The Sedona Conference Working Group Series

The Sedona Conference

Incident Response Guide

A Project of The Sedona Conference Working Group
on Data Security and Privacy Liability (WG11)

March 2018
Public Comment Version
Submit comments by **June 19, 2018**, to
comments@sedonaconference.org.

The Sedona Conference Incident Response Guide

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

MARCH 2018 PUBLIC COMMENT VERSION

Author:	The Sedona Conference
Editor-in-Chief:	Robert E. Cattanach
Editors:	M. James Daley April Doss Warren G. Kruse II Kari M. Rollins Jo Anne Schwendinger Leon Silver Joseph Swanson Michael Whitt
Steering Committee Liaison:	Matthew Meade
Staff Editors:	Susan McClain Michael Pomarico

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, click on the "Sponsors" navigation bar on the homepage of our website.

Preface

Welcome to the public comment version of The Sedona Conference *Incident Response Guide*, a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages. We hope the *Incident Response Guide* will be of immediate and practical benefit to organizations, attorneys, and jurists.

The Sedona Conference acknowledges Editor-in-Chief Bob Cattanach for his leadership and commitment to the project. We also thank editors Jim Daley, April Doss, Warren Kruse, Kari Rollins, Jo Anne Schwendinger, Leon Silver, Joe Swanson, and Michael Whitt for their efforts. We acknowledge the assistance of Sam Bolstad, Samir Islam, Lauri Dolezal, and Colman McCarthy. Finally, we also thank Matt Meade, who provided valuable counsel as Steering Committee liaison.

Please note that this version of the *Incident Response Guide* is open for public comment and suggestions for improvement are welcome. Please submit comments by June 19, 2018, to comments@sedonaconference.org. The editors will review the public comments and determine what edits are appropriate for the final version.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
March 2018

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 in 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 other more specific obligations that may exist depending on the industry sector involved, particularly health care and financial, and especially the requirements of other international jurisdictions including the European Union with the advent of its General Data Protection Regulation (GDPR).

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 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

I. INTRODUCTION

In today's connected world, compromise of electronically stored information (ESI) 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, 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 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 analysis of legal obligations.

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, at the locations where they exist. This can help assess legal obligations in the ordinary course of business, as well as 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.

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."

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 cybersecurity framework?
- Does the Vendor have adequate insurance, including cyber liability coverage?
- What history does the Vendor have in suffering from 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, the nature of security threats, and standard industry practices.

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, 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 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 be held.

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).

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. 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—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, vulnerabili-

ties, 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 Public Comment Version of The Sedona Conference *Commentary on Application of Attorney-Client Privilege and Work Product Protection to Documents and Communications Generated in the Data Security Context* (forthcoming 2018). For the purposes of this Guide, suffice it to say that counsel is likely to play a significant role in responding to any incident.

IV. EXECUTING THE INCIDENT RESPONSE PLAN

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

The IRP is triggered when a "threat actor"[1] initiates an action which disrupts the organization's cyber infrastructure[2] 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 or 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 media or conventional press), or even the malicious actor him or herself.

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, they may inform the full IRT and even inform 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 that the incident is minor and needs no escalation, prior to the incident defaulting to a more serious status.

---

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

2 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.

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 (ERM) 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 staffed internally by the organization:

- IT
- Cybersecurity
- Legal
- Compliance
- Privacy
- Human Resources
- Risk Management
- 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 also 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 has been affected ("I"), and whether the availabil-

ity 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 whether more significant effort will be required.[3]

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) integrally involved in directing these initial steps will help ensure that the IRT is cognizant of its legal obligations. 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, 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.

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;
- insurance policy requirements;
- contractual-reporting or information-sharing requirements;
- legal hold requirements and obligations to preserve evidence; 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 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.

---

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

D. Evolution of the Incident Response

At the beginning of any incident, necessary information is invariably 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 same process may take several days. 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, 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 that will have 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, which is by no means guaranteed merely by counsel's involvement. Counterbalancing that consideration is the need to disseminate critical information throughout the IRT more quickly. Quick dissemination risks forfeiting privilege and work-product protections because such communications may later be determined not to qualify for protection.

To be clear, not all communications with counsel qualify for protection; 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 be directed initially to counsel.

In addition to legal requirements, operational considerations 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 which 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.

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. Working with law enforcement typically arises in one of three circumstances:

- There will be a legal requirement to report the matter to law enforcement authorities.
- Reporting the matter to law enforcement is discretionary, with the affected organization retaining some latitude to decide whether reporting the incident to law enforcement 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 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 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 which 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 have a culture of skepticism regarding government action, and find themselves less inclined to believe that information passed to law enforcement entities will be put to good use. Although these intangible factors tend to be matters of culture and policy, rather than strictly legal questions, it is important that organizations with strong preferences in this regard consider these decisions at the leadership level, as leadership may want to consider shareholder expectations, customer expectations, past public relations and public policy positions, or other factors that are unique to that 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 dealing with this issue is to establish, either directly or through outside counsel, a relationship with key law enforcement entities in advance of an incident. By doing that, any reporting to law enforcement is more likely to be done 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 a 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;[4]

- whether a law enforcement investigation could disrupt business operations;[5] 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 entity to which crimes are reported. 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),

---

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

[5] 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.

then state or local law enforcement agencies may be best suited to investigate the theft as a local law enforcement matter. The same might be the case in instances in which a former employee is suspected of committing identity theft while carrying out check cashing fraud using paper checks stolen from the organization.

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 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 was taking place. In such cases that involve a mix of a data security incident and serious criminal activity, the organization should expect to 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.

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 ("ECTF") generally lead U.S. 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. In April 2015, the U.S. Department of Justice issued detailed guidance to victims on factors to consider when reporting cyber

crimes.[6] This guidance can serve as a useful reference both in cybersecurity planning and preparedness, and during incident response. 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.[7] The FBI works through its Cyber Division and its Cyber Task Forces, located in each of its 56 field offices.[8]

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 Center (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."[9]

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.

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 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.

---

6 U.S. DEP'T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS (Version 1.0, April 2015), *available at* https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf.

7 FED. BUREAU OF INVESTIGATION, LAW ENFORCEMENT CYBER INCIDENT REPORTING, *available at* https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf/view (last visited Dec. 13, 2017).

8 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."

9 Europol, *European Cybercrime Centre—EC3*, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (last visited Dec. 13, 2017).

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, and preferably well before the 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; often, once network actions have been taken (including remedial actions like isolating infected servers or devices), it is 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.

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.

- Pre-existing 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 pre-existing communications channels by some personnel with non-sensitive 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).

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 their own IT services staff (whether in-house or provided by a Vendor) can handle the incident investigation on their own. For smaller organizations in particular, there can be a tendency to try to handle the investigation in-house first, 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.

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. Just like the organizations they serve, consulting firms also 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.

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. This topic will be addressed in greater detail in the Public Comment Version of The Sedona Conference *Commentary on Application of Attorney-Client Privilege and Work Product Protection to Documents and Communications Generated in the Data Security*

Context (forthcoming 2018), 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.

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 any 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 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.htmlhttps://www.experian.com/consumer-products/credit-monitoring.html. *That easily qualifies as a concrete injury.*[10]

The clear message from *Neiman Marcus* is that offering credit monitoring is a factor that the court will consider in connection with establishing standing.

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

---

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

very small percentage of the crimes that can be inflicted on them."[11] "Breached companies . . . like to 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."[12] 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."[13]

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 non-financial purposes, i.e., to get a new driver's license, passport, or other identity document."[14] Moreover, credit monitoring will not tell you if someone is using your medical information to get free medical care or medication.

A number of states have adopted a 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).[15]

California's recently 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

---

11 *Are Credit Monitoring Services Worth It?*, KREBS ON SECURITY (Mar. 19, 2014), https://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it (quoting Avivah Litan, fraud analyst at Gartner, Inc.).

12 *Id.*

13 Gregory Karp, *Why Credit Monitoring Will Not Help You After a Data Breach*, CHICAGO TRIBUNE (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.

14 KREBS ON SECURITY, *supra* note 11 (quoting Avivah Litan, fraud analyst at Gartner, Inc.).

15 CAL. CIV. CODE § 1798.82(d)(2)(G).

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.[16]

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.[17] 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."[18] Connecticut Attorney General George Jepsen stated the following, in connection with the announcement of the new Connecticut law:

> The bill also calls for companies who experience breaches to provide no less than one year 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.[19]

The clear message from the Connecticut law, and one which appears to be gaining additional traction in this space, is that companies should not necessarily rely solely on credit monitoring, and need to determine what identity theft prevention service would be appropriate under the circumstances.

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 requirements in their incident response. 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.

---

16 *Id.* at § 1798.82(h).

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

18 *Id.*

19 George Jepsen, *Statement from AG Jepsen on Final Passage of Data Breach Notification and Consumer Protection Legislation*, STATE OF CONN. OFFICE OF THE ATTORNEY GEN. (June 2, 2015), http://www.ct.gov/ag/cwp/view.asp?Q=566508&A=2341 (emphasis added).

G. PCI-Related Considerations

In April of 2016, the Payment Card Industry Security Standards Council (the "Council") promulgated Version 3.2 of the Data Security Standard ("PCI DSS" or "Standard") with new 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."[20] 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."[21] Requirement 12.10.2 requires that the plan be reviewed and tested at least annually.[22]

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.

---

20 PAYMENT CARD INDUS. SEC. STANDARDS COUNCIL, DATA SECURITY STANDARD 113 (Ver. 3.2, Apr. 2016), *available at* https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1510781420590.

21 *Id.*

22 *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 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. 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 regulators have been amending data breach notification laws, organizations should scrutinize the relevant state statutes and state websites for information regarding any changes or amendments to the requirements and rules discussed below.

B. Is Notification Required?

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, including: 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. 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; or if the organization falls under the purview of the Gramm-Leach-Bliley Act (GLBA) or HIPAA).

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-three states recognize some form of this exception[23] (*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	Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Mississippi, Missouri, Nebraska, New Hampshire, New Jersey, North Carolina, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Utah, Vermont, Washington, West Virginia, Wisconsin, and 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, eight states that offer little to no guidance on the meaning of "reasonable likelihood of harm" are: Alaska, Arkansas, Connecticut, Louisiana, Mississippi, Oregon, Pennsylvania, and Washington.[24] 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 is left to the organization in these eight states, 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.

Other states offer more clarity as it relates to the "no harm" exception. For example, states like Florida, Hawaii, Indiana, Kansas, Michigan, Missouri, North Carolina, Oklahoma, Rhode Island, South

---

[23] *See* ALASKA STAT. § 45.48.010(c); ARIZ. REV. STAT. § 18-545(L)(1); ARK. CODE ANN. § 4-110-105(d); COLO. REV. STAT. § 6-1-716(2); 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); LA. REV. STAT. ANN. § 51:3074(G); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MD. CODE ANN., COM. LAW. § 14-3504(b)(2); MICH. COMP. LAWS § 445.72(1); MISS. CODE ANN. § 75-24-29(3); MO. ANN. STAT. § 407.1500(2)(5); 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.C. GEN. STAT. § 75-61(14); OKLA. STAT. tit. 24, § 163(A)-(B); OR. REV. STAT. § 646A.604(8); 73 PA. CONS. STAT. § 2302; 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); VT. STAT. ANN. tit. 9, §§ 2430(8)(C), 2435(d); WASH. REV. CODE § 19.255.010(1); W. VA. CODE § 46A-2A-102(a)-(b); WIS. STAT. § 134.98(2)(cm); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

[24] *See* ALASKA STAT. § 45.48.010(c); ARK. CODE ANN. § 4-110-105(d); CONN. GEN. STAT. § 36a-701b(b)(1); LA. REV. STAT. ANN. § 51:3074(G); MISS. CODE ANN. § 75-24-29(3); OR. REV. STAT. § 646A.604(8); 73 PA. CONS. STAT. § 2302; WASH. REV. CODE § 19.255.010(1).

Carolina, Utah, Vermont, West Virginia, and Wisconsin define "harm" in terms of identity theft, fraud, or other illegal use.[25] In these fourteen 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. Other states such as Arizona and Iowa, as well as Florida, tie "harm" to economic loss.[26] 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.

Ten other states use a slightly different metric. In Colorado, Delaware, Idaho, Maine, Maryland, Nebraska, New Hampshire, New Jersey, Vermont, and Wyoming, the "no harm" exception is generally defined by the actual or potential misuse of the personal information.[27] In these ten states, notice is *not* required if, after reasonable investigation, the organization simply determines that the misuse of the 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	Alaska, Arkansas, Connecticut, Louisiana, Mississippi, Oregon, Pennsylvania, Washington[28]
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, Vermont, Wyoming[29]

---

25 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.C. GEN. STAT. § 75-61(14); OKLA. STAT. tit. 24, § 163(A); 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); VT. STAT. ANN. tit. 9, §§ 2430(8)(C), 2435(d); W. VA. CODE § 46A-2A-102(a)-(b); WIS. STAT. § 134.98(2)(cm).

26 ARIZ. REV. STAT. § 44-7501(L)(1); FLA. STAT. § 501.171(4)(c); IOWA CODE § 715C.2(6).

27 COLO. REV. STAT. § 6-1-716(2); 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, §§ 2430(8)(C), 2435(d); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

28 *See* ALASKA STAT. § 45.48.010(c); ARK. CODE ANN. § 4-110-105(d); CONN. GEN. STAT. § 36a-701b(b)(1); LA. REV. STAT. ANN. § 51:3074(G); MISS. CODE ANN. § 75-24-29(3); OR. REV. STAT. § 646A.604(8); 73 PA. CONS. STAT. § 2302; WASH. REV. CODE § 19.255.010(1).

29 COLO. REV. STAT. § 6-1-716(2); 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, §§ 2430(8)(C), 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**, or other **illegal use** of the personal information	Florida, Hawaii, Indiana, Kansas, Michigan, Missouri, North Carolina, Oklahoma, Rhode Island, South Carolina, Utah, Vermont, West Virginia, Wisconsin[30]
Reasonable likelihood of harm = reasonably likely to cause substantial **economic loss** or **financial harm** to the individual	Arizona, Florida, Iowa[31]

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, seven states require the organization to document that determination and maintain that written record for three to five years, 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	3 years[32]
Alaska, Florida, Iowa, Missouri, New Jersey, Oregon	5 years[33]

Some states, however, require more than mere 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.[34] In Alaska and Vermont, even

---

30 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.C. GEN. STAT. § 75-61(14); OKLA. STAT. tit. 24, § 163(A); 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); VT. STAT. ANN. tit. 9, §§ 2430(8)(C), 2435(d); W. VA. CODE § 46A-2A-102(a)-(b); WIS. STAT. § 134.98(2)(cm).

31 ARIZ. REV. STAT. § 44-7501(L)(1); FLA. STAT. § 501.171(4)(c); IOWA CODE § 715C.2(6).

32 *See* MD. CODE ANN., COM. LAW § 14-3504(b)(4).

33 *See* ALASKA STAT. § 45.48.010(c); FLA. STAT. § 501.171(4)(c); IOWA CODE § 715C.2(6); MO. ANN. STAT. § 407.1500(2)(5); N.J. STAT. ANN. § 56:8-163(a); OR. REV. STAT. § 646A.604(8).

34 CONN. GEN. STAT. § 36a-701b(b)(1); FLA. STAT. § 501.171(4)(c); OR. REV. STAT. § 646A.604(8) ("may" consult, not required).

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.[35] In Florida, after consultation with law enforcement, the organization is to notify the Florida Department of Legal Affairs of the "no harm" determination in writing within thirty days of making the determination.[36] Importantly, the notification and consultation required by these very few states is not considered part of the public record and is not open to inspection by the public, even upon request.

2. The Personal Information Was Encrypted

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.[37]

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 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 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.

---

35 ALASKA STAT. § 45.48.010(c); VT. STAT. ANN. tit. 9, § 2435(d).

36 FLA. STAT. § 501.171(4)(c).

37 *See* ALASKA STAT. § 45.48.090(7); ARIZ. REV. STAT. § 44-7501(L)(1); ARK. CODE ANN. § 4-110-103(7); CAL. CIV. CODE § 1798.82(a); COLO. REV. STAT. § 6-1-716(1)(a); 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(a)(b)(2); IOWA CODE § 715C.1(11); KAN. STAT. ANN. § 50-7a01(b), (g)-(h); KY. REV. STAT. ANN. § 365.732(1)(a); LA. REV. STAT. ANN. § 51:3073(4); ME. REV. STAT. ANN. tit. 10, § 1347(6); MD. CODE ANN., COM. LAW § 14-3501(d); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.72(1); MINN. STAT. § 325E.61(1)(a); 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.Y. GEN. BUS. LAW § 899-aa(1)(b)-(c); 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); 73 PA. CONS. STAT. § 2302; P.R. LAWS ANN. tit. 10, § 4051(a); R.I. GEN. LAWS § 11-49.3-3(a)(1), (8); S.C. CODE ANN. § 39-1-90(A), (D); 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(3); VT. STAT. ANN. tit. 9, § 2430(5); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(1); W. VA. CODE § 46A-2A-101(1), (6); WIS. STAT. § 134.98(1)(b); WYO. STAT. ANN. § 40-12-501(a)(vii).

Notably, Tennessee recently amended its breach notification laws, effective July 1, 2016 (and again in 2017), and now mandates that if a "breach" of computerized personal information has occurred, notice must be made *regardless* of whether the information was encrypted. Though this represents a dramatic divergence from the way other states treat encrypted data, it is debatable whether this change will have any significant practical impact on how an organization moves forward with notice. As Tennessee law defines a noticeable breach as the unauthorized acquisition of computerized data that "materially compromises the security, confidentiality, or integrity of the personal information"[38] maintained by the organization, the organization may find that given the encryption utilized, there is no reasonable likelihood that the security, confidentiality, or integrity of the computerized data was materially compromised, and thus, no notice is required.

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

Almost all states and the D.C. have an exception for the "good faith" access to, or acquisition of, personal information by employees or agents of the organization.[39] Generally, under this exception, facts that 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" 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.

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

---

38 TENN. CODE ANN. § 47-18-2107(1).

39 *See* ALASKA STAT. § 45.48.050; ARIZ. REV. STAT. § 44-7501(L)(1); ARK. CODE ANN. § 4-110-103(1)(B); CAL. CIV. CODE § 1798.82(g); COLO. REV. STAT. § 6-1-716(1)(a); 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(a)(b)(1); IOWA CODE § 715C.1(1); KAN. STAT. ANN. § 50-7a01(h); KY. REV. STAT. ANN. § 365.732(1)(a); LA. REV. 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.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); 73 PA. CONS. STAT. § 2302; P.R. LAWS ANN. tit. 10, § 4051(c); R.I. GEN. LAWS § 11-49.3-3(a)(1); S.C. CODE ANN. § 39-1-90(D)(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 § 19.255.010(4); W. VA. CODE § 46A-2A-101(1); WIS. STAT. § 134.98(2)(cm); WYO. STAT. ANN. § 40-12-501(a)(i).

a specific period of time (e.g., thirty 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 which 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. 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 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.[40]

- 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.

---

[40] A contacts 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.

With regard to organizations that are not specially regulated, the following twenty-five U.S. states and territories have laws with requirements regarding notification to regulators: California, Connecticut, Florida, Hawaii, Indiana, Iowa, Louisiana, Maine, Maryland, Massachusetts, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Oregon, Rhode Island, South Carolina, Vermont, Virginia, Washington, and Puerto Rico[41] (*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, fifteen require notice to the relevant regulator *regardless* of how many residents have been impacted by the breach[42] (*see* Table VI.C.1(A): U.S. Jurisdictions Requiring Notice to Regulators). The other ten, 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.[43]

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

U.S. Jurisdiction	Minimum Threshold Required	To Whom Regulator Notice Must Be Made
California[44]	500+ residents	Office of the Attorney General
Connecticut[45]	No minimum/1+ resident	Office of the Attorney General

41 CAL. CIV. CODE § 1798.82(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(c); 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; R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(K); VT. STAT. ANN. tit. 9, § 2435(b)(3); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(15).

42 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(c); N.Y. GEN. BUS. LAW § 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); VA. CODE ANN. § 18.2-186.6(B).

43 CAL. CIV. CODE § 1798.82(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); R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(K); WASH. REV. CODE § 19.255.010(15).

44 CAL. CIV. CODE § 1798.82(f).

45 CONN. GEN. STAT. § 36a-701b(b)(2).

U.S. Jurisdiction	Minimum Threshold Required	To Whom Regulator Notice Must Be Made
Florida[46]	500+ residents	Department of Legal Affairs of the Office of Attorney General
Hawaii[47]	1,000+ residents	Office of Consumer Protection
Indiana[48]	No minimum/1+ resident	Office of the Attorney General
Iowa[49]	500+ residents	Director of the Consumer Protection Division of the Iowa Office of Attorney General
Louisiana[50]	No minimum/1+ resident	Consumer Protection Section of the Louisiana Office of the Attorney General
Maine[51]	No minimum/1+ resident	Office of the Attorney General
Maryland[52]	No minimum/1+ resident	Office of the Attorney General
Massachusetts[53]	No minimum/1+ resident	Office of the Attorney General Director of Consumer Affairs and Business Regulation
Missouri[54]	1,000+ residents	Office of the Attorney General
Montana[55]	No minimum/1+ resident	Consumer Protection Division of the Montana Office of the Attorney General
Nebraska[56]	No minimum/1+ resident	Office of the Attorney General
New Hampshire[57]	No minimum/1+ resident	Office of the Attorney General
New Jersey[58]	No minimum/1+ resident	Division of State Police in the Department of Law and Public Safety of the State of New Jersey

46 FLA. STAT. § 501.171(3)(a).

47 HAW. REV. STAT. § 487N-2(f).

48 IND. CODE § 24-4.9-3-1(c).

49 IOWA CODE § 715C.2(8).

50 LA. ADMIN. CODE tit. 16, § 701.A.

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

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

53 MASS. GEN. LAWS ch. 93H, § 3(b).

54 MO. ANN. STAT. § 407.1500(2)(8).

55 MONT. CODE ANN. § 30-14-1704(8).

56 NEB. REV. STAT. § 87-803(2).

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

58 N.J. STAT. ANN. § 56:8-163(c).

U.S. Jurisdiction	Minimum Threshold Required	To Whom Regulator Notice Must Be Made
New York[59]	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[60]	No minimum/1+ resident	Consumer Protection Division of the Office of the Attorney General
North Dakota[61]	250+ residents	Office of the Attorney General
Oregon[62]	250+ residents	Oregon Attorney General's Office
Puerto Rico[63]	No minimum/1+ resident	Department of Consumer Affairs for Puerto Rico
Rhode Island[64]	500+ residents	Office of the Attorney General
South Carolina[65]	1,000+ residents	Consumer Protection Division of the Department of Consumer Affairs for South Carolina
Vermont[66]	No minimum/1+ resident	Office of the Attorney General
Virginia[67]	No minimum/1+ resident	Office of the Attorney General
Washington[68]	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 minimum content requirements for these regulator notices. Indeed, Iowa, Rhode Island, and Puerto Rico are the only U.S. states or territories (of the twenty-five that require notice to regulators) that do *not* specify what the organization's notice to the relevant regulator should contain in terms of content.[69] 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.

---

59 N.Y. GEN. BUS. LAW § 899-aa(8)(a).

60 N.C. GEN. STAT. § 75-65(e1).

61 N.D. CENT. CODE § 51-30-02.

62 OR. REV. STAT. § 646A.604(1)(b).

63 P.R. LAWS ANN. tit. 10, § 4052.

64 R.I. GEN. LAWS § 11-49.3-4(a)(2).

65 S.C. CODE ANN. § 39-1-90(K).

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

67 VA. CODE ANN. § 18.2-186.6(B).

68 WASH. REV. CODE § 19.255.010(15).

69 IOWA CODE § 715C.2(8); P.R. LAWS ANN. tit. 10, § 4052; R.I. GEN. LAWS § 11-49.3-4(a)(2).

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 which 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.[70] 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.[71] 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 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.[72]

- 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: Alaska, Colorado, Florida, Georgia,[73] Hawaii, Indiana, Kansas, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nevada, New Hampshire, New Jersey, New York, North Carolina,

---

70 N.J. STATE POLICE, CYBER CRIMES UNIT, http://www.njsp.org/division/investigations/cyber-crimes.shtml (last visited Dec. 13, 2017).

71 N.C. GEN. STAT. § 75-65(e1).

72 *See* N.C. DEP'T OF JUSTICE AND N.C. ATTORNEY GEN. JOSH STEIN, REPORT A SECURITY BREACH, http://www.ncdoj.gov/getdoc/81eda50e-8feb-4764-adca-b5c47f211612/Report-a-Security-Breach.aspx (last visited Dec. 13, 2017).

73 Importantly, Georgia's data breach notification laws pertain only to entities who qualify as "data collectors" or "information brokers," as defined by the statute; these are generally entities that, for a fee, are in the business of collecting, aggregating, and analyzing personal information for third parties. GA. CODE ANN. § 10-1-912(a).

Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Vermont, Virginia, West Virginia, and Wisconsin.[74]

With the exception of Massachusetts, 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 impacted residents to 10,000 or more impacted residents 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.[75]

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

U.S. Jurisdictions	Minimum Threshold Required
Minnesota, Rhode Island[76]	500+ residents
Alaska, Colorado, D.C., Florida, Hawaii, Indiana, Kansas, Kentucky, Maine, Maryland, Michigan, Missouri, Nevada, New Hampshire, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, Tennessee, Vermont, Virginia, West Virginia, Wisconsin[77]	1,000+ residents

---

74 ALASKA STAT. § 45.48.040(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); 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(f); 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; R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(K); 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).

75 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.

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

77 ALASKA STAT. § 45.48.040(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.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).

U.S. Jurisdictions	Minimum Threshold Required
New York[78]	5,000+ residents
Georgia, Texas[79]	10,000+ residents
Massachusetts[80]	No minimum—*only if so directed* by Director of Consumer Affairs and Business Regulation

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."[81] 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.[82] Further, in providing notice to these agencies, state regulations make clear that the organization should not provide the agencies with the names or other PII of the breach notice recipients.

2. Timing of Notice

When investigating 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.

---

78 N.Y. GEN. BUS. LAW § 899-aa(8)(b).

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

80 MASS. GEN. LAWS ch. 93H, § 3(b).

81 ALASKA STAT. § 45.48.040(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(f); 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; R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(K); 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).

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

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."

Only twelve states and D.C. start the notification clock when the organization first discovers or is first notified of the breach. The states joining D.C. include: Alaska, Florida, Hawaii, Illinois, Indiana, Iowa, Massachusetts, Michigan, Missouri, North Carolina, Oregon, and Vermont.[83] Generally, those laws provide that notice shall be provided to the impacted individuals *after* "discovering or being notified of the breach"[84] or, alternatively, *after* the organization "knows or has reason to know of a breach of security."[85]

The remaining U.S. states and territories, either implicitly or 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 and territories include: Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Idaho, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Dakota, Ohio, Oklahoma, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.[86] The key here is the

---

83 ALASKA STAT. § 45.48.010(a); D.C. CODE § 28-3852(a); FLA. STAT. § 501.171(3); HAW. REV. STAT. § 487N-2(a); 815 ILL. COMP. STAT. 530/10(a); IND. CODE ANN. § 24-4.9-3-1(a); IOWA CODE § 715C.2(1); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS ANN. § 445.72(1); MO. ANN. STAT. § 407.1500(2)(1); N.C. GEN. STAT. § 75-65(a); OR. REV. STAT. § 646A.604(1)(a); VT. STAT. ANN. tit. 9, § 2435(b)(1).

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

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

86 ARIZ. REV. STAT. § 44-7501(A) (explicitly); ARK. CODE ANN. § 4-110-105(a)(1) (by implication); CAL. CIV. CODE § 1798.82(a); COLO. REV. STAT. § 6-1-716(2)(a) (explicitly); CONN. GEN. STAT. § 36a-701b(b)(1) (by implication); DEL. CODE ANN. tit. 6, § 12B-102(a) (explicitly); GA. CODE ANN. § 10-1-912(a) (by implication); IDAHO CODE § 28-

point in time when the investigation finally reveals that personal information belonging to residents 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.	Alaska, D.C., Florida, Hawaii, Illinois, Indiana, Iowa, Massachusetts, Michigan, Missouri, North Carolina, Oregon, and Vermont[87]
The notification clock is triggered after completion of a reasonable and prompt investigation to determine whether, in fact, a "breach" has occurred.	Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Dakota, Ohio, Oklahoma, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming[88]

51-105(1) (explicitly); KAN. STAT. ANN. § 50-7a02(a) (explicitly); KY. REV. STAT. ANN. § 365.732(2) (by implication); LA. REV. STAT. ANN. § 51:3074(A) (by implication); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B) (explicitly); MD. CODE ANN., COM. LAW § 14-3504(b)(1)-(2) (explicitly); MINN. STAT. § 325E.61(1) (by implication); MISS. CODE ANN. § 75-24-29(3) (explicitly); MONT. CODE ANN. § 30-14-1704(1) (by implication); NEB. REV. STAT. § 87-803(1); NEV. REV. STAT. ANN. § 603A.220(1) (by implication); N.H. REV. STAT. ANN. § 359-C:20(I)(a) (explicitly); N.J. STAT. ANN. § 56:8-163(a) (by implication); N.Y. GEN. BUS. LAW § 899-aa(2) (by implication); N.D. CENT. CODE § 51-30-02 (by implication); OHIO REV. CODE ANN. § 1349.19(B) (by implication); OKLA. STAT. tit. 24, § 163(A) (by implication); 73 PA. CONS. STAT. § 2303(a) (by implication); P.R. LAWS ANN. tit. 10, § 4052 (by implication); R.I. GEN. LAWS § 11-49.3-4(a)(2) (by implication); S.C. CODE ANN. § 39-1-90(A) (by implication); TENN. CODE ANN. § 47-18-2107(b) (by implication); TEX. BUS. & COM. CODE ANN. § 521.053(b) (by implication); UTAH CODE ANN. § 13-44-202(1)(a) (explicitly); VA. CODE ANN. § 18.2-186.6(B) (by implication); WASH. REV. CODE § 19.255.010(1) (by implication); W. VA. CODE § 46A-2A-102(a); WIS. STAT. § 134.98(2); WYO. STAT. ANN. § 40-12-502(a) (explicitly).

87 ALASKA STAT. § 45.48.010(a); D.C. CODE § 28-3852(a); FLA. STAT. § 501.171(3) (notice to Department of Legal Affairs; notice to individuals is covered by a different standard as noted below); HAW. REV. STAT. § 487N-2(a); 815 ILL. COMP. STAT. 530/10(a); IND. CODE ANN. § 24-4.9-3-1(a); IOWA CODE § 715C.2(1); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS ANN. § 445.72(1); MO. ANN. STAT. § 407.1500(2)(1); N.C. GEN. STAT. § 75-65(a); OR. REV. STAT. § 646A.604(1)(a); VT. STAT. ANN. tit. 9, § 2435(b)(1).

88 ARIZ. REV. STAT. § 44-7501(A) (explicitly); ARK. CODE ANN. § 4-110-105(a)(1) (by implication); CAL. CIV. CODE § 1798.82(a) (by implication); COLO. REV. STAT. § 6-1-716(2)(a) (explicitly); CONN. GEN. STAT. § 36a-701b(b)(1) (by implication); DEL. CODE ANN. tit. 6, § 12B-102(a) (explicitly); FLA. STAT. § 501.171(4) (by implication); GA. CODE ANN. § 10-1-912(a) (by implication); IDAHO CODE § 28-51-105(1) (explicitly); KAN. STAT. ANN. § 50-7a02(a) (explicitly); KY. REV. STAT. ANN. § 365.732(2) (by implication); LA. REV. STAT. ANN. § 51:3074(A) (by implication); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B) (explicitly); MD. CODE ANN., COM. LAW § 14-3504(b)(1)-(2) (explicitly); MINN. STAT. § 325E.61(1) (by implication); MISS. CODE ANN. § 75-24-29(3) (explicitly); MONT. CODE ANN. § 30-14-1704(1) (by implication); NEB. REV. STAT. § 87-803(1); NEV. REV. STAT. ANN. § 603A.220(1) (by implication);

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

  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 expeditious time possible*" and "*without unreasonable delay*."[89] In addition to D.C., U.S. states and territories providing only this vague timing expectation include: Alaska, Arizona, Arkansas, California, Colorado, Delaware, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Oklahoma, Oregon, Pennsylvania, Puerto Rico, South Carolina, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming.[90] 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.

N.H. REV. STAT. ANN. § 359-C:20(I)(a) (explicitly); N.J. STAT. ANN. § 56:8-163(a) (by implication); N.Y. GEN. BUS. LAW § 899-aa(2) (by implication); N.D. CENT. CODE § 51-30-02 (by implication); OHIO REV. CODE ANN. § 1349.19(B) (by implication); OKLA. STAT. tit. 24, § 163(A) (by implication); 73 PA. CONS. STAT. § 2303(a) (by implication); P.R. LAWS ANN. tit. 10, § 4052 (by implication); R.I. GEN. LAWS § 11-49.3-4(a)(2) (by implication); S.C. CODE ANN. § 39-1-90(A) (by implication); TENN. CODE ANN. § 47-18-2107(b) (by implication); TEX. BUS. & COM. CODE ANN. § 521.053(b) (by implication); UTAH CODE ANN. § 13-44-202(1)(a) (explicitly); VA. CODE ANN. § 18.2-186.6(B) (by implication); WASH. REV. CODE § 19.255.010(1) (by implication); W. VA. CODE § 46A-2A-102(a); WIS. STAT. § 134.98(2); WYO. STAT. ANN. § 40-12-502(a) (explicitly).

89 *See, e.g.*, ALASKA STAT. § 45.48.010(b).

90 *Id.*; ARIZ. REV. STAT. § 44-7501(A); ARK. CODE ANN. § 4-110-105(a)(2); CAL. CIV. CODE § 1798.82(a); COLO. REV. STAT. § 6-1-716(2)(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); IND. CODE § 24-4.9-3-1(a); IOWA CODE § 715C.2(1); KAN. STAT. ANN. § 50-7a02(a); KY. REV. STAT. ANN. § 365.732(2); LA. REV. STAT. ANN. § 51:3074(C); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MD. CODE ANN., COM. LAW § 14-3504(b)(3); 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(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); OR. REV. STAT. § 646A.604(1)(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); WASH. REV. CODE § 19.255.010(16); W. VA. CODE § 46A-2A-102(a)-(b); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

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

Interestingly, for all the talk of timing, only seven states specify a time period during which notice to impacted individuals must be made. These states include: Connecticut (ninety days), Florida (thirty days), Ohio (forty-five days), Rhode Island (forty-five days), Tennessee (forty-five days), Vermont (forty-five 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 days after* the discovery of such breach unless a shorter time is required under federal law."[91] In Ohio, Rhode Island, Tennessee, and Wisconsin, notice to the impacted individual(s) must be made in the most expedient time possible "*but not later than forty-five days following* [the organization's] discovery or notification of the breach."[92] In Florida, notice to impacted individuals must be made as expeditiously as practicable and without unreasonable delay "*but no later than 30 days after* the determination of a breach."[93] In each of these states, the time period stipulated for notification 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. Careful analysis will be required to determine when attorneys general should be notified essentially contemporaneously with notice to impacted individuals, which can vary by state.

---

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

92 OHIO REV. CODE ANN. § 1349.19(B)(2); R.I. GEN. LAWS § 11-49.3-4(a)(2); TENN. CODE ANN. § 47-18-2107(b); WIS. STAT. § 134.98(3). Emphasis added.

93 FLA. STAT. § 501.171(4)(a) (emphasis added).

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

Notice must be made "*in the most expeditious time possible*" and "*without undue delay*."	Alaska, Arizona, Arkansas, California, Colorado, Delaware, D.C., Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Oklahoma, Oregon, Pennsylvania, Puerto Rico, South Carolina, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming[94]
Notice must be made without unreasonable delay "*but no later than **90 days** after* the discovery of the breach unless a shorter time is required under federal law."	Connecticut[95]
Notice must be made in the most expedient time possible "*but not later than **45 days** after the* discovery or notification of the breach."	Ohio, 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[96]
Notice must be made as expeditiously as practicable and without unreasonable delay "*but no later than **30 days** after* the determination of a breach."	Florida[97]

94 ALASKA STAT. § 45.48.010(b); ARIZ. REV. STAT. § 44-7501(A); ARK. CODE ANN. § 4-110-105(a)(2); CAL. CIV. CODE § 1798.82(a); COLO. REV. STAT. § 6-1-716(2)(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); IND. CODE § 24-4.9-3-1(a); IOWA CODE § 715C.2(1); KAN. STAT. ANN. § 50-7a02(a); KY. REV. STAT. ANN. § 365.732(2); LA. REV. STAT. ANN. § 51:3074(C); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MD. CODE ANN., COM. LAW § 14-3504(b)(3); 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(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); OR. REV. STAT. § 646A.604(1)(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); WASH. REV. CODE § 19.255.010(16); W. VA. CODE § 46A-2A-102(a)-(b); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

95 CONN. GEN. STAT. § 36a-701b(b)(1).

96 OHIO REV. CODE ANN. § 1349.19(B)(2); 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).

97 FLA. STAT. § 501.171(4)(a).

Notice must be made in the most expedient time possible "*but no later than **14 days*** after the discovery or notification of the breach."	Vermont[98]

- 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 two states, Maryland and New Jersey, notice to the relevant state regulators, if required, must always be made *prior to* the organization's notice to impacted individuals.[99] Vermont required notice to the Attorney General *prior to* notice to impacted individuals if the data collector has filed a sworn submission with the Attorney General as explained in Table VI.C.2(B) above and is therefore governed by the 45 rather than the 14-day notice period.[100] In Florida, Iowa, Louisiana, and Vermont, notice must be made within a specified time after either the determination of the breach or the notice to impacted individuals.[101]

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

Notice *Prior to* Notice to Individuals	Maryland[102] New Jersey Vermont Attorney General or Department of Financial Regulation (only if the 45-day notification period applies)[103]
As expeditiously as practicable, but no later than 30 days *after* the determination of the breach or reason to believe a breach occurred	Florida[104] (Department of Legal Affairs)
Within five business days after giving notice of the breach of security to any consumer	Iowa (Department of Consumer Protection Division)[105]

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

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

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

101 FLA. STAT. § 501.171(4)(a); IOWA CODE § 715C.2(8); LA. ADMIN. CODE tit. 16, § 701(B); VT. STAT. ANN. tit. 9, § 2435(b)(3).

102 MD. CODE ANN., COM. LAW § 14-3504(h); N.J. Stat. Ann. § 56:8-163(c).

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

104 FLA. STAT. § 501.171(4)(a).

105 IOWA CODE § 715C.2(8).

Within 10 days of distribution of notice to residents	Louisiana (Consumer Protection Section)[106]
Within 14 business days of "discovery of the security breach or when the data collector provides notice to consumers," whichever is sooner	Vermont Department of Financial Regulation[107]

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

  With the exception of Minnesota, 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." Minnesota, on the other hand, requires notice to be made to the credit reporting agencies within 48 hours of when a "person discovers circumstances requiring notification" for breaches involving more than 500 residents.[108] Arguably, Minnesota's unusual phrasing could be read to require notifications to credit reporting agencies within 48 hours after the breach is first discovered, well in advance of any required notice to impacted residents.[109]

- Delay of notice due to law enforcement

  Across all U.S. jurisdictions, regardless of whether their data breach notification laws contain vague or very specific timing requirements, 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 Connecticut, Delaware, Florida, Hawaii, Mississippi, New Jersey, North Carolina, Vermont, and Wisconsin, as noted in the table below. In other jurisdictions, however, delaying notification after law enforcement has 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 York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, West Virginia,

---

106 LA. ADMIN. CODE tit. 16, § 701(B).

107 VT. STAT. ANN. tit. 9, § 2435(b)(3)(A) for those entities regulated by that Department.

108 MINN. STAT. § 325E.61(2).

109 *Id.*

Wisconsin, and Wyoming.[110] In fact, there may be some very good practical, non-legal reasons *not* to delay notification and, therefore, the organization will want to strategically consider whether to delay notification when it is optional.

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.	Connecticut, Delaware, Florida, Hawaii, Mississippi, New Jersey, North Carolina, Vermont, Wisconsin[111]
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 York, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming[112]

110 ALASKA STAT. § 45.48.020; ARIZ. REV. STAT. § 44-7501(C); 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); IOWA CODE § 715C.2(3)); KAN. STAT. ANN. § 50-7a02(c); KY. REV. STAT. ANN. § 365.732(4); LA. REV. STAT. ANN. § 51:3074(D); ME. REV. STAT. ANN. tit. 10, § 1348(3); MD. CODE ANN., COM. LAW § 14-3504(d); 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(3); NEV. REV. STAT. ANN. § 603A.220(3); N.H. REV. STAT. ANN. § 359-C:20(II); N.Y. GEN. BUS. LAW § 899-aa(4); N.C. GEN. STAT. § 75-65(c); 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); 73 PA. CONS. STAT. § 2304; R.I. GEN. LAWS § 11-49.3-4(b); S.C. CODE ANN. § 39-1-90(C); 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).

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

112 ALASKA STAT. § 45.48.020; ARIZ. REV. STAT. § 44-7501(C); ARK. CODE ANN. § 4-110-105(c); CAL. CIV. CODE § 1798.82(c); COLO. REV. STAT. § 6-1-716(2)(c); DEL. CODE ANN. tit. 6, § 12B-102(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); IOWA CODE § 715C.2(3); KAN. STAT. ANN. § 50-7a02(c); KY. REV. STAT. ANN. § 365.732(4); LA. REV. STAT. ANN. § 51:3074(D); ME. REV. STAT. ANN. tit. 10, § 1348(3); MD. CODE ANN., COM. LAW § 14-3504(d); 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(3); NEV. REV. STAT. ANN. § 603A.220(3); N.H. REV. STAT. ANN. § 359-C:20(II); N.Y. GEN. BUS. LAW § 899-aa(4); N.C. GEN. STAT. § 75-65(c); 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); 73 PA. CONS. STAT. § 2304; R.I. GEN. LAWS § 11-49.3-4(b); S.C. CODE ANN. § 39-1-90(C); 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.

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.

- 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 (4) via "substitute" notice. Not just one method need be employed; the facts and circumstances of a particular data breach may necessitate the use of one or more of the above methods.

- Letter Notice

  Every 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 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 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 pre-existing business relationship with the impacted individual(s);[113] (2) if the impacted individual(s) has expressly consented to receive electronic notices under the Electronic Signatures in Global and National Commerce Act, codified

§ 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).

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

at 15 U.S.C. §§ 7001–7031 ("ESIGN"),[114] or otherwise expressed consent to receive such notices;[115] (3) if the organization primarily conducts its business through Internet account transactions or on the Internet generally;[116] 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).[117] 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, Nebraska does not permit electronic-only notice under any circumstances; New York allows it if the customer has consented, but not if consent was required as a condition to doing business electronically.[118]

---

[114] 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.

[115] ALASKA STAT. § 45.48.030(2); ARIZ. REV. STAT. § 44-7501(D)(2); ARK. CODE ANN. § 4-110-105(e)(2); CAL. CIV. CODE § 1798.82(j)(2); COLO. REV. STAT. § 6-1-716(1)(c)(III); CONN. GEN. STAT. § 36a-701b(e)(3); DEL. CODE ANN. tit. 6, § 12B-101(3)(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. REV. STAT. ANN. § 51:3074(E)(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(d); 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); R.I. GEN. LAWS § 11-49.3-3(c)(ii); S.C. CODE ANN. § 39-1-90(E)(2); TENN. CODE ANN. § 47-18-2107(e)(2); TEX. BUS. & COM. CODE ANN. § 521.053(e)(2); UTAH CODE ANN. § 13-44-202(5)(ii); VT. STAT. ANN. tit. 9, § 2435(b)(6)(A)(ii); WASH. REV. CODE § 19.255.010(8)(b); W. VA. CODE § 46A-2A-101(7)(C).

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

[117] ALASKA STAT. § 45.48.030(2); ARIZ. REV. STAT. § 44-7501(D)(2); COLO. REV. STAT. § 6-1-716(1)(c)(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); UTAH CODE ANN. § 13-44-202(5)(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).

[118] The following states and D.C. 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

  Telephonic notice 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.[119] Depending on the state, however, certain criteria may have to be satisfied to permit telephonic notice, such as keeping a log of the call,[120] speaking directly with the impacted individual (i.e., not simply leaving a voicemail),[121] or notifying by telephone only if the organization has previously communicated with the impacted individual by telephone.[122]

- 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.[123] The requirements for

---

119 ARIZ. REV. STAT. § 44-7501(D)(3); COLO. REV. STAT. § 6-1-716(1)(c)(II); CONN. GEN. STAT. § 36a-701b(e)(2); DEL. CODE ANN. tit. 6, § 12B-101(3)(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)(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).

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

121 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).

122 WIS. STAT. § 134.98(3)(b).

123 ALASKA STAT. § 45.48.030(3); ARIZ. REV. STAT. § 44-7501(D)(4); ARK. CODE ANN. § 4-110-105(e)(3)(B); CAL. CIV. CODE § 1798.82(j)(3); COLO. REV. STAT. § 6-1-716(1)(c)(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-

substitute 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 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 in excess of $5,000 to $250,000); and/or (3) the organization does not have sufficient contact information for impacted individuals to notify them directly.[124] Utah is the only exception to this rule. In contrast with other jurisdictions, Utah's data breach notification law contains no prerequisites for the use of substitute notice. Instead, in Utah, substitute notification is permissible regardless of cost or number of individuals impacted, and requires only publication of the notice "in a newspaper of general circulation" *and* publication of the notice to https://www.utahlegals.com/, a state-sponsored website utilized exclusively for posting public notices of all types.[125]

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. REV. STAT. ANN. § 51:3074(E)(3); ME. REV. STAT. ANN. tit. 10, § 1347(4)(C); MD. CODE ANN., COM. LAW § 14-3504(e)(4); 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)(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(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); R.I. GEN. LAWS § 11-49.3-3(c)(iii); S.C. CODE ANN. § 39-1-90(E)(4); TENN. CODE ANN. § 47-18-2107(e)(3); TEX. BUS. & COM. CODE ANN. § 521.053(f); UTAH CODE ANN. § 13-44-202(5)(iv); VT. STAT. ANN. tit. 9, § 2435(b)(6)(B); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(8)(c); W. VA. CODE § 46A-2A-101(7)(D); WYO. STAT. ANN. § 40-12-502(d)(iii).

124 ALASKA STAT. § 45.48.030(3); ARIZ. REV. STAT. § 44-7501(D)(4); ARK. CODE ANN. § 4-110-105(e)(3)(A)(iii); CAL. CIV. CODE § 1798.82(j)(3); COLO. REV. STAT. § 6-1-716(1)(c)(IV); CONN. GEN. STAT. § 36a-701b(e)(4); DEL. CODE ANN. tit. 6, § 12B-101(3)(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. REV. STAT. ANN. § 51:3074(E)(3); ME. REV. STAT. ANN. tit. 10, § 1347(4)(C); MD. CODE ANN., COM. LAW § 14-3504(e)(4); 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)(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(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); R.I. GEN. LAWS § 11-49.3-3(c)(iii); S.C. CODE ANN. § 39-1-90(E)(4); TENN. CODE ANN. § 47-18-2107(e)(3); TEX. BUS. & COM. CODE ANN. § 521.053(f); VT. STAT. ANN. tit. 9, § 2435(b)(6)(B); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(8)(c); W. VA. CODE § 46A-2A-101(7)(D); WYO. STAT. ANN. § 40-12-502(d)(iii).

125 UTAH CODE ANN. §§ 13-44-202(5)(iv), 45-1-101(2).

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, Arizona, Arkansas, Colorado, 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, Tennessee, Texas, and Utah. However, while not required, 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: California, Florida, Hawaii, Illinois, Iowa, Maryland, Massachusetts, Michigan, Missouri, New Hampshire, New York, North Carolina, Oregon, Puerto Rico, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.[126]

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 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.[127]

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

---

126 CAL. CIV. CODE § 1798.82(d); 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.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(14); W. VA. CODE § 46A-2A-102(d); WIS. STAT. § 134.98(2)(a); WYO. STAT. ANN. § 40-12-502(e).

127 CAL. CIV. CODE § 1798.82(k).

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.

Finally, California, Hawaii, Michigan, North Carolina, Puerto Rico, Vermont, and Washington require that the notice be clear and conspicuous and crafted using plain language.[128] 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, Arizona, Arkansas, Colorado, 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, Tennessee, Texas, and Utah
A general description of the incident	California, Hawaii, Iowa, Michigan, Missouri, New Hampshire, North Carolina, Oregon, Puerto Rico, Vermont, Virginia, Wyoming[129]
Date of the breach (or estimated date or date range within which the breach occurred)	California, Florida, Iowa, New Hampshire, Oregon, Vermont, Wyoming[130]

128 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(14)(a).

129 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.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); WYO. STAT. ANN. § 40-12-502(e).

130 CAL. CIV. CODE § 1798.82(d); FLA. STAT. § 501.171(4)(e)(1); IOWA CODE § 715C.2(5); N.H. REV. STAT. ANN. § 359-C:20(IV); OR. REV. STAT. § 646A.604(5); VT. STAT. ANN. tit. 9, § 2435(b)(5); WYO. STAT. ANN. § 40-12-502(e).

Content Required	U.S. Jurisdiction
Categories of personal information reasonably believed to have been breached (e.g., username, password, date of birth, social security number)	California, Florida, Hawaii, Iowa, Maryland, Michigan, Missouri, New York, North Carolina, Oregon, Puerto Rico, Vermont, Virginia, Washington, West Virginia, Wyoming[131]
Whether notice was delayed as a result of a law enforcement investigation	California, Wyoming[132]
The steps the organization has taken to protect impacted individuals and their personal information from further unauthorized access or acquisition	California, Hawaii, Michigan, North Carolina, Vermont, Virginia, Wyoming[133]
Advice regarding additional steps the impacted individuals can take to further protect themselves and their personal information	California, Hawaii, Illinois, Iowa, Maryland, Massachusetts, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, Wyoming[134]
Contact information for the organization reporting the breach	California, Florida, Hawaii, Maryland, Michigan, Missouri, New Hampshire, New York, North Carolina, Oregon, Puerto Rico, Vermont, Virginia, Washington, West Virginia, Wyoming[135]
Toll-free numbers and addresses of the three major credit reporting agencies and/or FTC	California, Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, Washington, West Virginia, Wyoming[136]

131 CAL. CIV. CODE § 1798.82(d); 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.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(14)(b); W. VA. CODE § 46A-2A-102(d); WYO. STAT. ANN. § 40-12-502(e).

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

133 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).

134 CAL. CIV. CODE § 1798.82(d); 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.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5); VT. STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A); WYO. STAT. ANN. § 40-12-502(e).

135 CAL. CIV. CODE § 1798.82(d); 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.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(14)(b); W. VA. CODE § 46A-2A-102(d); WYO. STAT. ANN. § 40-12-502(e).

136 CAL. CIV. CODE § 1798.82(d); 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.C. GEN. STAT. § 75-65(d); OR. REV. STAT.

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 "For More Information."[137] 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).[138] 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).[139] 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 months.[140] Though not included in the statute, Connecticut now requires organizations to provide twenty-four months of free credit monitoring.[141]

§ 646A.604(5); WASH. REV. CODE § 19.255.010(14)(b); W. VA. CODE § 46A-2A-102(d); WYO. STAT. ANN. § 40-12-502(e).

137 CAL. CIV. CODE § 1798.82(d).

138 N.C. GEN. STAT. § 75-63(p).

139 MASS. GEN. LAWS ch. 93H, § 3(b).

140 *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.

141 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 depends 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 timely activated?
- 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 also re-examine 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 this 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

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").

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.

III. Incident Response Team (IRT) 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*]

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.[142]
- 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.

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:

---

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

- **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 non-critical 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

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 restrict 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 re-imaged to a clean and uncompromised state.

VII. Reporting

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

VIII. Enforcement

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

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

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 1-888-685-1111 (general) 1-888-766-0008 (fraud alert) 1-800-685-1111 (security freeze) www.freeze.equifax.com	P.O. Box 2104 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze	P.O. Box 2000 Chester, PA 19022 1-800-888-4213 (general) 1-800-680-7289 (identity theft and fraud) 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, 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

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.

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 1-888-685-1111 (general) 1-888-766-0008 (fraud alert) 1-800-685-1111 (security freeze) www.freeze.equifax.com	P.O. Box 2104 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze	P.O. Box 2000 Chester, PA 19022 1-800-888-4213 (general) 1-800-680-7289 (identity theft and fraud) 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

[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

[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 F:
GLBA AND HIPAA

I. Special Requirements in the United States:

A. Gramm-Leach-Bliley Act (GLBA)[143]

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;
   - 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);

---

[143] GLBA 15 U.S.C. § 6801 *et. seq.*

- 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 12 to 24 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)[144]/Health Information Technology for Economic and Clinical Health (HITECH) Act[145]

1. Notification obligations triggered following breach

   - Breach presumed when there is an impermissible use or disclosure of Personal Health Information (PHI) unless risk assessment demonstrates low probability that PHI has been compromised

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 60 days following the discovery of a breach

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.

---

144 HIPAA 42 U.S.C. § 1320d *et. seq.*

145 HITECH 42 U.S.C. § 17931 *et. seq.*