General
Iowa[83]	500+ residents	Director of the

74 . ALA. CODE § 8-38-6(a).

75 . ARIZ. REV. STAT. § 18-552(B)(2)(b).

76 . CAL. CIV. CODE § 1798.82(f).

77 . COLO. REV. STAT. § 6-1-716(2)(f).

78 . CONN. GEN. STAT. § 36a-701b(b)(2).

79 . FLA. STAT. § 501.171(3)(a).

80 . HAW. REV. STAT. § 487N-2(f).

81 . 815 ILL. COMP. STAT. 530/10

82 . IND. CODE § 24-4.9-3-1(c).

83 . IOWA CODE § 715C.2(8).

U.S. Jurisdiction	Minimum Threshold Required	To Whom Regulator Notice Must Be Made
		Consumer Protection Division of the Iowa Office of Attorney General
Louisiana[84]	No minimum / 1+ resident	Consumer Protection Section of the Louisiana Office of the Attorney General
Maine[85]	No minimum / 1+ resident	Office of the Attorney General
Maryland[86]	No minimum / 1+ resident	Office of the Attorney General
Massachusetts[87]	No minimum / 1+ resident	Office of the Attorney General Director of Consumer Affairs and Business Regulation
Missouri[88]	1,000+ residents	Office of the Attorney General
Montana[89]	No minimum / 1+ resident	Consumer Protection Division of the Montana Office of the Attorney General
Nebraska[90]	No minimum / 1+ resident	Office of the Attorney General

84 . LA. ADMIN. CODE tit. 16, § 701.A.

85 . ME. REV. STAT. ANN. tit. 10, § 1348(5).

86 . MD. CODE ANN., COM. LAW § 14-3504(h).

87 . MASS. GEN. LAWS ch. 93H, § 3(b).

88 . MO. ANN. STAT. § 407.1500(2)(8).

89 . MONT. CODE ANN. § 30-14-1704(8).

90 . NEB. REV. STAT. § 87-803(2).

U.S. Jurisdiction	Minimum Threshold Required	To Whom Regulator Notice Must Be Made
New Hampshire[91]	No minimum / 1+ resident	Office of the Attorney General
New Jersey[92]	No minimum / 1+ resident	Division of State Police in the Department of Law and Public Safety of the State of New Jersey
New Mexico[93]	1,000+ residents	Office of the Attorney General
New York[94]	No minimum / 1+ resident	Office of the Attorney General; New York State Consumer Protection Board of the Department of State; Division of State Police
North Carolina[95]	No minimum / 1+ resident	Consumer Protection Division of the Office of the Attorney General
North Dakota[96]	250+ residents	Office of the Attorney General
Oregon[97]	250+ residents	Oregon Attorney General's Office
Puerto Rico[98]	No minimum / 1+ resident	Department of Consumer Affairs for

91 . N.H. REV. STAT. ANN. § 359-C:20(I)(b).

92 . N.J. STAT. ANN. § 56:8-163(12)(c).

93 . N.M. STAT. ANN. § 57-12C-10.

94 . N.Y. GEN. BUS. LAW § 899-aa(8)(a).

95 . N.C. GEN. STAT. § 75-65(e1).

96 . N.D. CENT. CODE § 51-30-02.

97 . OR. REV. STAT. § 646A.604(1)(b).

98 . P.R. LAWS ANN. tit. 10, § 4052.

U.S. Jurisdiction	Minimum Threshold Required	To Whom Regulator Notice Must Be Made
		Puerto Rico
Rhode Island[99]	500+ residents	Office of the Attorney General
South Carolina[100]	1,000+ residents	Consumer Protection Division of the Department of Consumer Affairs for South Carolina
South Dakota[101]	250+ residents	Office of the Attorney General
Texas[102]	250+ residents	Office of the Attorney General
Vermont[103]	No minimum / 1+ resident	Office of the Attorney General
Virginia[104]	~~1000+ residents~~No minimum / 1+ resident	Office of the Attorney General
Washington[105]	500+ residents	Office of the Attorney General

Beyond minimum thresholds and timing requirements (discussed below), the majority of states and territories requiring notice to relevant regulators also dictate specific or

99 . 11 R.I. GEN. LAWS § 11-49.3-4(a)(2).

100 . S.C. CODE ANN. § 39-1-90(K).

101 . S.D. CODIFIED LAWS § 22-40-20.

102 . TEX. BUS. & COM. CODE ANN. § 521.053(i).

103 . VT. STAT. ANN. tit. 9, § 2435(b)(3).

104 . VA. CODE ANN. § 18.2-186.6(B).

105 . WASH. REV. CODE § 19.255.010(2)(7).

minimum content requirements for these regulator notices. Colorado, Iowa, Puerto Rico, and South Dakota are the only U.S. states or territories (of the thirty-two that require notice to regulators) that do *not* specify what the organization's notice to the relevant regulator should contain in terms of content.[106] As discussed in greater detail below, because the content requirements vary by jurisdiction, organizations should carefully review the relevant statutes when drafting notices to the relevant regulators.

Finally, when preparing for and making notice to a relevant regulator, in addition to the specific statute, the organization should also consult the relevant regulator's website. Consultation with the relevant regulator's website is equally as important as consulting the specific statutory language because regulator websites often have detailed information regarding notice logistics not included in the statutes. For example, the New Jersey State Police website contains a webpage devoted to cyber crimes that contains specific instructions, a telephone number, and a hyperlink for organizations making notice to the Division of State Police that are not contained in the New Jersey data breach notification statute.[107] The North Carolina data breach statute states that the organization must provide notice to the Consumer Protection Division of the North Carolina Attorney General's Office but does not specify how that notice should be made.[108] The website for the Attorney General's Office contains several webpages devoted to security breaches, including one webpage that explains that submission of any notice to the

---

[106] . COLO. REV. STAT. § 6-1-716(2)(f); IOWA CODE § 715C.2(8); P.R. LAWS ANN. tit. 10, § 4052; S.D. CODIFIED LAWS § 22-40-20.

[107] . STATE OF N.J. OFFICE OF THE ATTORNEY GEN., CYBER CRIMES UNIT, N.J. STATE POLICE, http://www.njsp.org/division/investigations/cyber-crimes.shtml (last visited Dec. 2, 2019).

[108] . N.C. GEN. STAT. § 75-65(e1).

Consumer Protection Division of the Attorney General's Office must be made via the specially designated online form and portal created by the division for such notices.[109]

As with the other aspects of breach notification requirements, the organization must consider the notification requirements of any applicable jurisdictions outside the U.S. where individuals whose data is affected reside, as requirements in such jurisdictions may differ from those in the U.S. In Canada, for example, the federal privacy statute, PIPEDA and provincial privacy statute in Quebec require mandatory notification to both affected individuals and the federal and/or Quebec privacy commissioner, as applicable, in prescribed circumstances. PIPEDA also requires, and the Quebec privacy statute allows, organizations to notify other organizations or government institutions if it believes they may be able to reduce or mitigate any harm from the breach.110 In contrast, the privacy statute in Alberta does not require automatic mandatory notifications to affected individuals, but does require notification to the province's privacy commissioner,111 and empowers the privacy commissioner to require notifications to affected individuals.112 There is

---

109 . *See* JOSH STEIN, ATTORNEY GENERAL, *REPORT A SECURITY BREACH*, N.C. DEP'T OF JUST., https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-your-business-from-id-theft/report-a-security-breach/ (last visited Dec. 2, 2019).

110 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 10.2, <https://canlii.ca/t/7vwj#sec10.2>, retrieved on 2023-04-19; Act respecting the protection of personal information in the private sector, CQLR c P-39.1, s 3.5, <https://canlii.ca/t/xpm#sec3.5>, retrieved on 2023-04-19.

111 Personal Information Protection Act, SA 2003, c P-6.5, s 34.1, <https://canlii.ca/t/81qp#sec34.1>, retrieved on 2023-04-19.

112 Personal Information Protection Act, SA 2003, c P-6.5, s 37.1, <https://canlii.ca/t/81qp#sec37.1>, retrieved on 2023-04-19.

no minimum number of affected individuals required to trigger a reporting obligation to relevant privacy commissioners under any Canadian privacy statutes.

- Notice to Credit/Consumer Reporting Agencies

  In providing notice to consumers, and to state regulators in some instances, some jurisdictions also require the organization to contemporaneously provide notice to all credit or consumer reporting agencies, such as Experian, Equifax, and TransUnion. Whether the organization must provide notice to the credit reporting agencies varies by jurisdiction and depends upon the number of residents impacted by the breach and/or whether the organization is a specially regulated entity. This section will focus on organizations that are *not* specially regulated (e.g., entities that are not financial institutions, or covered entities under HIPAA, etc.). Organizations that are specially regulated should refer to the specific federal, state, or territorial statutes to assess whether and when notice to the credit reporting agencies may be required.

With regard to organizations that are not specially regulated, the following states and D.C. have laws with requirements regarding notification to credit or consumer reporting agencies: ~~Alabama, Alaska, Arizona, Colorado, Florida, Georgia,[90] Hawaii, Indiana, Kansas, Kentucky, Maine, Maryland, Massachusetts,~~ Michigan, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, West Virginia, and Wisconsin.[113]

[113].KY. REV. STAT. ANN. § 365.732(7); ME. REV. STAT. ANN. tit. 10, § 1348(4); MD. CODE ANN., COM. LAW § 14-3506(a); MICH. COMP. LAWS § 445.72(8);

With the exception of Massachusetts and South Dakota, these jurisdictions require notification to the credit or consumer reporting agencies *only if* a certain minimum number of residents have been impacted by the data breach. This minimum threshold ranges from 500 to 10,000 or more and varies by jurisdiction (*see* Table VI.C.1(B): U.S. Jurisdictions Requiring Notice to Credit/Consumer Reporting Agencies). Unlike all the other states and D.C., Massachusetts requires the organization to provide notice to the credit or consumer reporting agencies *only if so directed* by the Director of Consumer Affairs and Business Regulation.[114] South Dakota, on the other hand, requires notification to the consumer reporting agencies if just one South Dakota resident is impacted by the data breach.[115]

Table VI.C.1(B): U.S. Jurisdictions Requiring Notice to Credit/Consumer Reporting Agencies

MD. CODE ANN., COM. LAW § 14-3506(a); MICH. COMP. LAWS § 445.72(8); MINN. STAT. § 325E.61(2); MO. ANN. STAT. § 407.1500(2)(8); MONT. CODE ANN. § 30-14-1704(7); NEV. REV. STAT. ANN. § 603A.220(6); N.H. REV. STAT. ANN. § 359-C:20(VI)(a); N.J. STAT. ANN. § 56:8-163(12)(f); N.M. STAT. ANN. § 57-12C-10; N.Y. GEN. BUS. LAW § 899-aa(8)(b); N.C. GEN. STAT. § 75-65(f); OHIO REV. CODE ANN. § 1349.19(G); OR. REV. STAT. § 646A.604(6); 73 PA. CONS. STAT. § 2305; 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(K); S.D. CODIFIED LAWS § 22-40-24; TENN. CODE ANN. § 47-18-2107(g); TEX. BUS. & COM. CODE ANN. § 521.053(h); VT. STAT. ANN. tit. 9, § 2435(c); VA. CODE ANN. § 18.2-186.6(E); W. VA. CODE § 46A-2A-102(f); WIS. STAT. § 134.98(2)(br).

114 . MASS. GEN. LAWS ch. 93H, § 3(b). In this sense the Massachusetts Statute appears to be an anomaly, as it is difficult to envision many circumstances in which such notice would not be directed. Given that it would be reasonable to assume that the Director of Consumer Affairs would almost always require such notice, it may be more expedient simply to notify consumer reporting agencies as a matter of course.

115 . S.D. CODIFIED LAWS § 22-40-24.

U.S. Jurisdictions	Minimum Threshold Required
Minnesota, Rhode Island[116]	500+ residents
Alabama, Alaska, Arizona, Colorado, D.C., Florida, Hawaii, Indiana, Kansas, Kentucky, Maine, Maryland, Michigan, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, Tennessee, Vermont, Virginia, West Virginia, Wisconsin[117]	1,000+ residents
New York[118]	5,000+ residents
Georgia, Texas[119]	10,000+ residents
Massachusetts[120]	No minimum—*only if so directed* by Director of Consumer Affairs and

116 . MINN. STAT. § 325E.61(2); 11 R.I. GEN. LAWS § 11-49.3-4(a)(2).

117 . ALA. CODE § 8-38-7; ALASKA STAT. § 45.48.040(a); ARIZ. REV. STAT. § 18-552(B)(2)(a); COLO. REV. STAT. § 6-1-716(2)(d); D.C. CODE § 28-3852(c); FLA. STAT. § 501.171(5); HAW. REV. STAT. § 487N-2(f); IND. CODE § 24-4.9-3-1(b); KAN. STAT. ANN. § 50-7a02(f); KY. REV. STAT. ANN. § 365.732(7); ME. REV. STAT. ANN. tit. 10, § 1348(4); MD. CODE ANN., COM. LAW § 14-3506(a); MICH. COMP. LAWS § 445.72(8); MO. ANN. STAT. § 407.1500(2)(8); NEV. REV. STAT. ANN. § 603A.220(6); N.H. REV. STAT. ANN. § 359-C:20(VI)(a); N.J. STAT. ANN. § 56:8-163(f); N.M. STAT. ANN. § 57-12C-10; N.C. GEN. STAT. § 75-65(f); OHIO REV. CODE ANN. § 1349.19(G); OR. REV. STAT. § 646A.604(6); 73 PA. CONS. STAT. § 2305; S.C. CODE ANN. § 39-1-90(K); TENN. CODE ANN. § 47-18-2107(g); VT. STAT. ANN. tit. 9, § 2435(c); VA. CODE ANN. § 18.2-186.6(E); W. VA. CODE § 46A-2A-102(f); WIS. STAT. § 134.98(2)(br).

118 . N.Y. GEN. BUS. LAW § 899-aa(8)(b).

119 . GA. CODE ANN. § 10-1-912(d); TEX. BUS. & COM. CODE ANN. § 521.053(h).

120 . MASS. GEN. LAWS ch. 93H, § 3(b).

U.S. Jurisdictions	Minimum Threshold Required
	Business Regulation
South Dakota[121]	No minimum/1+ resident

In all of these states and D.C., assuming the minimum thresholds for impacted residents are met, if PII is compromised, the organization is required to provide notice to "all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis."[122] These "consumer reporting agencies" include Experian, Equifax, and TransUnion. For the most part, the content required for these notices to credit reporting agencies is the same under all state statutes, and includes information on the timing, distribution, and content of the individual consumer notices. However, a few states (Colorado, Maine, and Michigan) also require the notice to the agencies to include the number of impacted residents to whom notice was or will be made.[123] Further, in providing notice to these agencies, state regulations make clear

121 . S.D. CODIFIED LAWS § 22-40-24.

122 . ALA. CODE § 8-38-7; ALASKA STAT. § 45.48.040(a); ARIZ. REV. STAT. § 18-552(B)(2)(a); COLO. REV. STAT. § 6-1-716(2)(d); D.C. CODE § 28-3852(c); FLA. STAT. § 501.171(5); GA. CODE ANN. § 10-1-912(d); HAW. REV. STAT. § 487N-2(f); IND. CODE § 24-4.9-3-1(b); KAN. STAT. ANN. § 50-7a02(f); KY. REV. STAT. ANN. § 365.732(7); ME. REV. STAT. ANN. tit. 10, § 1348(4); MD. CODE ANN., COM. LAW § 14-3506(a); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS § 445.72(8); MINN. STAT. § 325E.61(2); MO. ANN. STAT. § 407.1500(2)(8); NEV. REV. STAT. ANN. § 603A.220(6); N.H. REV. STAT. ANN. § 359-C:20(VI)(a); N.J. STAT. ANN. § 56:8-163(12)(f); N.M. STAT. ANN. § 57-12C-10; N.Y. GEN. BUS. LAW § 899-aa(8)(b); N.C. GEN. STAT. § 75-65(f); OHIO REV. CODE ANN. § 1349.19(G); OR. REV. STAT. § 646A.604(6); 73 PA. CONS. STAT. § 2305; 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(K); S.D. CODIFIED LAWS § 22-40-24; TENN. CODE ANN. § 47-18-2107(g); TEX. BUS. & COM. CODE ANN. § 521.053(h); VT. STAT. ANN. tit. 9, § 2435(c); VA. CODE ANN. § 18.2-186.6(E); W. VA. CODE § 46A-2A-102(f); WIS. STAT. § 134.98(2)(br).

123 . COLO. REV. STAT. § 6-1-716(2)(d); ME. REV. STAT. ANN. tit. 10, § 1348(4); MICH. COMP. LAWS § 445.72(8).

that the organization should not provide the agencies with the names or other PII of the breach notice recipients.

Again, if the incident involves the data of individuals located outside the U.S., the organization should consider any obligations to notify credit/consumer reporting agencies under the laws of those jurisdictions. For example, in Canada, for example, the federal and provincial privacy statutes do not explicitly require organizations to report incidents to credit/consumer reporting agencies, but there is a general requirement under the federal privacy statute, PIPEDA, to notify any third party that may help reduce the risk of harm to affected individuals if the breach otherwise triggers an obligation to notify such individuals.[124] Depending on the circumstances, this may include credit/consumer reporting agencies, banks, credit card companies, payment processors and others.

2. Timing of Notice

When investigating[125] and responding to a data incident, timing is always of paramount importance. Even though few states impose specific time periods to notify impacted individuals, regulators first scrutinize the timing of notification when evaluating whether the organization has satisfied data breach notification laws. It is also one of the very first things consumers and plaintiffs' attorneys scrutinize. Indeed, in regulatory inquiries and privacy litigation alike, the timing of notification to impacted individuals is often one of the most criticized aspects of a data breach, with the impacted individuals wanting to know why the organization didn't notify them sooner.

[124] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 10.2, <https://canlii.ca/t/7vwj#sec10.2>, retrieved on 2023-04-19.
[125]

As such, when determining how swiftly notification must be made (and, therefore, how swiftly the investigation into the data incident must be conducted), there are generally two questions to answer:

- When does the notification clock start to run?
- Once the clock starts to run, how long does the organization have before it must notify impacted individuals?

Both of these criteria are subject to interpretation in most states, as explained below.

- When does the notification clock start to run?

  To reasonably assess when notification must be provided, the point from which the clock starts to run must first be determined by the organization. Though notification laws vary by U.S. jurisdiction, there are generally two points in time during a data incident from which the notification clock could start to run: (1) when the organization first discovers or is first notified of the breach; or (2) after the organization completes a reasonable and prompt investigation to determine whether, in fact, the data incident rises to the level of a "breach."

Thirty-~~three~~five states, D.C., and Puerto Rico start the notification clock when the organization first discovers or is first notified of the breach and following the determination of the scope of the breach. The states joining D.C. and Puerto Rico include: Alaska, Arkansas, California, Florida, Georgia, Hawaii, Illinois, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia and Wisconsin.[126] Generally, those

[126] ALASKA STAT. § 45.48.010(a)(b); ARK. CODE ANN. § 4-110-105(a)(1)(2); CAL. CIV. CODE § 1798.82(a); D.C. CODE § 28-3852(a); FLA. STAT. § 501.171(4);

laws provide that notice shall be provided to the impacted individuals *after* "discovering or being notified of the breach"[127] or, alternatively, *after* the organization "knows or has reason to know of a breach of security."[128]

The remaining U.S. states explicitly start the notification clock running after completion of a reasonable and prompt investigation to determine whether, in fact, a "breach" has occurred. These U.S. states include: Alabama, Arizona, Colorado, Connecticut, Delaware, Idaho, Kansas, ~~Maine, Maryland,~~ Mississippi, Missouri, Nebraska, New Hampshire, New Mexico, South Dakota, Utah, and Wyoming.[129] The key here is the point in time when the investigation reasonably determines that personal information belonging to residents

---

CAL. CIV. CODE § 1798.82(a); D.C. CODE § 28-3852(a); FLA. STAT. § 501.171(4); GA. CODE ANN. § 10-1-912(a); HAW. REV. STAT. § 487N-2(a); 815 ILL. COMP. STAT. 530/10(a); IND. CODE ANN. § 24-4.9-3-3(a); IOWA CODE § 715C.2(1); KY. REV. STAT. ANN. § 365.732(2); LA. STAT. ANN. § 51:3074(E); MD. CODE ANN., COM. LAW § 14-3504(b)(1); MASS. GEN. LAWS ch. 93H, § 3(a)(b); ME. REV. STAT. ANN. tit. 10, § 1348(1); MICH. COMP. LAWS ANN. § 445.72(4); MINN. STAT. § 325E.61(1); MONT. CODE ANN. § 30-14-1704(1); NEV. REV. STAT. ANN. § 603A.220(1); N.J. STAT. ANN. § 56:8-163(12)(a); N.Y. GEN. BUS. LAW § 899-aa(2); N.C. GEN. STAT. § 75-65(a)(b); N.D. CENT. CODE § 51-30-02; OHIO REV. CODE ANN. § 1349.19(B); OKLA. STAT. tit. 24, § 163(A); OR. REV. STAT. § 646A.604(3); 73 PA. CONS. STAT. § 2303(a); P.R. LAWS ANN. tit. 10, § 4052; 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(A); TENN. CODE ANN. § 47-18-2107(b)(c); TEX. BUS. & COM. CODE ANN. § 521.053(b); VT. STAT. ANN. tit. 9, § 2435(b)(1); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(8); W. VA. CODE § 46A-2A-102(a)(c); WIS. STAT. § 134.98(3).

127 . *See, e.g.*, ALASKA STAT. § 45.48.010(a).

128 . *See, e.g.*, MASS. GEN. LAWS ch. 93H, § 3.

129 . ALA. CODE § 8-38-4(a),5(b); ARIZ. REV. STAT. § 18-552(A-B); COLO. REV. STAT. § 6-1-716(2)(a); CONN. GEN. STAT. § 36a-701b(b)(1); DEL. CODE ANN. tit. 6, § 12B-102(a); IDAHO CODE § 28-51-105(1); KAN. STAT. ANN. § 50-7a02(a); MISS. CODE ANN. § 75-24-29(3); MO. ANN. STAT. § 407.1500(2)(1)(C), (5); NEB. REV. STAT. § 87-803(1); N.H. REV. STAT. ANN. § 359-C:20(1)(a); N.M. STAT. ANN. § 57-12C-6(B)(C); S.D. CODIFIED LAWS § 22-40-20; UTAH CODE ANN. § 13-44-202(1)(a)(b); WYO. STAT. ANN. § 40-12-502(a).

has been "breached" as defined by the relevant law of the U.S. jurisdiction.

Table VI.C.2(A):
When Does the Notification Clock Start to Run?

The notification clock is triggered after discovery or notification that personal information of residents has been improperly accessed or compromised, or after the organization knows or has reason to know of a breach of security. Notification in these states must be made without unreasonable delay and in the most expeditious time possible, allowing for the determination of the scope of the breach, and/or determination of the individuals to be contacted, to restore the reasonable integrity of the information system, and consistent with the needs of law enforcement.	Alaska, Arkansas, California, D.C., Florida, Georgia, Hawaii, Illinois, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia, Wisconsin[130]

[130] . ALASKA STAT. § 45.48.010(a)(b); ARK. CODE ANN. § 4-110-105(a)(1)(2); CAL. CIV. CODE § 1798.82(a); D.C. CODE § 28-3852(a); FLA. STAT. § 501.171(4); GA. CODE ANN. § 10-1-912(a); HAW. REV. STAT. § 487N-2(a); 815 ILL. COMP. STAT. 530/10(a); IND. CODE ANN. § 24-4.9-3-3(a); IOWA CODE § 715C.2(1); KY. REV. STAT. ANN. § 365.732(2); LA. STAT. ANN. § 51:3074(E); MASS. GEN. LAWS ch. 93H, § 3(a)(b); ; ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MICH. COMP. LAWS ANN. § 445.72(4); MINN. STAT. § 325E.61(1); MONT. CODE ANN. § 30-14-1704(1); NEV. REV. STAT. ANN. § 603A.220(1); N.J. STAT. ANN. § 56:8-163(12)(a); N.Y. GEN. BUS. LAW § 899-aa(2); N.C. GEN. STAT. § 75-65(a)(b); N.D. CENT. CODE § 51-30-02; OHIO REV. CODE ANN. § 1349.19(B); OKLA. STAT. tit. 24, § 163(A); OR. REV. STAT. § 646A.604(3); 73 PA. CONS. STAT. § 2303(a); P.R. LAWS ANN. tit. 10, § 4052; 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(A); TENN. CODE ANN. § 47-18-2107(b)(c); TEX. BUS. & COM. CODE ANN. § 521.053(b); VT. STAT. ANN. tit. 9, § 2435(b)(1); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(2)(8); W. VA. CODE § 46A-2A-102(a)(c); WIS. STAT. § 134.98(3).

The notification clock is triggered after completion of a reasonable and prompt investigation of the security incident to determine whether, in fact, a "breach" has occurred. In these states, the statutes explicitly allow for a reasonable investigation.	Alabama, Arizona, Colorado, Connecticut, Delaware, Idaho, Kansas, ~~Maine, Maryland,~~ Mississippi, Missouri, Nebraska, New Hampshire, New Mexico, South Dakota, Utah, Wyoming[131]

- How long does the organization have before it must make notification to impacted individuals?

  As with many other aspects of notice, the timing requirements for notification vary by jurisdiction and depend upon whether the organization is otherwise specially regulated (e.g., as a financial institution, as an insurance company, or as a covered entity under HIPAA). This section will focus on organizations that are *not* specially regulated. Organizations that are specially regulated should refer to the specific federal, state, and territorial statutes to determine the timing requirements for notification.

Interestingly, once the notification clock starts to run, the vast majority of data breach notification laws actually do *not* place a specific time limit by which notification must be made. Instead, they require—rather ambiguously—that notification must be provided to impacted individuals "*in the most*

[131] . ALA. CODE § 8-38-5(b); ARIZ. REV. STAT. § 18-552(B)(1); COLO. REV. STAT. § 6-1-716(2)(a); CONN. GEN. STAT. § 36a-701b(b)(1); DEL. CODE ANN. tit. 6, § 12B-102(a); IDAHO CODE § 28-51-105(1); KAN. STAT. ANN. § 50-7a02(a); MD. CODE ANN., COM. LAW § 14-3504(b)(1)—(2); MISS. CODE ANN. § 75-24-29(3); MO. ANN. STAT. § 407.1500(2)(1)(C), (5); NEB. REV. STAT. § 87-803(1); N.H. REV. STAT. ANN. § 359-C:20(I)(a); N.M. STAT. ANN. § 57-12C-6(B)(C); S.D. CODIFIED LAWS § 22-40-20; UTAH CODE ANN. § 13-44-202(1)(a)—(b); WYO. STAT. ANN. § 40-12-502(a).

expeditious time possible" and "*without unreasonable delay*."[132] In addition to D.C., U.S. states and territories providing only this vague timing expectation include: Alaska, Arkansas, California, Delaware, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, ~~Maine,~~ Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Oklahoma, Pennsylvania, Puerto Rico, South Carolina, Texas, Utah, Virginia, West Virginia, and Wyoming.[133] In these jurisdictions, while notice must be made without undue or unreasonable delay, the timing of such notice may account for the time it takes the organization to determine the scope of the breach and/or to restore the reasonable integrity of the system breached (as discussed above). And, though beyond the scope of this *Guide*, notification to impacted individuals under GDPR (if required) similarly must be made "without undue delay."[134]

Though these jurisdictions do not specify an exact number of days by which notice must be provided, the organization

---

[132] . *See, e.g.*, ALASKA STAT. § 45.48.010(b).

[133] . *Id.*; ARK. CODE ANN. § 4-110-105(a)(2); CAL. CIV. CODE § 1798.82(a); DEL. CODE ANN. tit. 6, § 12B-102(a); D.C. CODE § 28-3852(a); GA. CODE ANN. § 10-1-912(a); HAW. REV. STAT. § 487N-2(a); IDAHO CODE § 28-51-105(1); 815 ILL. COMP. STAT. 530/10(a); IOWA CODE § 715C.2(1); KAN. STAT. ANN. § 50-7a02(a); KY. REV. STAT. ANN. § 365.732(2); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS § 445.72(1); MINN. STAT. § 325E.61(1); MISS. CODE ANN. § 75-24-29(3); MO. ANN. STAT. § 407.1500(2)(1); MONT. CODE ANN. § 30-14-1704(1); NEB. REV. STAT. § 87-803(1); NEV. REV. STAT. ANN. § 603A.220(1); N.H. REV. STAT. ANN. § 359-C:20(I)(a); N.J. STAT. ANN. § 56:8-163(12)(a); N.Y. GEN. BUS. LAW § 899-aa(2); N.C. GEN. STAT. § 75-65(a); N.D. CENT. CODE § 51-30-02; OKLA. STAT. tit. 24, § 163(A); 73 PA. CONS. STAT. § 2303(a); P.R. LAWS ANN. tit. 10, § 4052; S.C. CODE ANN. § 39-1-90(A); TEX. BUS. & COM. CODE ANN. § 521.053(b); UTAH CODE ANN. § 13-44-202(2); VA. CODE ANN. § 18.2-186.6(B); W. VA. CODE § 46A-2A-102(a)—(b); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

[134] . GDPR, *supra* note 1, Art. 34(1).

does not have license to remain idle following the discovery or notification of a data incident. Practically speaking, this still means the organization must work as swiftly and efficiently as possible to investigate the incident, determine the scope, and restore the integrity of the breached network. As discussed in prior sections, an investigation into the facts of the data incident should begin *immediately* to determine whether the facts give rise to a "breach" as defined by applicable state law. Similarly, the moment an investigation reveals that the personal information of residents has been "breached," the organization should move as quickly as possible to provide the requisite notice to impacted individuals. Indeed, regulators may—and likely will—scrutinize in close detail when and how long it took the organization to determine the scope of the breach and/or restore network integrity and the length of time it took the organization to notify impacted individuals thereafter. Delayed notification could result in fines and litigation. Historically, regulators have not shied away from imposing such fines or initiating investigations when, among other things, the regulator determined that notification had been unreasonably or unjustifiably delayed. These cases show that in jurisdictions where timing is unspecified, there is no magic number (e.g., two weeks, one month, or two months could be too long); instead, the inquiry is fact-specific, and the organization will need to be able to show that it was moving as quickly as possible to investigate and notify.

~~Eighteen~~Twenty states actually specify a time period during which notice to impacted individuals must be made: Alabama (forty-five days), Arizona (forty-five days), Colorado (thirty days), Connecticut (~~ninety~~sixty days), Delaware (sixty days), Florida (thirty days), Indiana (forty-five days), Louisiana (sixty days), Maine (thirty days), Maryland (forty-five days), New Mexico (forty-five days), Ohio (forty-five days), Oregon (forty-five days), Rhode Island (forty-five days), South Dakota (sixty days), Texas (sixty days), Tennessee (forty-five days),

Vermont (forty-five days), Washington (thirty days), and Wisconsin (forty-five days). In Connecticut, for example, notice to impacted individuals must be made without unreasonable delay "*but not later than ~~ninety~~sixty days after* the discovery of such breach unless a shorter time is required under federal law." ~~As summarized above~~[135] Similarly, in Delaware, Louisiana, South Dakota, and ~~soon~~ Texas, notice to impacted individuals must be made in the most expedient time possible and without unreasonable delay, ~~"~~*but not later than sixty days* from the discovery of the breach.~~"~~[136] In Alabama, Arizona, Indiana, Maryland, New Mexico, Ohio, Oregon, Rhode Island, Tennessee, Vermont, and Wisconsin, notice to the impacted individual(s) must be made in the most expedient time possible and/or without unreasonable delay *but within or not later than forty-five days following* the organization's discovery, determination, or notification from a third-party that a breach has occurred.[137] In Florida, Colorado, Maine, and Washington, notice to impacted individuals must be made as expeditiously as practicable and without unreasonable delay "*but no [or not] later than 30 days after*" the determination or discovery of a breach.[138] In South Dakota, notice to impacted individuals must be made "*not later than sixty days from*" the discovery or notification from a third-party that a breach has occurred.[139] In each of these states, the time period stipulated for notification

---

135 . CONN. GEN. STAT. § 36a-701b(b)(1) (emphasis added).

136 . DEL. CODE ANN. tit. 6, § 12B-102(c); LA. STAT. ANN. § 51:3074(E); S.D. Codified Laws § 22-40-20, TEX. BUS. & COM. CODE ANN. § 521.053(b).

137 . ALA. CODE § 8-38-5(b); ARIZ. REV. STAT. § 18-552(B); IND. CODE § 24-4.9-3-3(a); MD. CODE ANN., COM. LAW § 14-3504(b)(3); OHIO REV. CODE ANN. § 1349.19(B)(2); OR. REV. STAT. § 646A.604(3); 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); TENN. CODE ANN. § 47-18-2107(b); VT. STAT. ANN. tit. 9, § 2435(b)(1); WIS. STAT. § 134.98(3).

138 . COLO. REV. STAT. § 6-1-716(2)(a); FLA. STAT. § 501.171(4)(a); ME. REV. STAT. ANN. tit. 10, § 1348(1); WASH. REV. CODE § 19.255.010(8).

139 . S.D. Codified Laws § 22-40-20.

is *subject to* the legitimate needs of law enforcement, thereby signaling that the needs of law enforcement may supersede and justifiably delay notice beyond the statutory time period.

Table VI.C.2(B):
Timing by Which Notification Must be Made to Impacted Individuals Once Notification Clock is Triggered

Notice must be made "in the most expeditious time possible" and "without undue delay."	Alaska, Arkansas, California, D.C., Georgia, Hawaii, Idaho, Illinois, ~~Indiana,~~ Iowa, Kansas, Kentucky, ~~Maine,~~ Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Oklahoma, Pennsylvania, Puerto Rico, South Carolina, Utah, Virginia, West Virginia, Wyoming[140]

[140] . ALASKA STAT. § 45.48.010(b); ARK. CODE ANN. § 4-110-105(a)(2); CAL. CIV. CODE § 1798.82(a); D.C. CODE § 28-3852(a); GA. CODE ANN. § 10-1-912(a); HAW. REV. STAT. § 487N-2(a); IDAHO CODE § 28-51-105(1); 815 ILL. COMP. STAT. 530/10(a); IOWA CODE § 715C.2(1); KAN. STAT. ANN. § 50-7a02(a); KY. REV. STAT. ANN. § 365.732(2); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS § 445.72(4); MINN. STAT. § 325E.61(1); MISS. CODE ANN. § 75-24-29(3); MO. ANN. STAT. § 407.1500(2)(1); MONT. CODE ANN. § 30-14-1704(1); NEB. REV. STAT. § 87-803(1); NEV. REV. STAT. ANN. § 603A.220(1); N.H. REV. STAT. ANN. § 359-C:20(I)(a); N.J. STAT. ANN. § 56:8-163(a); N.Y. GEN. BUS. LAW § 899-aa(2); N.C. GEN. STAT. § 75-65(a); N.D. CENT. CODE § 51-30-02; OKLA. STAT. tit. 24, § 163(A); 73 PA. CONS. STAT. § 2303(a); P.R. LAWS ANN. tit. 10, § 4052; S.C. CODE ANN. § 39-1-90(A);; UTAH CODE ANN. § 13-44-202(2); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(16); W. VA. CODE § 46A-2A-102(a)—(c); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

~~Notice must be made without unreasonable delay *but "no later than ninety days after* the discovery of the breach unless a shorter time is required under federal law."~~	~~Connecticut[117]~~
Notice must be made in the most expedient time possible and without unreasonable delay *but "not later than* [sixty] *days*" from the discovery or notification of the breach.	Connecticut, Delaware, Louisiana, South Dakota, Texas[141]

[141] . CONN. GEN. STAT. § 36a-701b(b)(1); DEL. CODE ANN. tit. 6, § 12B-102(c); LA. STAT. ANN. § 51:3074(E); S.D. CODIFIED LAWS § 22-40-20, TEX. BUS. & COM. CODE ANN. § 521.053(b).

Notice must be made in the most expedient time possible and without unreasonable delay *but "not later than* [forty-five] *days*" from the discovery of the breach.	Alabama, Arizona, Indiana, Maryland, New Mexico, Ohio, Oregon, Rhode Island, Tennessee, Vermont (if the collector has previously submitted to the Vermont Attorney General a sworn statement regarding the data collector's data security policies), Wisconsin[142]
Notice must be made as expeditiously as practicable and without unreasonable delay *but "no later than thirty days after"* the determination of a breach.	Colorado, Florida, Maine, Washington[143]

- If required, when should notice be made to regulators?

  The majority of jurisdictions with requirements regarding notification to relevant regulators generally require, either implicitly or explicitly, that notice be made contemporaneously with notice to the impacted residents. However, a few jurisdictions have enunciated timing-specific requirements for notice to regulators.

In Maryland and New Jersey, notice to the relevant state regulators, if required, must always be made *prior to* the

142 . ALA. CODE § 8-38-5(b); ARIZ. REV. STAT. § 18-552(B); IND. CODE § 24-4.9-3-3(a); MD. CODE ANN., COM. LAW § 14-3504(b)(3); N.M. STAT. ANN. § 57-12C-6(A)(C); OHIO REV. CODE ANN. § 1349.19(B)(2); OR. REV. STAT. § 646A.604(3)(a); R.I. GEN. LAWS § 11-49.3-4(a)(2); TENN. CODE ANN. § 47-18-2107(b); VT. STAT. ANN. tit. 9, § 2435(b)(1); WIS. STAT. § 134.98(3).

143 . COLO. REV. STAT. § 6-1-716(2)(a); FLA. STAT. § 501.171(4)(a); ME. REV. STAT. ANN. tit. 10, § 1348(1); WASH. REV. CODE § 19.255.010(8)

organization's notice to impacted individuals.[144] In Vermont, notification to the Attorney General is required within fourteen business days of the discovery of the breach or when the entity gives notification to impacted individuals, whichever is sooner.[145] If, however, the organization has previously filed a sworn submission with the Vermont Attorney General attesting to the organization's written information security and incident response policies and procedures, then it need only notify the Attorney General prior to notifying impacted individuals (which thereby obviates the fourteen-business-day notification rule, assuming notification to impacted individuals occurs more than fourteen business days from the date of discovering the breach).[146] In Alabama, Arizona, Colorado, Florida, Iowa, Louisiana, South Dakota, Vermont, and Washington, notice must be made within a specified time after either the determination of the breach or the notice to impacted individuals.[147]

Table VI.C.2(C):
Timing by Which Notification Must be Made
to State Regulatory Authorities (If Specified by Statute)

144 . MD. CODE ANN., COM. LAW § 14-3504(h); N.J. STAT. ANN. § 56:8-163(12)(c)(1).

145 . VT. STAT. ANN. tit. 9, § 2435(b)(3)(B)(i).

146 . VT. STAT. ANN. tit. 9, § 2435(b)(3)(B)(i)—(ii).

147 . ALA. CODE § 8-38-6(a); ARIZ. REV. STAT. § 18-552(B)(2)(b); FLA. STAT. § 501.171(3)(a); IOWA CODE § 715C.2(8); LA. ADMIN. CODE tit. 16, § 701(B); VT. STAT. ANN. tit. 9, § 2435(b)(3).

148 . MD. CODE ANN., COM. LAW § 14-3504(h)(1); N.J. STAT. ANN. § 56:8-163(12)(c)(1).

Notice *Prior to* Notice to Individuals	Maryland,[148] New Jersey, Vermont (unless requisite sworn statement previously submitted to Attorney General)[149]
Within five business days after giving notice of the breach of security to any consumer	Iowa
Within ten days of distribution of notice to residents	Louisiana[150]
Within fourteen business days of "discovery of the security breach or when the data collector provides notice to consumers," whichever is sooner (if no previously sworn statement filed with Vermont Attorney General)	Vermont[151]
No later than thirty days after	Colorado, Florida,

[148] . MD. CODE ANN., COM. LAW § 14-3504(h)(1); N.J. STAT. ANN. § 56:8-163(12)(c)(1).

[149] . VT. STAT. ANN. tit. 9, § 2435(b)(3)(B)(i)—(ii).

[150] . LA. ADMIN. CODE tit. 16, § 701(B).

[151] . VT. STAT. ANN. tit. 9, § 2435(b)(3)(B)(i)—(ii).

discovery of or determination that breach occurred.	Washington[152]
Within forty-five days after determination that a breach has occurred.	Arizona, New Mexico, Rhode Island[153]
Within forty-five days of "notice from a third-party agent that a breach has occurred or upon the entity's determination that a breach has occurred and is reasonably likely to cause substantial harm."	Alabama[154]
Within 60 days "from the discovery or notification of the breach of system security."	South Dakota, Texas[155]

As with the other aspects of breach notification requirements, the organization must consider the timing requirements in any jurisdictions outside of the U.S. where notifications may be required, as they differ from the U.S.

Again, though beyond the scope of the *Guide*, and in stark contrast to the timing requirements of U.S. state data breach notification laws, the GDPR mandates notification of a data breach to the applicable EU supervisory authority "without undue delay and, where feasible, *not later than 72 hours after*

[152] . COLO. REV. STAT. § 6-1-716(2)(f); FLA. STAT. § 501.171(3)(a); WASH. REV. CODE § 19.255.010(7).

[153] . ARIZ. REV. STAT. § 18-552(B)(2)(b); N.M. STAT. ANN. § 57-12C-10; 11 R.I. GEN. LAWS § 11-49.3-4(a)(2).

[154] . ALA. CODE § 8-38-6(a).

[155] . S.D. CODIFIED LAWS § 22-40-20; TEX. BUS. & COM. CODE ANN. § 521.053(b) & (i).

having become aware" of the breach.[156] Initially, this was one of the tightest notice deadlines; however, it has since been superseded by countries like Brazil and South Korea with their 48-hour deadlines as well as India recent updates to require notice with 6 hours to CERT-In. As discussed above, this mandate, again, appears to prioritize and place greater importance on notification to the supervisory authority than the impacted individuals—requiring notification to be made to the authorities not later than seventy-two hours after becoming aware of a breach, in contrast to the requirement that notification to impacted individuals need only be made (if at all) "without undue delay." Not surprisingly, the question of when an entity "becomes aware" of a "personal data breach" (which is defined broadly to encompass any manner of data incidents) ~~and, thus~~. In fact, an organization may become aware of a security breach before it becomes aware of a personal data breach as defined under GDPR. Thus, when the seventy-two-hour clock starts running has caused much anxiety and debate among practitioners and organizations alike.

~~The GDPR's~~

In Canada, on the other hand, there are no specific timelines within which mandatory notifications under Canada's federal privacy statute or the provincial privacy statutes in Alberta or Quebec must be provided. Rather, any mandatory notifications to the Alberta privacy commissioner must be given "without unreasonable delay,"[157] and any required notifications to affected individuals under the Quebec privacy statute and under PIPEDA, and to the Quebec and federal privacy commissioners, must be provided "as soon as feasible after the ~~organization determines the breach has occurred.~~"[158]

---

156 . GDPR, *supra* note 1, Art. 33(1).

157 Personal Information Protection Act, SA 2003, c P-6.5, s 34.1(1), <https://canlii.ca/t/81qp#sec34.1>, retrieved on 2023-04-19.

International notification requirements are extremely important for U.S. practitioners to keep in mind when taking into account more nuanced incident response considerations for organizations subject to both ~~GDPR~~international and U.S. data breach laws. For example, in the initial run-up to the effective date of GDPR, some consultants reportedly advised that an incident response plan should invoke automatic notification under any circumstance that even suggests a data compromise, in order to avoid any risk of enforcement in the EU under Article 33. An incident response plan incorporating that default trigger could, however, create other unintended consequences for multinational public companies also doing business in the U.S. The EDPB has expressed its concerns on "over notification" and DPAs have also outlined that notification of breaches that are not personal data breaches may indicate that an organization does not have adequate data and security measures to assess a potential breach.[159]

Specifically, a more nuanced incident response plan may want to consider more carefully the merits of an automatic notification default at the first hint of data compromise, since that notification might in turn require similar notifications in the U.S. (with potentially only seventy-two hours to contemplate the consequences). Coordinated notifications allow the organization to track its correspondence with the regulators and maintain the narrative at a similar pace. Within the EU, under the GDPR, organizations that carry out cross-border processing in more than one Member State may be permitted to notify a single data protection authority, as opposed to multiple, in the event of a cross-border breach.

158 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, ss 10.1(2) and(6), <https://canlii.ca/t/7vwj#sec10.1>, retrieved on 2023-04-19; *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1, s 3.5, <https://canlii.ca/t/xpm#sec3.5>, retrieved on 2023-04-19.

159 See Multistakeholder Expert Group to the Commission 2020 Evaluation of the General Data Protection Regulation, page 36.

Recent EDPB guidance has stated however that this mechanism does not apply to non-EU organizations, even where such organizations have an EU representative.[160]

This concern would be especially important when assessing the other potential disclosure consequences that must be considered by publicly traded companies.

- If required, when should notice be made to credit reporting agencies?

  With the exception of Arizona, Minnesota, and New Mexico, there is no specific period of time within which notice to the credit reporting agencies must be made. Generally, the jurisdiction's statutes provide that notice, if required, should be made to the credit reporting agencies contemporaneously with individual consumer notices and "without unreasonable delay." In Arizona and New Mexico, consistent with the timing requirements for notification to individuals and the state attorneys general, notification to credit reporting agencies must be made "within forty-five days after" the determination that a breach has occurred.[161] Minnesota, on the other hand, requires notice to be made to the credit reporting agencies within forty-eight hours of when a "person discovers circumstances requiring notification" for breaches involving more than 500 residents.[162] Arguably, Minnesota's unusual phrasing could be read to require notifications to credit reporting agencies within forty-eight hours after the breach

160 See European Data Protection Board Guidelines 9/2022 on personal data breach notification under GDPR Version 2.0 28 March 2023.

161 . ARIZ. REV. STAT. § 18-552(B)(2)(a); N.M. STAT. ANN. § 57-12C-10.

162 . MINN. STAT. § 325E.61(2).

is first discovered, well in advance of any required notice to impacted residents.[163]

If similar reporting requirements apply under the laws of a jurisdiction outside the U.S., the organization will need to consider those timelines. For example, any required notices under Canada's federal privacy statute to organizations that may be able to reduce the risk of harm to individuals must be made "as soon as feasible after the organization determines that the breach has occurred."[164]

- Delay of notice due to law enforcement

  Across all U.S. jurisdictions, regardless of whether the data breach notification laws contain vague or very specific timing requirements or permit notification to occur after a reasonable investigation to determine the scope of the breach or restore the integrity of impacted systems, there is generally only one justifiable reason for delaying notification: if law enforcement has determined that notification will impede or interfere with an ongoing investigation. Indeed, delay arguably could be mandatory in Alabama, Connecticut, Delaware, Florida, Hawaii, Mississippi, New Jersey, North Carolina, Vermont, and Wisconsin, as noted in the table below.[165] In other jurisdictions, however, delaying notification after law enforcement has

163 . *Id*.

164 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 10.2, <https://canlii.ca/t/7vwj#sec10.2>, retrieved on 2023-04-19.

165 . ALA. CODE § 8-38-5(c); CONN. GEN. STAT. § 36a-701b(d); DEL. CODE ANN. tit. 6, § 12B-102(c)(2); FLA. STAT. § 501.171(4)(b); HAW. REV. STAT. § 487N-2(c); MISS. CODE ANN. § 75-24-29(5); N.J. STAT. ANN. 56:8-163(12)(c)(2); N.C. GEN. STAT. § 75-65(c); VT. STAT. ANN. tit. 9, § 2435(b)(4); WIS. STAT. §134.98(5).

made a determination that notification will impede or interfere with an ongoing investigation is merely optional, including in Alaska, Arizona, Arkansas, California, Colorado, D.C., Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Mexico, New York, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming.[166] In fact, there may be some very good practical, nonlegal reasons *not* to delay notification and, therefore, the organization will want to strategically consider whether to delay notification when it is optional.

[166] . ALASKA STAT. § 45.48.020; ARIZ. REV. STAT. § 18-552(D); ARK. CODE ANN. § 4-110-105(c); CAL. CIV. CODE § 1798.82(c); COLO. REV. STAT. § 6-1-716(2)(c); D.C. CODE § 28-3852(d); GA. CODE ANN. § 10-1-912(c); IDAHO CODE § 28-51-105(3); 815 ILL. COMP. STAT. 530/10(b-5); IND. CODE ANN. § 24-4.9-3-3(a)(3); IOWA CODE § 715C.2(3)); KAN. STAT. ANN. § 50-7a02(c); KY. REV. STAT. ANN. § 365.732(4); LA. STAT. ANN. § 51:3074(F); ME. REV. STAT. ANN. tit. 10, § 1348(3); MD. CODE ANN., COM. LAW § 14-3504(d)(1); MASS. GEN. LAWS ch. 93H, § 4; MICH. COMP. LAWS ANN. § 445.72(4); MINN. STAT. § 325E.61(1)(c); MO. ANN. STAT. § 407.1500(2)(3); MONT. CODE ANN. § 30-14-1704(3); NEB. REV. STAT. § 87-803(4); NEV. REV. STAT. ANN. § 603A.220(3); N.H. REV. STAT. ANN. § 359-C:20(II); N.M. Stat. Ann. § 57-12C-9(A); N.Y. GEN. BUS. LAW § 899-aa(4); N.D. CENT. CODE § 51-30-04; OHIO REV. CODE ANN. § 1349.19(D); OKLA. STAT. tit. 24, § 163(D); OR. REV. STAT. § 646A.604(3)(c); 73 PA. CONS. STAT. § 2304; 11 R.I. GEN. LAWS § 11-49.3-4(b); S.C. CODE ANN. § 39-1-90(C); S.D. Codified Laws § 22-40-21; TENN. CODE ANN. § 47-18-2107(d); TEX. BUS. & COM. CODE ANN. § 521.053(d); UTAH CODE ANN. § 13-44-202(4); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(3); W. VA. CODE § 46A-2A-102(e); WIS. STAT. §134.98(5); WYO. STAT. ANN. § 40-12-502(b).

Table VI.C.2(D): U.S. Jurisdictions That Allow Delay of Notice Due to Law Enforcement

Notice must be delayed if law enforcement determines that notice may impede or interfere with an ongoing investigation.	Alabama, Connecticut, Delaware, Florida, Hawaii, Mississippi, New Jersey, North Carolina, Vermont, Wisconsin[167]

[167] . ALA. CODE § 8-38-5(c); CONN. GEN. STAT. § 36a-701b(d); DEL. CODE ANN. tit. 6, § 12B-102(c)(2)); FLA. STAT. § 501.171(4)(b); HAW. REV. STAT. § 487N-2(c); MISS. CODE ANN. § 75-24-29(5); N.J. STAT. ANN. 56:8-163(12)(c)(2); N.C. GEN. STAT. § 75-65(c); VT. STAT. ANN. tit. 9, § 2435(b)(4); WIS. STAT. §134.98(5).

Notice may be delayed if law enforcement determines that notice may impede or interfere with an ongoing investigation.	Alaska, Arizona, Arkansas, California, Colorado, D.C., Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Mexico, New York, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wyoming[168]

[168] . ALASKA STAT. § 45.48.020; ARIZ. REV. STAT. § 18-552(D); ARK. CODE ANN. § 4-110-105(c); CAL. CIV. CODE § 1798.82(c); COLO. REV. STAT. § 6-1-716(2)(c); D.C. CODE § 28-3852(d); GA. CODE ANN. § 10-1-912(c); IDAHO CODE § 28-51-105(3); 815 ILL. COMP. STAT. 530/10(b-5); IND. CODE § 24-4.9-3-3(a)(3); IOWA CODE § 715C.2(3); KAN. STAT. ANN. § 50-7a02(c); KY. REV. STAT. ANN. § 365.732(4); LA. STAT. ANN. § 51:3074(F); ME. REV. STAT. ANN. tit. 10, § 1348(3); MD. CODE ANN., COM. LAW § 14-3504(d)(1); MASS. GEN. LAWS ch. 93H, § 4; MICH. COMP. LAWS § 445.72(4); MINN. STAT. § 325E.61(1)(c); MO. ANN. STAT. § 407.1500(2)(3); MONT. CODE ANN. § 30-14-1704(3); NEB. REV. STAT. § 87-803(4); NEV. REV. STAT. ANN. § 603A.220(3); N.H. REV. STAT. ANN. § 359-C:20(II); N.M. STAT. ANN. § 57-12C-9(A); N.Y. GEN. BUS. LAW § 899-aa(4); N.D. CENT. CODE § 51-30-04; OHIO REV. CODE ANN. § 1349.19(D); OKLA. STAT. tit. 24, § 163(D); OR. REV. STAT. § 646A.604(3)(b); 73 PA. CONS. STAT. § 2304; 11 R.I. GEN. LAWS § 11-49.3-4(b); S.C. CODE ANN. § 39-1-90(C); S.D. CODIFIED LAWS § 22-40-21; TENN. CODE ANN. § 47-18-2107(d); TEX. BUS. & COM. CODE ANN. § 521.053(d); UTAH CODE ANN. § 13-44-202(4); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(3); W. VA. CODE § 46A-2A-102(e); WYO. STAT. ANN. § 40-12-502(b).

Again, if the incident is one that may require notices under the laws of a jurisdiction outside the U.S., the organization will need to consider whether the laws of that jurisdiction allow for delays to otherwise prescribed notice timelines. For example, in Canada, Quebec's privacy statute expressly provides that affected individuals needs not be notified "so long as doing so could hamper an investigation" by law enforcement in relation to a crime.[169]

3. Method and Content of Notice

Much like the other logistics-related notice requirements, the method and content requirements for notification varies by jurisdiction and, therefore, the organization must carefully review the applicable statutory language to ensure compliance with the law of the jurisdiction, especially if the breach implicates individuals from more than one jurisdiction. Again, as with prior sections, this section addresses only those content requirements for organizations that are not specially regulated. Organizations that are specially regulated (e.g., via HIPAA or the GLBA) should refer to the specific statutes of states, territories, and D.C., as well as any applicable federal statutes, to determine the form and content requirements for notification. Certain international jurisdictions will also have additional requirements, including language, content and method of delivery.

- Method of Notice to Impacted Individuals

  Notice can be made to impacted individuals in one of several ways, depending on the facts and the applicable laws in each jurisdiction: (1) via written letter, (2) via email, (3) by telephone or even text, or (4) via "substitute" notice. Not just one method need be employed; the facts and

169 Act respecting the protection of personal information in the private sector, CQLR c P-39.1, s 3.5, <https://canlii.ca/t/xpm#sec3.5>, retrieved on 2023-04-20.

circumstances of a particular data breach may necessitate the use of one or more of the above methods. The GDPR, for example, generally requires an organization to communicate in the manner by which it ordinarily communicates with data subjects.

- Letter Notice

  Every state jurisdiction that has a data breach notification law permits notice to be made to impacted individuals by direct, written letter via U.S. mail. To utilize this direct method of notice, the organization will need to have contact information for the impacted individuals. Thus, whether the organization will be able to send written notice will depend upon whether the organization was able to identify with certainty all of the individuals impacted by the breach and has contact information for those identifiable individuals. As discussed in greater detail below, to the extent the impacted individual resides in a jurisdiction that has enunciated specific content for the notice, the written notice letter will need to include that statutory content.

- Email Notice

  Email notice is generally permissible in almost all state jurisdictions with data breach notification laws; however, depending on the jurisdiction, certain criteria may need to be satisfied first before email can be utilized as a method of notice. These criteria could include: (1) if the organization has a preexisting business relationship with the impacted individual(s);[170]

[170] . MICH. COMP. LAWS § 445.72(5)(b); 73 PA. CONS. STAT. § 2302; VA. CODE ANN. § 18.2-186.6(B).

(2) if the impacted individual(s) has expressly consented to receive electronic notices under the Electronic Signatures in Global and National Commerce Act, codified at 15 U.S.C. §§ 7001–7031 ("ESIGN"),[171] or has otherwise expressed consent to receive such notices;[172] (3) if

[171] . The salient provisions of this requirement include the following:

- The customer has consented to receive communication by email and not withdrawn the consent.
- The customer was provided a clear and conspicuous statement:
  - informing her of her right to have records made available in paper form and the right to withdraw consent;
  - informing her of what transactions the consent applies to;
  - describing the procedures required to withdraw consent;
  - describing how the customer may get a paper copy; and
  - describing the hardware and software requirements to access electronic records.

[172] . ALASKA STAT. § 45.48.030(2); ARK. CODE ANN. § 4-110-105(e)(2); CAL. CIV. CODE § 1798.82(j)(2); COLO. REV. STAT. § 6-1-716(1)(f)(III); CONN. GEN. STAT. § 36a-701b(e)(3); DEL. CODE ANN. tit. 6, § 12B-101(5)(c); D.C. CODE § 28-3851(2)(B); GA. CODE ANN. § 10-1-911(4)(C); HAW. REV. STAT. § 487N-2(e)(2); IDAHO CODE § 28-51-104(4)(c); 815 ILL. COMP. STAT. 530/10(c)(2); IOWA CODE § 715C.2(4)(b); KAN. STAT. ANN. § 50-7a01(c)(2); KY. REV. STAT. ANN. § 365.732(5)(b); LA. STAT. ANN. § 51:3074(G)(2); ME. REV. STAT. ANN. tit. 10, § 1347(4)(B); MD. CODE ANN., COM. LAW § 14-3504(e)(2); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.72(5)(b); MINN. STAT. § 325E.61(1)(g)(2); MISS. CODE ANN. § 75-24-29(6)(c); MO. ANN. STAT. § 407.1500(2)(6)(b); MONT. CODE ANN. § 30-14-1704(5)(a)(ii); NEB. REV. STAT. § 87-802(4)(c); NEV. REV. STAT. ANN. § 603A.220(4)(b); N.J. STAT. ANN. § 56:8-163(12)(d); N.M. STAT. ANN. § 57-12C-6(D)(2); N.Y. GEN. BUS. LAW § 899-aa(5)(b); N.C. GEN. STAT. § 75-65(e)(2); N.D. CENT. CODE § 51-30-05(2); OR. REV. STAT. § 646A.604(4)(b); P.R. LAWS ANN. tit. 10, § 4053(1); 11 R.I. GEN. LAWS § 11-49.3-3(c)(ii); S.C. CODE ANN. § 39-1-90(E)(2); TENN. CODE

the organization primarily conducts its business through internet account transactions or on the internet generally;[173] and/or (4) if the organization previously used email to communicate with the impacted individual(s) or if email was the primary method of communicating with the impacted individual(s).[174] To the extent the organization is contemplating notice via email, it should scrutinize the applicable law of the jurisdiction to ensure the facts satisfy the preconditions required to effect notice by email. By way of example, New York allows it if the customer has consented, but not if consent was required as a condition to doing business electronically.[175]

- Telephonic Notice

ANN. § 47-18-2107(e)(2); TEX. BUS. & COM. CODE ANN. § 521.053(e)(2); UTAH CODE ANN. § 13-44-202(5)(a)(ii); VT. STAT. ANN. tit. 9, § 2435(b)(6)(A)(ii); WASH. REV. CODE § 19.255.010(2)(4)(b); W. VA. CODE § 46A-2A-101(7)(C).

173 . MD. CODE ANN., COM. LAW § 14-3504(e)(2); MICH. COMP. LAWS § 445.72(5)(b).

174 . ALA. CODE § 8-38-5(d); ALASKA STAT. § 45.48.030(2); ARIZ. REV. STAT. § 18-552(F)(2); COLO. REV. STAT. § 6-1-716(1)(f)(III); FLA. STAT. § 501.171(4)(d)(2); IND. CODE § 24-4.9-3-4(a)(4); IOWA CODE § 715C.2(4)(b); MINN. STAT. § 325E.61(1)(g)(2); MISS. CODE ANN. § 75-24-29(6)(c); N.H. REV. STAT. ANN. § 359-C:20(III)(b); OHIO REV. CODE ANN. § 1349.19(E)(2); OKLA. STAT. tit. 24, § 162(7)(c); OR. REV. STAT. § 646A.604(4)(b); S.C. CODE ANN. § 39-1-90(E)(2); S.D. CODIFIED LAWS § 22-40-22(2); UTAH CODE ANN. § 13-44-202(5)(a)(ii); VT. STAT. ANN. tit. 9, § 2435(b)(6)(A)(ii); VA. CODE ANN. § 18.2-186.6(A); WIS. STAT. § 134.98(3)(b); WYO. STAT. ANN. § 40-12-502(d).

175 . N.Y. GEN. BUS. LAW § 899-aa(5)(b). The following states and DC require compliance with ESIGN to qualify for electronic-only notice: Arkansas; California; Connecticut; Delaware; Georgia; Hawaii; Idaho; Illinois; Kansas; Kentucky; Louisiana; Maine; Massachusetts; Missouri; Montana; Nevada; New Jersey; North Carolina; North Dakota; Rhode Island; Tennessee; Texas; Washington; West Virginia.

Telephonic notice, including text notice in some foreign jurisdictions, is ~~also~~ permissible, though not in every jurisdiction. To the extent the organization has neither a mailing address nor an email address for an impacted individual, but it does have a telephone number, the organization should carefully review the relevant data breach notification law to ensure telephonic notice is permissible; otherwise, the organization may have to make substitute notice (as discussed below). The following states permit telephonic notice generally: Arizona, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Indiana, Maryland, Michigan, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Carolina, Utah, Vermont, Virginia, West Virginia, and Wisconsin.[176] Depending on the state, however, certain criteria may have to be satisfied to permit telephonic notice, such as keeping a log of the call,[177]

[176] . ARIZ. REV. STAT. § 18-552(F)(3); COLO. REV. STAT. § 6-1-716(1)(f)(II); CONN. GEN. STAT. § 36a-701b(e)(2); DEL. CODE ANN. tit. 6, § 12B-101(5)(b); GA. CODE ANN. § 10-1-911(4)(B); HAW. REV. STAT. § 487N-2(e)(3); IDAHO CODE § 28-51-104(4)(b); IND. CODE § 24-4.9-3-4(a)(2); MD. CODE ANN., COM. LAW § 14-3504(e)(3); MICH. COMP. LAWS ANN. § 445.72(5)(c); MISS. CODE ANN. § 75-24-29(6)(b); MO. ANN. STAT. § 407.1500(2)(6)(c); MONT. CODE ANN. § 30-14-1704(5)(a)(iii); NEB. REV. STAT. § 87-802(4)(b); N.H. REV. STAT. ANN. § 359-C:20(III)(c); N.Y. GEN. BUS. LAW § 899-aa(5)(c); N.C. GEN. STAT. § 75-65(e)(3); OHIO REV. CODE ANN. § 1349.19(E)(3); OKLA. STAT. tit. 24, § 162(7)(b); OR. REV. STAT. § 646A.604(4)(c); 73 PA. CONS. STAT. § 2302; S.C. CODE ANN. § 39-1-90(E)(3); UTAH CODE ANN. § 13-44-202(5)(a)(iii); VT. STAT. ANN. tit. 9, § 2435(b)(6)(A)(iii); VA. CODE ANN. § 18.2-186.6(A); W. VA. CODE § 46A-2A-101(7)(B); WIS. STAT. §134.98(3)(c).

[177] . N.H. REV. STAT. ANN. § 359-C:20(III)(c); N.Y. GEN. BUS. LAW § 899-aa(5)(c).

speaking directly with the impacted individual (i.e., not simply leaving a voicemail),[178] or notifying by telephone only if the organization has previously communicated with the impacted individual by telephone.[179]

- Substitute Notice

  Substitute notice is a legal construct devised by regulators to assist organizations in notifying impacted individuals of a data breach when the organization does not have sufficient contact information for the impacted individuals or the population of impacted individuals exceeds a certain threshold, such that direct notice would be inefficient and/or cost prohibitive. Substitute notice generally consists of two to three forms of communication: (1) a "conspicuous" publication of the notice to the organization's website; (2) publication of the notice in "major statewide media;" and/or (3) general email notice where email addresses for impacted individuals are available.[180] The requirements for substitute

178 . ARIZ. REV. STAT. § 18-552(F)(3); HAW. REV. STAT. § 487N-2(e)(3); MICH. COMP. LAWS § 445.72(5)(c); MO. ANN. STAT. § 407.1500(2)(6)(c); N.C. GEN. STAT. § 75-65(e)(3); OR. REV. STAT. § 646A.604(4)(c); VT. STAT. ANN. tit. 9, § 2435(b)(6)(A)(iii).

179 . WIS. STAT. § 134.98(3)(b).

180 . ALA. CODE § 8-38-5(e)(2); ALASKA STAT. § 45.48.030(3); ARIZ. REV. STAT. § 18-552(F)(4); ARK. CODE ANN. § 4-110-105(e)(3)(B); CAL. CIV. CODE § 1798.82(j)(3); COLO. REV. STAT. § 6-1-716(1)(f)(IV); CONN. GEN. STAT. § 36a-701b(e)(4); DEL. CODE ANN. tit. 6, § 12B-101(3)(d); D.C. CODE § 28-3851(2)(C)(ii); FLA. STAT. § 501.171(4)(f); GA. CODE ANN. § 10-1-911(4)(D); HAW. REV. STAT. § 487N-2(e)(4); IDAHO CODE § 28-51-104(4)(d); 815 ILL. COMP. STAT. 530/10(c)(3); IND. CODE § 24-4.9-3-4(b); IOWA CODE § 715C.2(4)(c); KAN. STAT. ANN. § 50-7a01(c)(3); KY. REV. STAT. ANN. § 365.732(5)(c); LA. STAT. ANN. § 51:3074(G)(3); ME. REV. STAT. ANN. tit. 10, § 1347(4)(C); MD. CODE ANN., COM. LAW § 14-3504(f); MASS. GEN. LAWS ch.

notice (e.g., how long the website notice must be maintained, or the media that are acceptable for publication) will vary by jurisdiction; and, therefore, to the extent the organization is contemplating substitute notice, it should consult each applicable law for guidance. Although substitute notice is generally permissible in all jurisdictions with data breach notification laws, certain prerequisites must be met before utilizing the substitute notice mechanism. These criteria, which vary by jurisdiction, could include: (1) the impacted class of individuals exceeds a certain threshold (ranging from in excess of 1,000 to 500,000 persons); (2) the cost of providing direct notice to the class of impacted individuals exceeds a certain minimum amount (ranging from in excess of $5,000 to $250,000); and/or (3) the organization does not have sufficient contact information for impacted individuals to notify

93H, § 1(a); MICH. COMP. LAWS § 445.72(5)(d); MINN. STAT. § 325E.61(1)(g)(3); MISS. CODE ANN. § 75-24-29(6)(d); MO. ANN. STAT. § 407.1500(2)(6)(d); MONT. CODE ANN. § 30-14-1704(5)(a)(iv); NEB. REV. STAT. § 87-802(4)(d); NEV. REV. STAT. ANN. § 603A.220(4)(c); N.H. REV. STAT. ANN. § 359-C:20(III)(d); N.J. STAT. ANN. § 56:8-163(12)(d)(3); N.M. STAT. ANN. § 57-12C-6(D)(3); N.Y. GEN. BUS. LAW § 899-aa(5)(d); N.C. GEN. STAT. § 75-65(e)(4); N.D. CENT. CODE § 51-30-05(3); OHIO REV. CODE ANN. § 1349.19(E)(4); OKLA. STAT. tit. 24, § 162(7)(d); OR. REV. STAT. § 646A.604(4)(d); 73 PA. CONS. STAT. § 2302; P.R. LAWS ANN. tit. 10, § 4053(2); 11 R.I. GEN. LAWS § 11-49.3-3(c)(iii); S.C. CODE ANN. § 39-1-90(E)(4); S.D. CODIFIED LAWS § 22-40-22(3); TENN. CODE ANN. § 47-18-2107(e)(3); TEX. BUS. & COM. CODE ANN. § 521.053(f); UTAH CODE ANN. § 13-44-202(5)(a)(iv); VT. STAT. ANN. tit. 9, § 2435(b)(6)(B); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(2)(4)(c); W. VA. CODE § 46A-2A-101(7)(D); WYO. STAT. ANN. § 40-12-502(d)(iii).

them directly.[181]This approach is also similar to the approach taken under GDPR.

Once the appropriate method of notification has been determined, the organization must next determine the content required for the notice.

- Contents of Notice to Impacted Individuals

  Though the content of the notice is arguably one of the most important aspects of the notice process, well over half of the states, territories, and D.C. do *not* have any specific content requirements written into their statutes, including: Alaska, Arkansas, Connecticut,

[181] . ALA. CODE § 8-38-5(e)(1); ALASKA STAT. § 45.48.030(3); ARIZ. REV. STAT. § 18-552(F)(4); ARK. CODE ANN. § 4-110-105(e)(3)(A); CAL. CIV. CODE § 1798.82(j)(3); COLO. REV. STAT. § 6-1-716(1)(f)(IV); CONN. GEN. STAT. § 36a-701b(e)(4); DEL. CODE ANN. tit. 6, § 12B-101(5)(d); D.C. CODE § 28-3851(2)(C)(i); FLA. STAT. § 501.171(4)(f); GA. CODE ANN. § 10-1-911(4)(D); HAW. REV. STAT. § 487N-2(e)(4); IDAHO CODE § 28-51-104(4)(d); 815 ILL. COMP. STAT. 530/10(c)(3); IND. CODE § 24-4.9-3-4(b); IOWA CODE § 715C.2(4)(c); KAN. STAT. ANN. § 50-7a01(c)(3); KY. REV. STAT. ANN. § 365.732(5)(c); LA. STAT. ANN. § 51:3074(G)(3); ME. REV. STAT. ANN. tit. 10, § 1347(4)(C); MD. CODE ANN., COM. LAW § 14-3504(f; MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.72(5)(d); MINN. STAT. § 325E.61(1)(g)(3); MISS. CODE ANN. § 75-24-29(6)(d); MO. ANN. STAT. § 407.1500(2)(7); MONT. CODE ANN. § 30-14-1704(5)(a)(iv); NEB. REV. STAT. § 87-802(4)(d); NEV. REV. STAT. ANN. § 603A.220(4)(c); N.H. REV. STAT. ANN. § 359-C:20(III)(d); N.J. STAT. ANN. § 56:8-163(12)(d)(3); N.M. STAT. ANN. § 57-12C-6(D)(3); N.Y. GEN. BUS. LAW § 899-aa(5)(d); N.C. GEN. STAT. § 75-65(e)(4); N.D. CENT. CODE § 51-30-05(3); OHIO REV. CODE ANN. § 1349.19(E)(4); OKLA. STAT. tit. 24, § 162(7)(d); OR. REV. STAT. § 646A.604(4)(d); 73 PA. CONS. STAT. § 2302; P.R. LAWS ANN. tit. 10, § 4053(2); 11 R.I. GEN. LAWS § 11-49.3-3(c)(iii); S.C. CODE ANN. § 39-1-90(E)(4); S.D. CODIFIED LAWS § 22-40-22(3); TENN. CODE ANN. § 47-18-2107(e)(3); TEX. BUS. & COM. CODE ANN. § 521.053(f); UTAH CODE ANN. § 13-44-202(5)(a)(iv); VT. STAT. ANN. tit. 9, § 2435(b)(6)(B); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(2)(4)(c); W. VA. CODE § 46A-2A-101(7)(D); WYO. STAT. ANN. § 40-12-502(d)(iii).

> Delaware, D.C., Georgia, Idaho, Indiana, Kansas, Kentucky, Louisiana, Maine, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Jersey, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, and Utah. While not required, however, it is advisable to consider including the general content components identified below to avoid claims from consumers and/or regulators alleging the insufficiency of notice.

In contrast with the above states and D.C., the following jurisdictions have breach notice content requirements to varying degrees: Alabama, Arizona, California, Colorado, Florida, Hawaii, Illinois, Iowa, Maryland, Massachusetts, Michigan, Missouri, New Hampshire, New Mexico, New York, North Carolina, Oregon, Puerto Rico, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.[182]

Importantly, although these jurisdictions set forth specific content requirements, many exempt organizations from compliance with the specific notification obligations if the organization already has its own breach notice plan in place and notifies impacted individuals according to that plan. For example, in California, if the organization maintains its own notification procedures as part of a data breach response or

[182] . ALA. CODE § 8-38-5(d); ARIZ. REV. STAT. § 18-552(E); CAL. CIV. CODE § 1798.82(d); COLO. REV. STAT. § 6-1-716(2)(a)(a.2); FLA. STAT. § 501.171(4)(e); HAW. REV. STAT. § 487N-2(d); 815 ILL. COMP. STAT. 530/10(a); IOWA CODE § 715C.2(5); MD. CODE ANN., COM. LAW § 14-3504(g); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS ANN. § 445.72(6); MO. ANN. STAT. § 407.1500(2)(4); N.H. REV. STAT. ANN. § 359-C:20(IV); N.M. STAT. ANN. § 57-12C-7; N.Y. GEN. BUS. LAW § 899-aa(7); N.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5); P.R. LAWS ANN. tit. 10, § 4053; VT. STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(6) [effective Mar. 1, 2020]; W. VA. CODE § 46A-2A-102(d); WIS. STAT. § 134.98(2)(a); WYO. STAT. ANN. § 40-12-502(e).

information security policy, and the organization notifies impacted individuals in accordance with those policies and procedures, and the timing of notice pursuant to that policy is otherwise consistent with California's timing requirements, then the organization is deemed to be in compliance with California's statutory notification requirements, even if the organization's policies and procedures are different from California's statutory notice requirements.[183]

Organizations may also be exempt from compliance with the statutory notice obligations if the breach is otherwise regulated by or subject to HIPAA, GLBA's Security Standards, or another federal statute. In these instances, if the organization makes notice to impacted individuals pursuant to those federal notice requirements, then the organization is deemed to have automatically complied with the notice statute of the relevant U.S. jurisdiction, even if the federal notice requirements differ from that jurisdiction's requirements. These federal statutes, however, may have specific content requirements to which the organization must adhere. Thus, the organization must scrutinize the statutes in the relevant states, territories, and D.C., as well as federal statutes.

Further, if a data breach impacts residents in more than one jurisdiction, and each of those jurisdictions has content requirements, the organization will need to comply with the content requirements for each of the relevant jurisdictions. Apart from Massachusetts, compliance with each of those notice requirements, however, does not necessarily mean the organization must draft and disseminate several different breach notices. Instead, with careful crafting and scrutiny of the requirements in each relevant statute, in most instances, a single notice can be drafted that includes and complies with statutory content requirements in all of the relevant jurisdictions.

183 . CAL. CIV. CODE § 1798.82(l).

Finally, California, Hawaii, Michigan, North Carolina, Puerto Rico, Vermont, and Washington require that the notice be clear and conspicuous and crafted using plain language.[184] Though not a requirement across all jurisdictions, it is advisable that all notices be drafted using plain and concise language.

Table VI.C.3(A):
General Content Requirements for Notice to Individuals

Depending on the applicable statute, the following categories of information may be required in a notice to impacted individuals:	
Content Required	**U.S. Jurisdiction**
No specific content requirements	Alaska, Arkansas, Connecticut, Delaware, D.C., Georgia, Idaho, Indiana, Kansas, Kentucky, Louisiana, Maine, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Jersey, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah
Content Required	**U.S. Jurisdiction**

[184] . CAL. CIV. CODE § 1798.82(d); HAW. REV. STAT. § 487N-2(d); MICH. COMP. LAWS § 445.72(6); N.C. GEN. STAT. § 75-65(d); P.R. LAWS ANN. tit. 10, § 4053; VT. STAT. ANN. tit. 9, § 2435(b)(5); WASH. REV. CODE § 19.255.010(6).

A general description of the incident	California, Hawaii, Iowa, Michigan, Missouri, New Hampshire, New Mexico, North Carolina, Oregon, Puerto Rico, Vermont, Virginia, Wyoming[185]
Content Required	**U.S. Jurisdiction**
Date of the breach (or estimated date or date range within which the breach occurred)	Alabama, Arizona, California, Colorado, Florida, Iowa, New Hampshire, New Mexico, Oregon, Vermont, Washington, Wyoming[186]

[185] . CAL. CIV. CODE § 1798.82(d); HAW. REV. STAT. § 487N-2(d)(1); IOWA CODE § 715C.2(5); MICH. COMP. LAWS § 445.72(6); MO. ANN. STAT. § 407.1500(2)(4); N.H. REV. STAT. ANN. § 359-C:20(IV); N.M. STAT. ANN. § 57-12C-7; N.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5)(a); P.R. LAWS ANN. tit. 10, § 4053; VT. STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A); WYO. STAT. ANN. § 40-12-502(e).

[186] . ALA. CODE § 8-38-5(d)(1); ARIZ. REV. STAT. § 18-552(E)(1); CAL. CIV. CODE § 1798.82(d); COLO. REV. STAT. § 6-1-716(2)(a)(a.2)(I); FLA. STAT. § 501.171(4)(e)(1); IOWA CODE § 715C.2(5); N.H. REV. STAT. ANN. § 359-C:20(IV); N.M. STAT. ANN. § 57-12C-7; OR. REV. STAT. § 646A.604(5)(b); VT. STAT. ANN. tit. 9, § 2435(b)(5); WASH. REV. CODE § 19.255.010(2)(6)(b)(iii); WYO. STAT. ANN. § 40-12-502(e).

Categories of personal information reasonably believed to have been breached (e.g., username, password, date of birth, social security number)	Alabama, Arizona, California, Colorado, Florida, Hawaii, Iowa, Maryland, Michigan, Missouri, New Hampshire, New Mexico, New York, North Carolina, Oregon, Puerto Rico, Vermont, Virginia, Washington, West Virginia, Wyoming[187]
Content Required	**U.S. Jurisdiction**
Whether notice was delayed as a result of a law enforcement	California, Wyoming[188]

[187] . ALA. CODE § 8-38-5(d)(2); ARIZ. REV. STAT. § 18-552(E)(2); CAL. CIV. CODE § 1798.82(d); COLO. REV. STAT. § 6-1-716(2)(a)(a.2)(II); FLA. STAT. § 501.171(4)(e)(2); HAW. REV. STAT. § 487N-2(d)(2); IOWA CODE § 715C.2(5); MD. CODE ANN., COM. LAW § 14-3504(g)(1); MICH. COMP. LAWS § 445.72(6); MO. ANN. STAT. § 407.1500(2)(4); N.H. REV. STAT. ANN. § 359-C:20(IV); N.M. STAT. ANN. § 57-12C-7; N.Y. GEN. BUS. LAW § 899-aa(7); N.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5)(c); P.R. LAWS ANN. tit. 10, § 4053; VT. STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(6)(b)(ii); W. VA. CODE § 46A-2A-102(d); WYO. STAT. ANN. § 40-12-502(e).

[188] . CAL. CIV. CODE § 1798.82(d); WYO. STAT. ANN. § 40-12-502(e).

investigation	
The steps the organization has taken to protect impacted individuals and their personal information from further unauthorized access or acquisition	Alabama, California, Hawaii, Michigan, North Carolina, Vermont, Virginia, Wyoming[189]
Advice regarding additional steps the impacted individuals can take to further protect themselves and their personal information	Alabama, California, Colorado, Hawaii, Illinois, Iowa, Maryland, Massachusetts, Michigan, Missouri, New Mexico, North Carolina, Oregon, Vermont, Virginia, Wyoming[190]
Content Required	**U.S. Jurisdiction**

[189] . ALA. CODE § 8-38-5(d)(3); CAL. CIV. CODE § 1798.82(d); HAW. REV. STAT. § 487N-2(d)(3); MICH. COMP. LAWS § 445.72(6); N.C. GEN. STAT. § 75-65(d); VT. STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A); WYO. STAT. ANN. § 40-12-502(e).

[190] . ALA. CODE § 8-38-5(d)(4); CAL. CIV. CODE § 1798.82(d); COLO. REV. STAT. § 6-1-716(2)(a)(a.2)(VI); HAW. REV. STAT. § 487N-2(d)(5); 815 ILL. COMP. STAT. 530/10(a)(iii); IOWA CODE § 715C.2(5); MD. CODE ANN., COM. LAW § 14-3504(g)(4); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS § 445.72(6); MO. ANN. STAT. § 407.1500.2(4); N.M. STAT. ANN. § 57-12C-7; N.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5)(f); VT. STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A); WYO. STAT. ANN. § 40-12-502(e).

Contact information for the organization reporting the breach	Alabama, California, Colorado, Florida, Hawaii, Maryland, Michigan, Missouri, New Hampshire, New Mexico, New York, North Carolina, Oregon, Puerto Rico, Vermont, Virginia, Washington, West Virginia, Wyoming[191]
Toll-free numbers and addresses of the three major credit reporting agencies and/or FTC	Arizona, California, Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon, Washington, West Virginia, Wyoming[192]

As with most aspects of notice, content requirements vary by jurisdiction, with some, like North Carolina and California, requiring very specific language to be included, and others, like Massachusetts, identifying information that should *not* be included. For example, California requires the notice to be titled "Notice of Data Breach" and to include very specific headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and

191 . ALA. CODE § 8-38-5(d)(5); CAL. CIV. CODE § 1798.82(d); COLO. REV. STAT. § 6-1-716(2)(a)(a.2)(III); FLA. STAT. § 501.171(4)(e)(3); HAW. REV. STAT. § 487N-2(d)(4); MD. CODE ANN., COM. LAW § 14-3504(g)(2); MICH. COMP. LAWS § 445.72(6); MO. ANN. STAT. § 407.1500(2)(4); N.H. REV. STAT. ANN. § 359-C:20(IV); N.M. STAT. ANN. § 57-12C-7; N.Y. GEN. BUS. LAW § 899-aa(7); N.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5)(d); P.R. LAWS ANN. tit. 10, § 4053; VT. STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(6)(i); W. VA. CODE § 46A-2A-102(d); WYO. STAT. ANN. § 40-12-502(e).

192 . ARIZ. REV. STAT. § 18-552(E)(3)—(4); CAL. CIV. CODE § 1798.82(d); COLO. REV. STAT. § 6-1-716(2)(a.2)(IV)—(V); 815 ILL. COMP. STAT. 530/10(a)(i)—(ii); IOWA CODE § 715C.2(5); MD. CODE ANN., COM. LAW § 14-3504(g)(3)—(4); MO. ANN. STAT. § 407.1500(2)(4); N.M. STAT. ANN. § 57-12C-7; N.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5)(e); WASH. REV. CODE § 19.255.010(6)(b)(iv); W. VA. CODE § 46A-2A-102(d); WYO. STAT. ANN. § 40-12-502(e).

"For More Information."[193] Similarly, North Carolina sets forth specific language to be used in explaining to impacted individuals what additional steps they may take to protect themselves (e.g., the use of a security freeze).[194] Massachusetts, on the other hand, actually prohibits the notice to include a description of the nature of the breach; therefore, in the event a data breach impacts residents in Massachusetts as well as other jurisdictions, like California, notice to Massachusetts residents will need to be made separately (since all other jurisdictions require notice to contain a brief description of the breach).[195] To that end, the Massachusetts Attorney General has created a sample data breach notification letter and posted it on the Massachusetts Attorney General's website. Though the Massachusetts data breach notification law does not require the use of this sample notice, based on the experience of the drafting team, the Massachusetts Attorney General's office has *strongly* encouraged the use of such sample notice in notifying impacted Massachusetts residents. As a result, scrutiny and consultation of the specific statutory language is advisable to ensure all specific content requirements are satisfied in any crafted notice.

In addition to the above general categories of content, many jurisdictions now require organizations to provide identity theft prevention and mitigation services (a.k.a. "credit monitoring") to impacted individuals *for free* for at least twelve

193 . CAL. CIV. CODE § 1798.82(d).

194 . N.C. GEN. STAT. § 75-63(p).

195 . MASS. GEN. LAWS ch. 93H, § 3(b).

months.[196] Connecticut now requires organizations to provide twenty-four months of free credit monitoring.[197]

For incidents requiring notifications in jurisdictions outside the U.S., the method, form and content of notices will be dictated by the laws of those jurisdictions. The organization should retain local counsel and consult local laws and regulators' websites to prepare notices that meet the jurisdiction-specific requirements. In some cases, the requirements in jurisdictions outside the U.S. may be sufficiently similar that substantively similar notices can be provided across multiple jurisdictions.

[196] . *See, e.g.*, CAL. CIV. CODE § 1798.82(d). Connecticut's Attorney General has adopted this approach as a matter of policy, even though it is not required under that state's statute.

[197] . Conn. Gen. Stat. § 36a-701b(b)(2)(B). A more detailed discussion of credit monitoring can be found in Section V.F., supra.

VII. AFTER-ACTION REVIEWS

A major theme of incident response guidance is that data breaches and security incidents are a recurring threat, and the threat landscape constantly changes. IRPs should be comprehensive, adaptive, and regularly updated to work effectively in this dynamic environment. After-action review is critical to the continuous improvement process. It also provides an opportunity to identify which areas of the IRP worked or failed, to update the IRP and internal practices and policies with a view towards preventing the same type of incident from occurring again, and to address blind spots that the IRP did not account for.

Data breaches and security incidents are a cycle, not discrete stages. There might not be a bright line that separates the "during" phase of incident response from the "after." Depending on the size and nature of the incident, the affected organization needs to continue monitoring for anomalies and repeated attempts to gain access to its systems, even as it compiles data for after-action reports. If an unauthorized access reoccurs, the organization may need to evaluate what phase of the IRP it truly is in, especially if the new attack is from the same source.

As the organization moves into the "after" phase, it should continue to use its IRP as a checklist. Depending on its level of detail, the IRP may call for an overall report to the management group that is responsible for the governance of the IRP, as well as reports for specific audiences. The nature and scope of the incident will also determine how broad or narrow the after-action report needs to be. Incidents that are localized may only require a review of practices within that group, while major incidents may necessitate an organization-wide review. The need and scope depend on the organization's size, the extent and sophistication of the

incident, and how well existing policies and procedures enabled identification and remediation of the incident.

Post-incident assessments should focus on how well the IRP worked as a guide to decision-making and action-planning before and during the incident. The roles and performance of internal functions and individuals, and of outside resources, should also be assessed. As a reflection on a crisis that has passed, the assessment should be constructive. The following should be considered:

- Did members of the IRT know answers to the questions that arose?
- If not, did they know how to find answers quickly?
- Were they able to improvise effectively if a novel situation presented itself?
- Was the IRP activated in a timely fashion?
- Were outside resources (e.g., outside counsel, forensic and security consultants, breach communications specialists, insurers) notified and engaged at the right times?
- Were necessary contracts in place, and did third parties perform to agreed-upon service levels?
- Were outside resources effective?
- Did members of the IRT (including outside resources) communicate effectively, timely, and efficiently?
- Was the incident due to a gap in the written information security plan or was it beyond the organization's control?

If the evaluation of either the IRP or the performance of the people who executed it reveals areas for improvement, a plan should be made to close the gaps. Even if the after-action report concludes that the incident was not reasonably

avoidable, why that conclusion was reached should be documented to demonstrate the organization's active adherence to the IRP, and the reasonableness of its practices.

In addition to evaluating the plan and the performance of the individuals who executed it, the organization should reexamine the policies, processes, and procedures that support data security and data incident preparedness in the period immediately following an incident. If inconsistencies or gaps in supporting documents come to light, they should be addressed. Gaps might also signal the need for additional training and table-top exercises. Particular attention should be paid to the incident's cause—some incidents are not reasonably avoidable because they result from pervasive, newly discovered flaws in technology systems. Other incidents may be caused because particular Vendors, technologies, or practices are not sufficiently robust. Technologies or practices that cause recurring issues, or that are implicated repeatedly in the organization's incidents, should be evaluated to see if they are reasonable and appropriate for the organization from a security perspective.

Given the criticality of communications to effective incident response, all aspects of communications strategy and tactics should be reviewed. Questions include:

- Were internal lines of communication sufficient and effective?
- Were communications with third-party service providers sufficient and effective?
- Were communications with law enforcement, regulatory bodies, insurers, and the public managed smoothly?

Reports that call for change or gap closure should include details that support the proposed change, the projected cost to implement it, a timeline, and a follow-up plan.

Beyond the tactical evaluations already suggested, post-incident reviews should examine more strategic issues, such as the adequacy of the organizational structure to support a robust incident response. The review should place particular emphasis on whether IRP responsibilities are mismatched, as in cases where responsibility is assigned to a person, department, or division that is unsuitable or lacks the appropriate competencies to carry out the assigned role. Based on the experience of the drafting team, the organization should give serious consideration to separating the security and incident response function from the IT function, because robust security and incident response functions do not always align well with the traditional IT role, which focuses on usability and efficiency of the organization's information technology systems.

The organization should tailor after-action reports to the specific recipient, to fit that person's or group's need to know. The organization should also take care to preserve confidentiality and all applicable privileges it has decided not to waive. Counsel to the IRT should maintain records and reports in accordance with the organization's records retention policy, with counsel being mindful of any additional steps that may be necessary to maintain any privileges that may apply. The after-action review should also examine whether the IRP and internal policies are still in compliance with the organization's legal obligations, especially where those obligations have changed since any previous after-action report.

Finally, in addition to identifying gaps and failures, the parts of the IRP that worked well should be singled out and applied to other parts of the IRP specifically, or the organization more generally. Areas of success may inform the organization how to correct areas that failed or underperformed. The primary objective of the after-action review is to become more prepared for the next incident.

VIII. CONCLUSION

The collection, analysis, and maintenance of information are increasingly essential elements to commerce. The custodian of the information collected is responsible for protecting it and, if it is compromised, taking actions necessary to comply with applicable notification requirements. We hope that organizations and practitioners will find the *Incident Response Guide* a useful tool to assist in preparing for and executing proper responses to incidents of data compromise.

~~APPENDIX A:~~
~~MODEL INCIDENT RESPONSE PLAN~~

APPENDIX A:
MODEL INCIDENT RESPONSE PLAN

II. ~~I.~~ Objective and Scope

This document defines the procedures for responding to information security incidents. It discusses how information is communicated to necessary personnel and how an incident's impact is evaluated. It further outlines guidelines for incident documentation and rules for evidence preservation.

Some examples of potential security incidents include:

- theft, damage, or unauthorized access (e.g., unauthorized logins, broken locks, missing log files, or unscheduled/unauthorized physical entry);
- inaccurate information within databases, logs, files, or other records;
- abnormal system behavior (e.g., unscheduled system reboots, unexpected messages, or abnormal errors in logs); and
- security event notifications (e.g., file integrity alerts, intrusion detection alarms, or physical security alarms).

It is the responsibility of all members of the Incident Response Team ("IRT") to read, understand, and adhere to the procedures described in this Incident Response Plan ("IRP").

III. ~~II.~~ Responsible Party

The IRT, with the assistance of designated outside resources as appropriate, is tasked with providing a fast, effective, and orderly response to security incidents. The team is authorized to take any appropriate steps deemed necessary to mitigate or resolve a security incident. It is responsible for investigating suspected security incidents in a timely manner and reporting any findings as set forth in this document.

IV. ~~III.~~ Incident Response Team Identification

[The composition of your IRT should reflect the needs of your organization; Section IV of the Incident Response Guide provides guidance on the composition of the IRT.]

[*LIST HERE – Include 24x7 Contact Information*]

V. ~~IV.~~ Reporting Procedures

The IRT should be notified immediately of any suspected or actual security incidents involving data systems, particularly any critical system, or systems that handle Personally Identifiable Information (PII). If it is unclear as to whether a situation should be considered a security incident, the IRT should be contacted to evaluate the situation.

Except for the steps outlined below, it is imperative that any investigative or corrective action be undertaken by trained personnel or under the oversight of trained personnel, to ensure the integrity of the incident investigation and recovery process.

When faced with a potential situation, the Information Technology (IT) team, in consultation with the IRT to the most reasonable degree possible, will take the following actions:

- A compromised computer system should be examined immediately.
  - The system should remain powered on and all currently running computer programs left as is.
  - Do not shutdown or restart the computer.
  - Immediately disconnect the computer from the network by removing the network cable from the back of the computer.[198]

[198] . If the computer is a virtual machine, it should be snapshotted and archived. Then the running version should have virtual Network Interface Controllers disabled but be left in running condition.

- Information about a security incident can come to light anywhere in the organization.
  - Information about any suspected or actual incidents are reported to the Chair of the IRT.
  - All communications with law enforcement or the public will be coordinated by the Legal Representative(s) of the IRT.
  - Document immediately all key information known about the incident, including:
- date and time of discovery, and the nature of the incident;
- immediate action taken in response to the incident; and
- date and time the IRT was notified of the incident.

VI. ~~V.~~ Severity Classification

The IRT will determine if the security incident justifies activating the IRP. If the IRT decides it does not, the incident will be delegated to one of the members of the IRT for resolution.

The following classifications will be used to help guide the response that the IRT should take:

- **Level One**—Potentially unfriendly activity, e.g.:
  - Unauthorized port scans
  - Virus detection with automated correction
  - Unexpected performance peak
  - Other routine minor events
- **Level Two**—Clear attempts to obtain unauthorized information or access, e.g.:
  - Unauthorized vulnerability scans
  - Attempt to access restricted areas

- Virus infection on a noncritical system
- Level One incidents occurring against systems storing sensitive data, including PII or Non-Public Information
- Level One incidents originating from unauthorized internal systems
- Repeated Level One incidents from a single source
- Other similar incidents

- **Level Three**—Serious attempt or actual breach of security, e.g.:
  - Multi-pronged attack
  - Denial-of-service attempt
  - Virus infection on a critical system or the network
  - Successful unauthorized access to sensitive data or systems
  - Repeated Level Two incidents from a single source
  - Other similar incidents

VII. ~~VI.~~ Response Procedures

A. Response Process

Any given response to an incident can include—or proceed through—each of the following stages: identification, classification, containment, eradication, recovery, and root cause analysis. When possible, these steps will be taken in parallel.

At a minimum, the following actions should be taken once an incident has been identified and classified:

- If **Level One**—Contain and Monitor

- Record source of the incident (e.g., user, internet protocol (IP) address, etc.).
- Use technology controls to temporarily or permanently block the source.
- Monitor the source for future incidents.

- If **Level Two**—Contain, Monitor, and Warn
  - Perform all actions in Level One.
  - Collect and protect information associated with the incident.
  - Determine the origin of the incident.
  - Eliminate the intruder's means of access and related vulnerabilities.
  - Provide breach notifications to applicable federal and state authorities, and to affected individuals as appropriate.
  - Notify insurance carrier and broker.
  - Review incident to determine if it should be reclassified to Level Three.
- If **Level Three**—Contain, Eradicate, Recover, and Analyze the Root Cause
  - Perform all actions in Level One and Level Two.
  - Contain the incident and determine further action. Consider limiting or eliminating network access and applying more restrictive access controls, deactivating switch ports, etc.
  - Collect and protect information associated with the incident, which may include offline methods. In the event that a forensic investigation is required, the IRT will identify appropriate internal and external resources to perform that investigation.

- Notify Chief Executive Officer of the situation and provide progress updates as necessary.
- Research potential risks or damage caused by the identified method of intrusion.

B. Root Cause Analysis

Not more than one week after completing the response for any incident and the required activation of the IRP, members of the IRT and the affected parties as identified by the IRT will meet to review the results of the investigation conducted to determine the root cause of the compromise and evaluate the effectiveness of the IRP. Other security controls will also be reviewed to determine their appropriateness for the current risks. Any identified areas in which the plan, policy, or security control can be made more effective or efficient, including training and education, must be updated accordingly. Upon conclusion of an investigation, compromised systems will be reimaged to a clean and uncompromised state.

VIII. ~~VII.~~ Reporting

All employees have an obligation to report any known or suspected violation of this policy to the IRT.

IX. ~~VIII.~~ Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

X. ~~IX.~~ Exceptions

Exceptions to this policy may exist where the exception has been:

- documented for its legitimate business purpose;
- approved by a Director or above; and
- recorded for audit purposes.

~~APPENDIX B:~~
~~MODEL NOTIFICATION LETTER~~

APPENDIX B:
MODEL NOTIFICATION LETTER – U.S.

Subject: IMPORTANT DATA SECURITY INCIDENT INFORMATION

[Date]

We greatly value your business and respect the privacy of your information, which is why we are writing to inform you that we recently learned of a serious data security incident, which took place [on [date] or from [date] to [date]], in which personal, private, and unencrypted credit and debit card information was accessed by an outside party and compromised.

The compromised information included your name, shipping address, billing address, credit card security code, and credit and/or debit card number. We are working around the clock, with the aid of outside resources, to help you avoid—or at least minimize—any negative consequences.

We are in the process of reporting the incident to the appropriate state agencies and federal authorities to initiate an investigation. Our notification has not been delayed as a result of any law enforcement investigation.

We are notifying you so you can take additional actions to minimize or eliminate potential personal harm. Because this is a serious incident, **we strongly encourage you to take the following preventive measures to help detect and mitigate any misuse of your information**:

1. [Client] is providing each impacted customer with free credit monitoring services through [details of credit monitoring services]. In the meantime, we encourage you to consider the other action items listed in this communication.

2. Closely monitor your financial accounts and promptly contact your financial institution if you notice any unusual activity. You may also wish to contact your credit or debit card issuer to determine whether a new card should be issued and whether additional levels of security or protective measures should be placed on your account(s).
3. We strongly encourage you to report incidents of suspected identity theft to your local law enforcement, the Federal Trade Commission, and your state attorney general.
4. We also recommend that you monitor your free credit reports. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, by calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.
5. You also may want to place a security freeze on your credit files by calling each of the three credit reporting agencies. Freezing credit files will prevent someone from using your personal information to open new accounts or borrow money in your name. Please understand that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card unless you temporarily or permanently remove the freeze.

While we have already notified the three major credit reporting agencies, we strongly encourage you to contact the credit reporting agencies directly to notify them, receive credit alerts, or freeze your credit files. Contact for the three agencies is provided below:

Equifax	Experian	TransUnion
~~P.O. Box 740241 Atlanta, GA 30374~~ADDRESS General: ~~1-888-685-1111~~ # Fraud alert: ~~1-888-766-0008~~ # Security freeze: ~~1-800-685-1111~~ # https://www.equifax.com/personal/credit-report-services/credit-freeze/	~~P.O. Box 2104 Allen, TX 75013~~ADDRESS ~~1-888-397-3742~~ # www.experian.com/freeze	~~P.O. Box 2000 Chester, PA 19022~~ADDRESS General: ~~1-800-888-4213~~ # Identity theft and fraud: ~~1-800-680-7289~~ # www.transunion.com/credit-freeze/place-credit-freeze

You may also contact the Federal Trade Commission to receive information about fraud alerts, security freezes, and preventing identity theft:

1-877-ID-THEFT (877-438-4338)
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
https://www.consumer.ftc.gov/features/feature-0014-identity-theft

Maryland residents may wish to review information provided by the Maryland Attorney General at ~~https://www.oag.state.md.us/idtheft/businessGL.htm~~https://www.oag.state.md.us/idtheft/businessGL.htm, by calling 888-743-0023, or writing to the Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202. Maryland residents may contact the attorney general for information about preventing identity theft.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov, by calling 877-566-7226, or by writing to the Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699. North Carolina residents may contact the attorney general for information about preventing identity theft.

We sincerely regret this incident and any inconvenience it may cause. We will do everything we can to mitigate any negative consequences of this unfortunate incident. We also want you to know that we have determined the cause of the incident and have taken action to prevent future incidents of this nature.

[Details about efforts to prevent future breaches].

Thanks for your ongoing patience and understanding as we work through this process. Please call [toll-free number] with any questions or to receive further assistance.

Sincerely,

[Signature and Contact Information]

~~APPENDIX C:~~
~~MODEL NOTIFICATION LETTER – MASSACHUSETTS~~

APPENDIX C:
MODEL NOTIFICATION LETTER—MASSACHUSETTS

Subject: IMPORTANT DATA SECURITY INCIDENT INFORMATION

[Date]

We recently learned of a serious data security incident, which took place [on [date] or from [date] to [date]], in which personal, private, and unencrypted information was likely compromised.

We believe the compromised information could reasonably be used to make fraudulent credit or debit card purchases. We are working around the clock, with the aid of outside resources, to help you avoid or at least minimize any negative consequences.

We are in the process of reporting the incident to the appropriate state agencies and federal authorities to initiate an investigation. Our notification has not been delayed as a result of any law enforcement investigation.

We are notifying you so you can take additional actions to minimize or eliminate potential personal harm. Because this is a serious incident, **we strongly encourage you to take the following preventive measures to help detect and mitigate any misuse of your information:**

1. [Client] is providing each impacted customer with free credit monitoring services [describe services].
2. Closely monitor your financial accounts and promptly contact your financial institution if you notice any unusual activity. You may also wish to contact your credit or debit card issuer to determine whether a new card should be issued and whether additional

levels of security or protective measures should be placed on your account(s).

3. We strongly encourage you to report incidents of suspected identity theft to your local law enforcement and state attorney general.
4. We also recommend that you monitor your free credit reports. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every twelve months by visiting www.annualcreditreport.com, by calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.
5. You also may want to place a security freeze on your credit files by calling each of the three credit reporting agencies. Freezing credit files will prevent someone from using your personal information to open new accounts or borrow money in your name. Please understand that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card unless you temporarily or permanently remove the freeze. Note that, in Massachusetts, placing or lifting a security freeze is free for victims of identity theft, but in other cases, credit reporting agencies may charge up to $5 each to place, lift, or remove a security freeze. If you choose to obtain a security freeze by directly contacting the credit reporting agencies, you must send a letter by regular certified mail to each of the credit reporting

agencies listed below. The letter should include your name, address, date of birth, social security number, and credit card number and expiration date for payment, if applicable. Each of the credit reporting agencies has specific requirements to place a security freeze. Review these requirements on the website for each prior to sending your written request. For more information see ~~http://www.mass.gov/ago/consumer-resources/consumer-information/scams-and-identity-theft/identity-theft/fraud-alerts.html~~http://www.mass.gov/ago/consumer-resources/consumer-information/scams-and-identity-theft/identity-theft/fraud-alerts.html.

While we have already notified the three major credit reporting agencies, we strongly encourage you to contact the credit reporting agencies directly to notify them, receive credit alerts, or freeze your credit files. Contact for the three agencies is provided below:

Equifax	**Experian**	**TransUnion**
~~P.O. Box 740241 Atlanta, GA 30374~~ADDRESS General: ~~1-888-685-1111~~# Fraud alert: ~~1-888-766-0008~~# Security freeze: ~~1-800-685-1111~~# https://www.equifax.com/personal/credit-report-services/credit-freeze/	~~P.O. Box 2104 Allen, TX 75013 1-888-397-3742~~ ADDRESS # www.experian.com/freeze	~~P.O. Box 2000 Chester, PA 19022~~ADDRESS General: ~~1-800-888-4213~~# Identity theft and fraud: ~~1-800-680-7289~~# www.transunion.com/credit-freeze/place-credit-freeze

You may also contact the Federal Trade Commission to receive information about fraud alerts, security freezes, and preventing identity theft:

1-877-ID-THEFT (877-438-4338)
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
https://www.consumer.ftc.gov/features/feature-0014-identity-theft

In addition, as a Massachusetts resident, you have the right to obtain a police report if you are the victim of identity theft.

We sincerely regret this incident and any inconvenience it may cause. We will do everything we can to mitigate any negative consequences of this unfortunate incident. We also want you to know that we have determined the cause of the incident and have taken action to prevent future incidents of this nature.

Thanks for your ongoing patience and understanding as we work through this process.

Sincerely,

[Name and Contact Information]

~~APPENDIX D:~~
~~MODEL ATTORNEY GENERAL BREACH NOTIFICATION—MARYLAND~~

APPENDIX D:
MODEL ATTORNEY GENERAL BREACH NOTIFICATION—MARYLAND

[typically communicated by counsel]

[Date]

VIA EMAIL

Office of the Attorney General of the State of Maryland

E-mail: Idtheft@oag.state.md.us

Re: Data Security Breach Notification

To Whom It May Concern:

[Client], a client of [name of law firm], is notifying the Office of the Attorney General of the State of Maryland that [client] intends to notify [number] residents of Maryland about the data security incident described below.

[On [date] or from [date] to [date]], a third party obtained customer data from [client] by hacking into [client]'s internal computer network. The data stolen included names, shipping and billing addresses, credit/debit card numbers, and credit security codes.

[Client] has reported the incident to appropriate law enforcement authorities to initiate an investigation and is in the process of notifying the three major U.S. credit reporting agencies. It also plans to offer free credit monitoring services to the affected residents. [Information about steps [client] is taking to restore the integrity of the system.]

[Client] now intends to notify affected Maryland residents of the data security incident. A sample of the notification to the Maryland residents is enclosed.

If you would like any additional information concerning the above event, please feel free to contact us at your convenience.

Sincerely,

[Counsel]
Enclosure

~~APPENDIX E:~~
~~MODEL ATTORNEY GENERAL BREACH NOTIFICATION—CONNECTICUT~~

APPENDIX E:
MODEL DATA SUBJECT BREACH NOTIFICATION—EUROPEAN UNION/UNITED KINGDOM

[DATE]

VIA EMAIL

SUBJECT LINE: NOTIFICATION OF A PERSONAL DATA BREACH

DEAR [NAME]:

WE REGRET TO INFORM YOU THAT WE HAVE RECENTLY DISCOVERED AN INCIDENT THAT AFFECTED THE SECURITY OF SOME OF THE PERSONAL DATA THAT WE HOLD ABOUT YOU. WE ARE WRITING TO INFORM YOU OF THE INFORMATION WE KNOW ABOUT THIS INCIDENT, STEPS WE HAVE TAKEN SINCE DISCOVERING THE INCIDENT, AND ADVICE TO YOU ON HOW TO MITIGATE ANY FURTHER EFFECTS.

THE BREACH INCIDENT WAS DISCOVERED ON [DATE] AND IS LIKELY TO HAVE TAKEN PLACE ON [DATE].

AS A RESULT OF OUR INVESTIGATION OF THE BREACH INCIDENT, WE HAVE IDENTIFIED THAT:

- THE BREACH AFFECTS THE FOLLOWING TYPES OF INFORMATION:
  - [TYPES OF INFORMATION, FOR EXAMPLE, FINANCIAL, SPECIAL CATEGORY DATA, CRIMINAL OFFENCE DATA].
- THE INFORMATION HAS BEEN [ACCIDENTALLY OR UNLAWFULLY DESTROYED OR CORRUPTED OR LOST OR ALTERED OR DISCLOSED WITHOUT AUTHORISATION OR ACCESSED BY [[NAME OR DESCRIPTION OF ORGANISATION] OR AN UNAUTHORISED PERSON]].

- THE BREACH OCCURRED UNDER THE FOLLOWING CIRCUMSTANCES AND FOR THE FOLLOWING REASONS:
  - [CIRCUMSTANCES].
  - [REASONS].

WE TAKE THE SECURITY OF YOUR PERSONAL DATA SERIOUSLY AND FOLLOWING THE INVESTIGATION CARRIED OUT INTO THE BREACH INCIDENT, WE HAVE IMPLEMENTED THE FOLLOWING ADDITIONAL MEASURES TO MITIGATE AGAINST THE RISK OF THIS TYPE OF INCIDENT HAPPENING AGAIN, INCLUDING [INSERT CONTAINMENT/REMEDIATION MEASURES].

THERE ARE SOME GENERAL STEPS THAT EVERYONE CAN TAKE TO HELP PROTECT THEIR PERSONAL DATA AGAINST THESE TYPES OF INCIDENTS. FOR EXAMPLE, WE RECOMMEND THAT YOU TAKE THE FOLLOWING MEASURES:

- USE DIFFERENT, SECURE PASSWORDS FOR DIFFERENT WEBSITES
- DO NOT STORE YOUR PASSWORDS ON YOUR COMPUTER/DEVICES (E.G. IN A TEXT FILE)
- ALWAYS BE AWARE OF ANY SUSPICIOUS EMAILS OR OTHER COMMUNICATIONS, WE WILL NOT CONTACT YOU IN ANY WAY TO REQUEST SENSITIVE PERSONAL DATA.
- [INSERT OTHER RELEVANT MEASURES].

[WE INFORMED THE [APPLICABLE REGULATOR(S)] OF THE BREACH ON [DATE].]

WE APOLOGISE FOR ANY INCONVENIENCE THIS INCIDENT MAY CAUSE YOU. PLEASE CONTACT OUR CUSTOMER SERVICE TEAM AT [INSERT EMAIL] OR [INSERT ADDRESS] IF YOU HAVE ANY QUESTIONS OR REQUIRE ANY FURTHER INFORMATION.

YOURS SINCERELY,

[NAME]

MODEL ATTORNEY GENERAL BREACH NOTIFICATION—CONNECTICUT

[typically communicated by counsel]

[Date]

VIA EMAIL

Office of the Attorney General of the State of Connecticut

Email: ag.breach@ct.gov

Re: Data Security Breach Notification

To Whom It May Concern:

[Client], a client of [name of law firm], is notifying the Office of the Attorney General of the State of Connecticut that [client] intends to notify [number] residents of Connecticut about the data security incident described below.

[On [date] or from [date] to [date]], a third party obtained customer data from [client] by improperly accessing [client]'s internal computer network. The data accessed included names, shipping and billing addresses, credit/debit card numbers, and credit security codes.

[Client] has reported the incident to appropriate law enforcement authorities to initiate an investigation and is in the process of notifying the three major U.S. credit reporting agencies. It also plans to offer free credit monitoring services to the affected residents. [Information about steps [client] is taking to restore the integrity of the system.]

[Client] now intends to notify affected Connecticut residents of the data security incident. A sample of the notification to the Connecticut residents is enclosed.

Notification was not delayed because of a law enforcement investigation.

If you would like any additional information concerning the above event, please feel free to contact us at your convenience.

Sincerely,

[Counsel]

Enclosure

~~APPENDIX~~APPENDIX F:
GLBA ~~AND~~AND HIPAA

I. Special Requirements in the United States:

A. Gramm-Leach-Bliley Act (GLBA)[199]

1. Governs data security for financial institutions and any other business engaged in financial activities, such as:

- lending, investing, or safeguarding money or securities for others;
- insuring, indemnifying, or guaranteeing against loss, harm, damage, illness, or death;
- providing or issuing annuities or acting as a broker for such;
- providing financial, investment, or economic advisory services; or
- underwriting or dealing in securities.

2. Obligations are triggered where there is:

- unauthorized access to, or use of, customer information maintained by a financial institution or its service provider;
- misuse of customer information or it is reasonably possible that customer information will be misused; or
- misuse of customer information that could result in substantial harm or inconvenience to customers.

3. Response should include:

- assessing nature and scope of incident;

[199] . Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et. seq.*

- identifying what customer information has been accessed or misused;
- notifying primary federal regulator of unauthorized access or use;
- providing Suspicious Activity Report ("SAR") to the Financial Crimes Enforcement Network (FinCEN);
- notifying law enforcement;
- containing and controlling the incident to prevent further unauthorized access or use;
- notifying customers, when warranted (if misuse has occurred or is reasonably possible, notify affected customers as soon as possible); and
- if the institution cannot determine which specific customers are affected, notifying the entire group of customers whose files have been accessed.

4. Notice should include the following:

- Description of the data breach
- Description of the customers' information subject to unauthorized access or use
- Telephone number customers can call for further information and assistance
- Reminder to customers to monitor accounts for twelve to twenty-four months
- Recommendation that customers promptly report incidents of suspected identity theft
- Description of what the institution has done to protect customers' information from further unauthorized access
- For large breaches, publication of notice on the organization's website and in major local media

- Information about what happened, how consumers can protect themselves from potential future harm, and contact information for the notifying party

B. Health Insurance Portability and Accountability Act of 1996 (HIPAA)[200]/Health Information Technology for Economic and Clinical Health (HITECH) Act[201]

1. Notification obligations triggered following breach

- Breach presumed when there is an impermissible use or disclosure of ~~Personal~~Protected Health Information (PHI), unless risk assessment demonstrates low probability that PHI has been compromised
- For matters involving ransomware, the United States Department of Health and Human Services has issued guidance that should be considered.[202]

2. When to notify

- Following the unauthorized acquisition, access, use, or disclosure of unsecured (i.e., unencrypted) information relating to individuals' past, present, or future physical or mental health and the provision of health care
- Without unreasonable delay, not later than sixty days following the discovery of a breach

---

[200] . Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d *et. seq.*

[201] . Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. § 17931 *et. seq.*

[202] https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html.

3. Who to notify

- Affected individuals
- Media, if over 500 individuals in a single state or jurisdiction
- Secretary of Health and Human Services
- Notice shall include:
  - a brief description of the breach;
  - a description of the types of information that were involved;
  - the steps affected individuals should take to protect themselves from potential harm;
  - what the provider is doing to investigate the breach, mitigate the harm, and prevent further breaches; and
  - contact information for the provider.

0

Document comparison by Workshare Compare on Monday, May 01, 2023 9:11:44 AM

Input:	
Document 1 ID	file://C:\Users\ayu\Downloads\v1 Incident Response Guide final Word 1-9-20.1.docx
Description	v1 Incident Response Guide final Word 1-9-20.1
Document 2 ID	file://C:\Users\ayu\Downloads\v2 Incident Response Guide 2d Edition.docx
Description	v2 Incident Response Guide 2d Edition
Rendering set	Standard

Legend:	
Insertion	
~~Deletion~~	
~~Moved from~~	
Moved to	
Style change	
Format change	
~~Moved deletion~~	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:	
	Count
Insertions	431
Deletions	176
Moved from	0
Moved to	0
Style changes	0
Format changes	0
Total changes	607