DATA SECURITY BREACH HANDBOOK

2019 EDITION

Jena Valdetero
David Zetoony
Bryan Cave Leighton Paisner LLP

TABLE OF CONTENTS

Page

ABOUT THE AUTHORS ii

INTRODUCTION 1

I. UNDERSTANDING THE NATURE AND SCOPE OF DATA EVENTS, INCIDENTS, AND BREACHES 4

A. Security Events 5
B. Security Incidents 5
C. Security Breaches 6

II. DATA SECURITY INCIDENT PREPAREDNESS 9

A. Cyber Insurance 11
B. Written Information Security Program 17
C. Incident Response Plan 20
D. Contractual Obligations to Business Partners 23

III. INCIDENT RESPONSE 24

A. Investigating a Security Incident 25
B. Coordination with Data Owners 29
C. Communication to the Public/Media 30
D. Communication with Law Enforcement 34
E. Communication with Impacted Consumers in the United States 35
F. Communications with Supervisory Authorities and Individuals in the European Union 48
G. Breaches Outside the US or EU 51
H. Unique Issues Relating To Payment Card Breaches 51

CONCLUSION 53

ABOUT THE AUTHORS

Jena Valdetero is a partner at Bryan Cave Leighton Paisner LLP where she serves as the head of the firm's Data Breach Response Team. She has provided counseling to clients on thousands of data privacy and security issues, with a specific focus on breach preparation and response. She is a Certified Information Privacy Professional, U.S. (CIPP/US), by the leading privacy trade organization, the International Association of Privacy Professionals, for which she served as a KnowledgeNet Co-Chair for the Chicago area. In addition to her privacy practice, Ms. Valdetero handles litigation matters on behalf of a variety of clients, including class action litigation, in both state and federal courts.

David Zetoony is a partner at Bryan Cave Leighton Paisner LLP and the leader of the firm's international data privacy and security practice. Mr. Zetoony has helped hundreds of clients respond to data security incidents, and, where necessary, has defended inquiries concerning the data security practices of corporations. He represents clients from a variety of industries ranging from national department stores to international outsourcers. He is the author of leading handbooks on data security including Data Privacy and Security: A Practical Guide for In-House Counsel, The EU General Data Protection Regulation: Answers to the Most Frequently Asked Questions, and the Better Business Bureau's Data Security Made Simpler. David has received numerous awards and recognitions including being named one of the top 10 attorneys worldwide in the areas of privacy, security, and cross-border information transfers, named a "trailblazer" of CyberSecurity & Data Privacy by the National Law Journal, and recognized by JD Supra as one of the most widely read names in the areas of privacy and security.

DATA SECURITY BREACHES:

Incident Preparedness and Response

by

Jena Valdetero

David Zetoony

Bryan Cave Leighton Paisner LLP

INTRODUCTION

It has been several years since data breaches first emerged as the lead news story. Despite increasing security and technology advancements, companies are still grappling with how to stay ahead of hackers and, when they cannot, how to respond to a breach in a way that minimizes business disruption and reputation risk.

Although statistics vary, in 2018 there were approximately 1,244 publicly reported data breaches and, according to one watchdog group, those breaches impacted nearly 450 million consumer records.[1] In the first five months of 2019, there were 555 data

[1] ***2018 End-of-Year Data Breach Report***, Identity theft Resource Ctr, https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/

breaches.[2] If this rate continues, 2019 is on pace to exceed 2018 numbers. In 2018, security compromises and data breaches most heavily affected the retail, finance, hospitality and manufacturing industries.[3] Together, these industries suffered 49% of all data compromising events. The other 51% of attacks affected a wide array of industries.[4] Consumers, regulators, shareholders, and business partners are scrutinizing whether organizations that suffer a data security breach had adequate security before the breach occurred, and are critically examining how organizations prepare for, investigate, and respond to security incidents. Instances in which stakeholders believe that an organization's preparation or response was inadequate have led to litigation, regulatory investigation, erosion of client base and, increasingly, changes in management.[5] Given this context, it is not surprising that when board members and general counsel are asked "What keeps you up at night?" the answer continues to be: "data security."[6]

---

[2] ***Data Breach Reports***, Identity Theft Resource Ctr. (May 31, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/06/2019-May-Data-Breach-Package-1.pdf

[3] Trustwave Holdings, Inc., Trustwave Global Security Report (2019) ***available at*** https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/

[4] ***Id.***

[5] ***See, e.g.,*** Tiffany Hsu, Los Angeles Times, "Target CEO Gregg Steinhafel Steps Down in Wake of Huge Data Breach" (May 5, 2014); Danielle Abril, Dallas Business Journal, "Sally Beauty To Replace Its CEO, Incurs $1.1M Cost from Data Breach" (May 1, 2014).

[6] IT/Cyber security was the most common response for both board members and general. FTI, Law in the Boardroom (2016) ***available at*** https://www.americanbar.org/content/dam/aba/administrative/litigation/

Since the publication of our first data breach response handbook, the legal ramifications for mishandling a data security incident have become more severe. In the United States, the number of federal and state laws and agencies that claim to regulate data security has mushroomed. The European Union also has enacted the General Data Protection Regulation which extended the United States framework for responding to data breaches across the EU, but with significantly enhanced penalties and an expanded definition of what data requires notification. In January 2020, California is set to become the first state to permit statutory damages following a data security breach if the litigant can prove that the breached company failed to implement and maintain reasonable and appropriate data security measures, overcoming the persistent hurdle litigants have faced to date of proving harm and damages. In order to effectively respond to a data security incident, in-house counsel must understand what a "security incident" entails, what their organization should do to prepare itself before the incident occurs, and what practical considerations will confront the organization when an incident arises. Effective response also requires understanding and preparing for the possibility that a data security incident may lead to lawsuits, regulatory investigations, or public scrutiny.

Over the years, Bryan Cave Leighton Paisner LLP has represented thousands of organizations planning for and responding to data security threats and breaches. This handbook provides a basic framework to assist in-house legal departments with handling a security incident. Section I explains what security incidents are, how often they occur, and which types of organizations are most at risk. It also discusses

---

materials/2017-women-in-litigation/materials/enforcement-trends/7_legal_survey_report.pdf.

the types of costs that a security breach may impose on an organization. Section II outlines how in-house counsel can help their organization prepare for a security incident and evaluate the degree to which the organization is already prepared. Section III walks through the different steps that must be taken once a security incident occurs, including how to investigate the incident and how to communicate with other potentially interested entities such as business partners or law enforcement. It also discusses steps to consider if the security incident is, in fact, a "breach" that might harm consumers.

I.
UNDERSTANDING THE NATURE AND SCOPE OF DATA EVENTS, INCIDENTS, AND BREACHES

People sometimes refer to a "data breach" loosely as any situation in which data may have been removed from, or lost by, an organization. Technically, however, "data breach" is a legally defined term that typically refers in the United States to a subset of such situations where there is evidence of an unauthorized "acquisition" of or "access" to certain types of sensitive personal information (***e.g.,*** Social Security numbers, driver's license numbers, or financial account numbers) that trigger a legal obligation by an organization to investigate the situation and to notify consumers, regulators, or business partners. As a result, it is important to realize that many of the situations that are referred to as "data breaches" in the media, and possibly by others in an organization, may not in fact meet the ***legal*** definition of the term. For the purpose of clarity, this handbook uses three terms to refer to security situations: a data security "event," "incident," and "breach."

A. Security Events

A "security event" refers to an attempt to obtain data from an organization or a situation in which data could, theoretically, be exposed. Many security events do not necessarily place the organization's data at significant risk of exposure. Although an event might be serious and turn into an "incident" or a "breach," many events are automatically identified and resolved without requiring any sort of manual intervention or investigation and without the need for legal counsel. For example, a failed log-in that suspends an account, a phishing email that is caught in a spam filter, or an attachment that is screened and quarantined by an antivirus program are all examples of security events that do not lead to an incident or breach and require little to no legal action.

B. Security Incidents

"Security incident" refers to an event for which there is a greater likelihood that data has left, or will leave, the organization, but uncertainty remains about whether unauthorized acquisition or access has occurred. For example, if an organization knows that a laptop has been lost, but does not know what information was on the laptop or whether it has fallen into the hands of someone who might have an interest in misusing data, the situation is a security incident. Another way to think of a security incident is as a situation in which you ***believe*** that electronic data that contains personal information ***may*** have been improperly accessed or acquired. As discussed in this handbook, security incidents almost always necessitate that an entity conduct a thorough investigation to test the suspicion that personal information was improperly accessed or acquired. Put differently, companies conduct investigations to determine whether there is, or is not, evidence that would redefine the "incident" as a "breach."

Security incidents are attributable to a variety of different causes—sometimes referred to as "attack vectors." While most breaches are caused by third parties, in 2018 approximately 26.3% were a direct result of employees from within an organization, which includes both inadvertent disclosure (i.e., human error) and insider threats.[7]

C. Security Breaches

As discussed above, a data "security breach" is a legally defined term. The definition varies depending on the data breach notification laws that are at issue. As a general matter, a security breach refers to a subset of security incidents where the organization discovers that sensitive information has been accessed or acquired by an unauthorized party and that acquisition has created the possibility that a consumer might be harmed by the disclosure. In the laptop example provided above, if your organization determines that the laptop was stolen and it contained unencrypted Social Security numbers, the incident would fall under the definition of a "security breach." As discussed below, security breaches almost always dictate that your organization consider the legal requirements of data breach laws.

Security breaches impact all types of entities. Two organizations—Privacy Rights Clearinghouse and Cyber Risk Analytics—systematically track publicly reported security breaches and provide up-to-date reports on evolving trends.[8]

---

[7] ***See*** Privacy Rights Clearinghouse, Data Breaches By Breach Type, ***available at*** https://www.privacyrights.org/data-breaches/breach-type?taxonomy_vocabulary_11_tid=2436

[8] ***See*** https://www.privacyrights.org/data-breaches and https://www.cyberriskanalytics.com/. In addition, several consulting

According to the former source, in 2018, approximately 53.4% of reported breaches impacted medical organizations, 11.6% impacted for-profit businesses, including retail and financial organizations, 3% impacted educational institutions, and 1.2% impacted government agencies and nonprofit entities. The industries remain unknown for the last 30.7% of incidents reported.[9]

Data breaches typically impact organizations in a number of ways:

Reputational Costs: A data breach can erode the confidence of customers or clients, which can significantly impact sales or the reputation of your organization. Often the indirect cost to the organization from adverse publicity outweighs direct costs and potential legal liabilities.

Business Continuity Costs: Breaches that create, expose, or exploit vulnerabilities in network infrastructure may require that a network be taken off-line to prevent further data-loss. For organizations that rely heavily on IT infrastructure, removing or decommissioning an affected system may have a direct impact on the organization.

---

firms that offer forensic investigation services publish annual reports concerning trends identified in their investigations of security incidents. These reports differ from the publicly reported breaches insofar as they largely rely on non-public data (***i.e.,*** incidents that may not have turned into breaches or that were not publicly reported). ***See, e.g***., Verizon 2019 Data Breach Investigation Report ***available at*** http://www.verizonenterprise.com/verizon-insights-lab/dbir/tool/

[9]***See*** Privacy Rights Clearinghouse, Data Breaches by Organization Type, ***available at*** https://www.privacyrights.org/data-breaches/organization?taxonomy_vocabulary_11_tid=2434 (referencing data security incidents from 2018)

Competitive Disadvantage: Breaches that involve competitively sensitive information such as trade secrets, customer lists, or marketing plans may threaten the ability of your organization to compete.

Investigation Costs: Security incidents involving IT infrastructure may require the services of a computer forensics expert in order to help investigate whether a breach has occurred and, if so, the extent of the breach.

Legal Costs: An investigation often will be led by experienced outside breach counsel who can protect communications under the shield of the attorney-client privilege and guide the company through the myriad legal and contractual requirements.

Contractual Costs: Your organization may be contractually liable to business partners in the event of a data security breach. For example, a breach involving an organization's electronic payment system typically will trigger obligations under agreements with its merchant bank or its payment processor. Those obligations may include, among other things, the assessment of significant financial penalties. As another example, some outsourcing contracts require companies that provide services to other companies to pay for the cost to notify impacted individuals and to indemnify their business partner from lawsuits.

Notification Costs: If your organization is required to, or voluntarily decides to, notify consumers of a data security incident, it may incur direct notification costs such as the cost of printing and mailing notification letters. Although most statutes do not formally require organizations to provide consumers with credit monitoring, identity−theft insurance, or identity−theft restoration services, in some situations offering such services at the organization's own cost has become an industry standard practice.

Regulatory Costs: A regulatory agency may decide to investigate whether an organization should have prevented a breach or whether it properly investigated and responded. In addition, some regulatory agencies are empowered to impose civil penalties or monetary fines in the event that they determine the organization's security practices were unreasonable or that the organization failed to properly notify consumers or the agency itself in a timely matter. Significant legal expenses are associated with a regulatory investigation.

Litigation Costs: Bryan Cave Leighton Paisner LLP's own 2019 Data Breach Litigation Report found that approximately 4% of publicly reported data security breaches result in the filing of a federal putative class action lawsuit. [10] This number is expected to rise considerably following the effective date of the California Consumer Privacy Act ("CCPA") in January 2020. Under the CCPA, successful plaintiffs will be able to recover statutory damages between $100-$750 per incident and attorney's fees. Although most suits have not resulted in a finding of liability, defense costs and settlement costs can be significant.

II.
DATA SECURITY INCIDENT PREPAREDNESS

Many legal departments and information technology professionals have relied on the adage that the best way to

[10] David Zetoony, Jena Valdetero, Andrea Maciejewski ***2019 Data Breach Litigation Report*** (available at https://www.bclplaw.com/en-US/thought-leadership/2019-data-breach-litigation-report.html).

prepare for a data security incident is to prevent one from happening in the first place. As a result, the historical focus for many organizations has been on taking steps to protect data and to prevent a breach from occurring. Such steps include instituting written information security programs that describe the security infrastructure of the organization, investing in defensive information technology resources, installing monitoring systems and training employees on good security practices. As the number of attacks from third parties that exploit previously unknown software vulnerabilities (sometimes referred to as "zero-day exploits") has risen dramatically, most organizations now realize that even the best security cannot prevent a breach. From that vantage point, preparing in advance for how your organization will respond when a security incident or breach occurs is essential.

Your organization will almost certainly survive a data breach, but how well it survives depends primarily on two factors directly within the control of the incident response team: (1) how quickly it responds to investigate and notify when a breach is discovered; and (2) how effectively it communicates about the breach to stakeholders (e.g., customers, employees, shareholders, regulators, the media, etc.).

Data security incident preparedness is a process that involves management, information technology, public relations, legal, and human resources. It typically includes the creation of a plan for how an organization will respond to an incident or a breach, as well as continual cross-staff and cross-department training to teach personnel about the plan and how to implement it. Each training exercise inevitably identifies areas in which an organization can improve its plan or provide additional training to improve its response.

In addition to supporting the organization's planning and training efforts, in-house counsel have a special role in terms of data security incident preparation. When a security breach occurs, there are several core legal documents that are typically implicated during, or after, the breach. In-house counsel should ensure that these documents are easily accessible and have a general awareness of the legal obligations or liabilities that these documents create. In-house counsel also should review the incident response plan to make sure it incorporates those same legal documents. The remainder of this section provides a brief description of each document that in-house counsel should evaluate and understand as part of the organization's preparation for a possible breach.

A. Cyber Insurance

76% of U.S. companies have purchased insurance specifically designed to cover part, or all, of the costs of a data security breach ("cyber-insurance").[11] Cyber-insurance policies differ in terms of what they cover, what they exclude, and the amount of retentions (***i.e.,*** the amount of money for which the insured organization is responsible before the policy provides reimbursement to the organization). If an organization has a cyber-insurance policy, in-house counsel should review it carefully before a security incident occurs so that the legal department understands the degree to which the policy protects (and does not protect) the organization from potential incident-related costs and liability. Policies also may obligate an organization to take specific actions, such as notifying the insurer or using pre-approved data incident response resources (***e.g.,*** investigators, credit monitoring, mailing services, public

[11]FICO Decisions: USA Views From The C-Suite Survey 2018, available at https://www.fico.com/en/resource-download-file/6341

relations firms, or outside counsel). Because data security law is rapidly evolving and changing, the policy should be reviewed annually to ensure that the protections it affords continue to align with changes in the legal landscape, coverage trends, and the organization's operations. In addition, your organization should carefully analyze the amount of coverage, any applicable self-insured retention, and any sub-limits to ensure they align with the likely costs and risks to the organization.

The following checklist provides a guide to evaluate a cyber-insurance policy. Before completing the checklist, it is important to determine whether an organization's goal in purchasing insurance is to help it handle typical data security incidents, to help it cope with catastrophic data security incidents/breaches, or both.

First Party Coverage: The policy should cover the likely costs incurred by an organization in responding to a breach, including the following:

1. <u>Forensic Investigators</u>

□ Does the policy cover the cost of retaining a forensic investigator?

□ If the organization processes payment cards, does the policy cover the cost of retaining a payment card brand forensic investigator, known as a PCI-PFI, whose investigator results would be reported to the card brands?

□ If a PCI-PFI is required to be retained, does the policy permit hiring a private forensic investigator to challenge the results of a PCI-PFI's investigation? **Tip: You generally will want to run parallel investigations as the PCI-PFI's findings may guide the fines/fees assessed by the card**

brands. Thus, hiring your own private forensic investigator will be essential to any assessment challenge.

- **Legal Counsel**

□ Does the policy cover legal expenses associated with retaining experienced breach counsel to lead the investigation and advise on legal requirements?

□ Can the organization retain counsel of its choosing, or is it limited to a panel of providers pre-selected by the insurance company? **Tip: You may be able to get your choice of counsel approved regardless of a panel limitation; your best shot at doing so will be when you are negotiating the purchase of the policy.**

- **Consumer Notifications**

□ Does the policy cover the cost of issuing notices to consumers?

□ Does the policy permit the organization to choose how it wishes to make notification (e.g., substitute notice where available for large breaches vs. mailing letters to individuals)?

□ Does the policy cover the cost of voluntary notification, or must notification be required by law? **Tip: Given the variations between what data elements warrant notification under the 50 state laws, a best practice is to follow the mantra "what you do for one, you do for all." For example, in a 50 state breach, not all states require notification if online account usernames and passwords**

are exposed. However, since the risk to all individuals is the same, generally an organization will wish to voluntarily notify individuals in states where it is not legally required.

- **Credit Monitoring Services**

□ Does the policy cover the cost of credit monitoring and identity theft protection services?

□ Will the policy pay for a minimum of two years of such services? **Tip: A small number of states have begun requiring credit monitoring services in certain circumstances (e.g., where Social Security numbers have been exposed). Massachusetts currently has the strictest legal requirement of two years. Following the mantra, "what you do for one you do for all," the organization should ensure coverage for a minimum of the strictest state law triggered by a breach.**

- **Public Relations**

□ Does the policy cover the retaining of a public relations expert to assist with communications arising from a breach?

□ Does the policy permit the organization to use its preferred PR firm? **Tip: You generally want to retain a PR company that specializes in data breach incident response. While the PR company you use to promote a new product, for example, may have a longstanding relationship with your organization, incident response management is different.**

- **Business Interruption**

□ Does the policy provide coverage for costs associated with an interruption or suspension of the insured's business as well as a service provider's business?

□ Does the coverage apply even where the insured voluntarily and intentionally shuts down its network to minimize the effects of a breach?

- **Software and Hardware Replacement**

□ Does the policy replace software and hardware damaged by a breach (sometimes called "bricking" coverage)?

- **Ransomware**

□ Does the policy pay for first dollar coverage of ransom payments?

□ Does the policy cover costs associated with hiring a vendor to facilitate a bitcoin payment? **Tip: Since most companies don't have their own bitcoin wallets, and obtaining one can be time consuming, a cottage industry has cropped up of vendors who, for a fee, will let you use their wallets to facilitate a ransom payment.**

Third Party Coverage: The policy also should cover any claims the insured may face from third parties, like individuals, regulators, and business partners.

Regulatory Proceedings

□ Does the policy cover regulatory proceedings that may result from a breach, including legal fees?

□ Does the policy also cover the fines or civil penalties that may be assessed as a result of a proceeding where insurable by the law of the most favorable jurisdiction? **Tip: It may be unclear whether certain regulatory penalties/fines are insurable as a matter of law, but the policy should provide for coverage where possible.**

Consumer Litigation

□ Does the policy pay for the cost of both defense and indemnification for consumer data breach lawsuits?

□ Does the policy exclude any potential causes of action that the organization may face in consumer lawsuits? **Tip: Many breach lawsuits will allege violation of a state consumer protection law. You should ensure that such claims will not be excluded under a policy's exclusion for state unfair and deceptive practices act claims (UDAP).**

□ Can the insured select their own defense counsel or must they use defense counsel pre-selected by the insurer?

Contractual Liabilities

□ Does the policy cover contractual liabilities that result from a data security breach? **Tip: Many policies will exclude contractual liabilities unless the liability also arises independent of the contract.**

□ If the organization accepts credit cards, does the policy cover contractual liabilities that may be owed to the organization's payment processor or merchant bank,

sometimes referred to as Payment Card Industry ("PCI") fines or assessments?

□ Does the policy exclude any type of contractual liability such as PCI fines or contracts that the organization may have with end-use consumers? **Tip: There are a variety of charges that can be assessed pursuant to the card brand rules. The policy should provide for coverage for all such charges.**

B. Written Information Security Program

After a security breach occurs, customers, the media, regulators, and other interested parties routinely ask what measures the organization took to prevent the breach in the first place. In-house counsel should consider, therefore, whether their organization would be able to produce documents that demonstrate that it was attempting to secure the information. Many outside observers will expect that this includes, at a minimum, a written information security program or "WISP." Indeed, Massachusetts requires companies to implement and maintain WISPs if they own or license personally identifiable information ("PII") about a state resident. In the event of a data breach impacting Massachusetts residents, an organization must inform regulators and impacted resident whether the organization maintains a WISP and whether it has or intends to update the WISP.[12]

While the most stringent, Massachusetts is not alone in enacting legislation mandating the implementation of safeguards to protect PII. Oregon, California, Texas, Rhode Island and Illinois all have enacted laws requiring certain levels of security for PII.

[12] Mass. Ann. Laws ch. 93H, § 3 (2018)

Financial institutions and health care entities also will need to comply with the WISP requirements of the Gramm-Leach- Bliley Act Safeguards Rule ("Safeguards Rule") and the Health Insurance Portability and Accountability Act ("HIPAA"), respectively. Companies will want to carefully review the requirements of those laws when creating a WISP.

The format and contents of a WISP can greatly vary depending on an organization's operations. Nonetheless, there are areas of commonality. Although in-house counsel should be aware of any regulations and standards that apply to the specific organization's industry, at a minimum, the organization's WISP should include a description of the following:

- The administrative safeguards that exist to keep sensitive personal information secure;

- The technical safeguards that exist to keep sensitive personal information secure;

- The physical safeguards that exist to keep sensitive personal information secure;

- The process used by the organization to identify, on a periodic basis, internal and external risks to the information that it maintains;

- The specific employee who is ultimately responsible for maintaining and implementing security policies;

- The sensitive information maintained by the organization;

- Where and how sensitive information will be stored within the organization;

- How sensitive information can be transported away from the organization;

- Procedures that discuss the following:

    - Username assignment
    - Password assignment
    - Encryption format
    - Provisioning of user credentials
    - De-provisioning of user credentials (e.g., for terminated employees)
    - Employee training on security topics
    - Destroying data
    - Retaining service providers that will have access to data

Some organizations choose to draft their WISP based on standards or formats created by third parties. Although there are many frameworks that can be looked to, some of the most popular frameworks are those published by the International Standards Organization ("ISO") or the National Institute for Standards and Technology ("NIST"). Other organizations retain third parties to certify that their WISP complies with these frameworks.

Beginning in January 2020, the California privacy law, the CCPA, will provide for statutory damages where an individual's sensitive information is breached if the plaintiff can establish that the organization failed to implement and maintain reasonable and appropriate security measures. Thus, it will be imperative for an organization show, at a minimum, that it has a WISP. In February 2016, California published the California Data Breach Report, in which it specifically identified the 20 controls set forth

in the Center for Internet Security's Critical Security Controls ("CIS") as the "minimum level of security" an organization should meet.[13] Indeed, the report states that the "failure to implement all of the Controls that apply to an organization's environment constitutes a lack of reasonable security."

Tip: Your organization's WISP should, at a minimum, incorporate both the WISP requirements set forth under Massachusetts's law and in CIS.

C. Incident Response Plan

An incident response plan explains how an organization handles security events, security incidents, and security breaches. Among other things, the plan helps employees from different departments understand the role that they are expected to play when investigating a security incident and identifies other people within the organization with whom they should be coordinating. The plan also can help educate employees concerning what they should and should not do when faced with a security incident and can provide them with a reference guide for resources that may help them effectively respond to an incident or breach.

Incident response plans take a variety of forms, and there is no mandated structure. The following topical recommendations, however, may help you draft an incident response plan or evaluate the thoroughness of one that already exists:

□**Definition of Security Event, Incident, and Breach**. Consider explaining the difference between an event,

[13] Available at http://src.bna.com/cFY

incident, and breach so those in the organization involved with incident response understand the distinction.

□**Security Event Escalation**. By their very nature security events are relatively common occurrences. Only a small percentage of events will become incidents, and an even smaller percentage of events will ultimately become breaches. Nonetheless, it is important to explain the process under which an event should be escalated to an incident, or a breach, and the impact that such an escalation has on who within the organization needs to become involved in an investigation and how the investigation should be handled.

□**Responsibilities For Conducting an Incident Investigation**. The plan should explain who within the organization is responsible for investigating security incidents, to whom information should be reported, and who has the authority (and responsibility) to seek additional resources when needed. To the extent that one of the purposes for conducting an investigation is to provide in-house counsel with information needed to make legal recommendations, the plan should consider whether an organization desires the investigation to be conducted under the auspice of the attorney-client and attorney work product privileges. If so, the plan should make clear that the investigation is operating under the direction of counsel and the plan should provide instructions to the employees who may be collecting information concerning how to preserve privilege, including involving legal counsel in the investigation of certain types of security incidents. **Tip: Be sure to designate a project manager to hold the team members accountable for their assigned tasks and to ensure that the investigation is proceeding quickly.**

□**Internal Contact Information**. Many plans also include a quick reference guide naming the people within an organization who can help in the investigation of a security incident. This should include the incident response team member and their cell phone numbers, along with individuals who can serve as back-up support in the event a response team member is unavailable.

□**External Contact Information**. Many plans include a quick reference guide naming the people outside of an organization who can help in the investigation of a security incident, which may include contacts with law enforcement (***e.g.,*** FBI and Secret Service), outside counsel, forensic investigators, call-center support, credit monitoring, public relations experts, etc. If the organization has a cyber-insurance policy, the approved vendors should be identified in the plan. **Tip: If your organization operates in the European Union and is subject to the GDPR, the plan should include the name of the lead supervisory authority and the relevant information for reporting a breach, as breaches resulting in a risk to the rights and freedoms of individuals may need to be reported to the regulator within 72 hours after your organization becomes aware of it.**

□**Recordkeeping**. Plans typically explain the type of documents and records that should be kept concerning the investigation in order to permit in-house counsel to reconstruct when the organization knew certain pieces of information and when the organization took certain steps. Such reconstruction may be necessary in litigation or a regulatory investigation.

□**Post-Incident Reporting.** Many plans discuss how the organization will take information learned during an incident and incorporate that back into the organization's security program. This might include "lessons-learned" from how an incident was handled or ways to prevent an incident from occurring again. Under the GDPR, organizations are required to document an incident, its effects, and any remedial action taken. If the organization decided it was not a reportable breach, it should document the basis for that decision.

D. Contractual Obligations to Business Partners

In situations in which a security incident involves data that is wholly owned by an organization, there may be few, if any, obligations for the organization to notify business partners. Often, however, business partners may have an interest in the information impacted. For example, if an incident involves data of another entity for which your organization is performing services, you may have an obligation in your service agreement or under state data breach notification statutes to notify that entity of an actual (or suspected) security incident. The contractual requirement sometimes requires notifying the partner in a relatively short time frame (***e.g.,*** immediately or within 24 hours) when an incident is ***suspected***. As another example, if an incident involves payment card information that you received from consumers, the agreement that you have with your payment processor or merchant bank may similarly require that you notify those entities or additional third parties (***e.g.,*** Visa, Mastercard, Discover, and American Express) of a potential security incident.

An essential component to preparing for a security incident is understanding the contractual obligations that your organization may have to business partners or affiliates.

If your organization is regulated by the GDPR, you may have notification obligations if you are serving as a processor for another company, or if you are a joint controller. **Tip: Ideally those obligations—including the telephone numbers or addresses of business contacts—would be summarized in the incident response plan for easy access in the event of a breach.**

III.
INCIDENT RESPONSE

As discussed above, the best way to investigate a security incident is to follow an incident response plan that was put in place before the incident occurred and that takes into consideration the specific needs and resources of an organization. If an organization does not have an incident response plan, the steps that follow outline best practices that take into account possible legal requirements and obligations. Among other things, these include recommendations for investigating the incident, coordinating with data owners, communicating to the public or media, communicating with law enforcement, communicating with consumers, and communicating with regulators. This section also discusses the types of services that organizations often offer to consumers whose information was involved in a data breach and unique issues that arise in the context of certain types of breaches.

A. Investigating a Security Incident

When deciding how to investigate a security incident, an organization should consider the following factors:

1. Include legal counsel at the inception of the investigation

Once a data breach has been discovered, the organization should notify its in-house legal counsel. That person can determine whether the involvement of outside legal counsel specializing in data breach response is necessary. If the organization does not have in-house legal counsel, then outside counsel should be consulted and retained as early as possible.

A primary benefit of involving counsel early in an investigation is to allow counsel to help decide whether the remainder of the investigation should be conducted under the cloak of attorney-client privilege. If counsel recommends that the investigation should be led by legal as the information obtained is necessary in order for counsel to provide the organization with legal advice, any employees that take part in the investigation should be instructed to copy counsel on all internal communications concerning the cause and the scope of the breach or, when speaking to others, to clearly indicate that they are collecting information at the behest of counsel. For example, if information needs to be requested from IT or HR by email, the subject line of the email should preferably read "Attorney Client Communication: Information Requested By Counsel" to make sure that anyone who reads the email at a later time understands the context in which it was sent, the purpose for which the information was being collected, and the fact that the communication may be privileged and exempt from disclosure outside of the organization. **Tip: Vendors should be retained by legal counsel to work at their direction in order to assist with providing legal advice to the organization.**

2. Form a core team of personnel to attend to the breach

Effectively investigating a security incident often requires a team of personnel. This may include representatives from IT/IS, legal or risk management, operations, marketing & communications, and human resources (if the breach involves employee misconduct or employees' PII). Ideally, the team will have been identified and trained on data breach response prior to any incident. One person should be designated to keep a log or running chronology of the investigation to enable the organization to reconstruct, if needed at a later time, what information the organization knew at what time. Personnel should take extreme care when documenting the investigation to only include factual assertions about the breach and to avoid creating a factually inaccurate record or a record with opinions that may be based on preliminary information.

3. Contain the breach and preserve evidence

When dealing with an electronic breach, it is important to preserve all evidence and isolate the source of the breach. An organization's IT department should be advised to identify the source of the breach and isolate the compromised systems from the network. The organization should take care not to destroy or alter evidence and to continue monitoring the system (e.g., unplug the affected system; do not restart it or turn it off).

If the organization's IT department has relatively little experience with investigating security incidents, do not necessarily assume that they will automatically preserve evidence or understand how evidence should be preserved. To the contrary, IT departments that have historically focused on business continuity or user-experience may inadvertently overlook the steps needed to preserve the chain-of-custody of evidence in an effort to try to remove suspected malware quickly or to restore

the functionality of certain items. In-house counsel may need to explain the importance of forensically preserving evidence in order to further examine, at a later point, whether the incident was in fact a breach, and, if so, the extent of the breach, including whether personal or sensitive data was accessed. In some instances, in-house counsel may need to help IT understand what it means to forensically preserve evidence, and to evaluate whether IT's methods for copying and logging data would be defensible before a regulator or in court.

4. Retain a third-party forensic investigator

Many competent IT departments lack the expertise, hardware, software, or personnel to preserve evidence in a forensically sound manner or to thoroughly investigate a security incident. In such a situation, in-house counsel needs to be able to recognize the deficiency quickly and recommend that the organization utilize external resources to help collect and preserve electronic evidence and investigate the incident.

As discussed above, in-house counsel should consider whether the investigator should be retained through in-house counsel or outside counsel to preserve the right to claim that the investigation and all notes related to it are protected by attorney-client privilege and the work product doctrine. The investigator should be able to investigate the attack vector, decipher the scope of the breach—including what records were viewed or acquired and how many times the third party gained access to the system—and identify whether, and how, data left the organization's information technology environment. These functions are sometimes referred to within the data security community as identifying "infiltration," "aggregation," and "exfiltration." The investigator also may be able to help in-house counsel coordinate with law enforcement efforts to catch a perpetrator, although unfortunately in most instances the

perpetrator will remain unidentified or be located outside of the jurisdiction of most U.S. law enforcement agencies.

When retaining a forensic investigator, it is important to remember they will be given access to your organization's networks and there is a high likelihood that, if a breach occurred, they may gain access to sensitive personal information as part of their investigation. As a result, you should review the agreement between the investigator and your organization carefully to make sure the investigator agrees to apply the security warranted for the type of information to which they may gain access, and provides appropriate indemnification for any data security lapses of its own. A best practice used by proactive organizations is to identify and retain a forensic investigator before a breach occurs. Doing so will ensure that the organization will be able to negotiate favorable terms and conditions in the retainer agreement before a crisis situation eliminates much of the organization's bargaining power. **Tip: If you are subject to the GDPR, you should consider having an investigator sign a data protection addendum governing the access to and use of personal data.**

5. Assign a crisis manager

Incident response teams are usually comprised of personnel from a variety of backgrounds and representing a variety of internal resources and departments. Because the members of a response team rarely have the same reporting structure, confusion about who has authority to convene an investigation, assign projects, or retain needed resources can lead to inefficiencies.

A pre-designated crisis manager that reports directly to, and has authority conferred from, senior management often facilitates the most efficient response. This person should work closely

with legal counsel to ensure attorney-client privilege is maintained. This person should hold each incident response team member and outside vendor accountable for completing their assigned tasks timely and efficiently.

B. Coordination with Data Owners

Many organizations rely on vendor agreements to carry out various business operations. These agreements may authorize the organization or the vendor to have access to or possess sensitive information owned by the other entity. As discussed below, state data breach notification laws typically place the onus on the ***owner*** of data to notify affected persons when sensitive personal information is wrongfully accessed or acquired. For instance, a data storage vendor may possess a database that contains Social Security numbers, but the database may belong to the vendor's client. In many states, the vendor may not have an obligation to notify affected persons itself, but it most likely has a legal obligation to notify its client, who in turn will have an obligation to notify the affected persons. Similar rules apply under the GDPR. A data processor is required to notify the data controller in the event of a data breach, and the data controller bears the responsibility for notifying the supervisory authority and the data subjects.

As a result, when responding to a data breach, an organization should analyze whether the affected information was collected directly by it, or whether the data belongs to a third party. If the data belongs to a third party, the organization should consult its contracts with the data owner and applicable data breach notification statutes to determine its notification obligations. In many instances, although the data owner technically has the legal obligation to notify affected persons, the data owner will look to the data user to make the notification or pay for the costs of notification. **Tip: An organization may wish to prepare a**

spreadsheet of the data notification provisions included in its key contracts. In the event of a breach, the spreadsheet can be quickly consulted to determine the obligations, as such contracts typically include short timeframes during which notification must occur.

C. Communication to the Public/Media

After a breach occurs, organizations should consider a proactive and reactive public relations and media strategy.

A proactive strategy assumes that your organization has control concerning when, and what, information will be conveyed to the public, to the media, and to the impacted consumers about the breach.

As discussed below, state and federal laws may require an organization to notify consumers or the media within a certain time period of discovering a breach. For example, HIPAA requires many organizations in the health care industry to notify prominent media outlets if 500 or more individuals within a geographic area are impacted.

But even if no federal or state law requires an organization to notify the media, there may be significant advantages to notifying individuals as early as is practical. The sooner individuals are notified that sensitive personal information may have been exposed, the sooner they can take proactive steps to reduce the likelihood that they will become the victim of identity theft or other fraud. For example, an early informed consumer can request that the major credit reporting agencies put a freeze on their credit or change the passwords associated with financial accounts. If proactive measures prevent individuals from becoming victims of fraud, they also reduce the likelihood that the consumer will sue your organization for damages allegedly

incurred by the breach. Early notification also may reduce the likelihood of allegations by regulators that your organization did not comply in a timely fashion with data breach notification laws.

While early notification can be beneficial in some situations, in other situations premature notification can harm both consumers and the organization. Data breach investigations, particularly those that involve the exposure of electronic records, can be extremely time-consuming. It may take some time to identify the true scope of the breach to determine whether a breach, in fact, occurred, or to verify which individuals may have been impacted. It also takes time to create an accurate communication to individuals and to coordinate with third parties, such as a mailing house, or ID theft protection service providers.

An organization that notifies consumers before the investigation is complete risks providing inaccurate information concerning the scope and nature of a breach. Specifically, if the investigation is not complete, some consumers may be told that their information was exposed when the investigation ultimately reveals that not to be the case. These consumers may be subjected to unnecessary worry, cost, and inconvenience to try to mitigate harm that will never materialize. Conversely, other consumers may be told that their information was not exposed when the investigation ultimately reveals that it was. These consumers may be confused and may fail to take protective measures that would mitigate a heightened risk of identity theft. Clarifying initial inaccurate information provided by an organization can be both difficult and time-consuming and can deflect the organization's resources and attention from responding to the breach itself. In addition, confusion by consumers and efforts to clarify that confusion can significantly increase the risk of litigation, as some consumers may incorrectly believe that the organization provided erroneous

information intentionally. Such a belief may adversely impact your brand and reputation.

There may be an additional drawback to prematurely notifying consumers of a security breach. If an investigation has not determined how a third party obtained information or whether the third party has misused the information, putting the culprit on notice that the organization is aware of the security breach may compromise the investigation.

Once an organization has decided on its proactive communications strategy, in-house counsel should work closely with the organization's communications resources concerning how that strategy will be implemented. Among other things, the following communications channels should be considered:

- Traditional Media. The organization should consider whether to provide information in print media or television media. This may take the form of a crafted press release or direct communications to specific reporters.

- Social Media. To the extent that your organization desires to disseminate information quickly, you should consider the potential risks and benefits of utilizing social media.

While it is important to consider the pros and cons of providing information to the public as part of a proactive media strategy, in many situations an organization does not control when the public becomes aware of a breach. The media may learn about a breach from a business partner, a government agency, a consumer, or a disgruntled employee. You should anticipate that in such a situation the media may report inaccurate information or may report speculation as "fact." In-house

counsel should be prepared to work closely with your organization's communications resources when determining how to respond to such reports. Among other things, the following factors should be considered:

- Difficulty Correcting the Record. Although a media report may be based on speculation, if the organization's investigation has not concluded, it may be difficult for the organization to correct the record.

- Difficulty Conveying the Tentative Nature of Early Information. If the organization makes a statement to the media based on the limited information that is available, there is a strong risk that the media may characterize the statement as the "position" of the organization and not fully explain qualifications and limitations of that position.

- Developments In Information May Be Interpreted as Intentional Withholding. As the investigation develops, the media may misinterpret additional information that is provided by the organization. The best case scenario may be that the media characterizes such information as a "revision" by the company. The worst case scenario may be that the media implies that the company should, or could, have disclosed the new information earlier.

- New Headlines. Each time an organization releases information to the media, it is a potential opportunity for the media to create a new headline concerning a breach. Establishing a pattern of continuously updating the media may result in creating a constant stream of media attention concerning your organization.

D. Communication with Law Enforcement

Many security incidents involve a crime that has been committed, or is in the process of being committed, against an organization. For example, when someone attempts to hack into an organization's network to obtain sensitive personal information, they may be committing criminal trespass, theft, attempted identity theft, computer fraud, wiretapping, or economic espionage, among a host of other statutory violations. Where a crime is being committed against an organization, the organization should consider reporting it to law enforcement. Contacting law enforcement may result in assistance stopping the criminal behavior, useful information that may help the organization's investigation of the incident, or prosecution of the culprit. It also may help demonstrate to the public that the organization was diligent in investigating the incident and taking steps to protect consumers. Note, however, that law enforcement's resources and ability to assist an organization, particularly when there is no identifiable monetary loss (e.g., actual fraud as a result of breached systems or money lost due to wire transfer fraud), is limited. Thus, it is important to set your incident response team's expectations about the extent to which law enforcement will be helpful.

There is no single federal or state law enforcement agency with jurisdiction over data breaches. In general, however, in-house counsel should consider contacting the Federal Bureau of Investigation's Cybercrimes unit or the United States Secret Service with regard to a security incident that involves the electronic exfiltration of information. The FBI offers online reporting at www.IC3.gov. For security incidents that involve paper records or known individuals (***e.g.,*** employees or former employees), in-house counsel also might consider contacting municipal law enforcement in the jurisdiction in which the individual resides or works.

When communicating with law enforcement, in-house counsel should be cognizant that information provided to law enforcement may lose the protection of the attorney-client privilege. Recent legislation – including the Cyber Security Act of 2015 – is designed to help companies share information with the government without losing privilege protection, but such legislation should be closely examined, as their applicability typically depends on the type of information shared, how the information will be used, and the law enforcement agency with which it will be shared.

E. Communication with Impacted Consumers in the United States

Although Congress has attempted to agree on federal data breach legislation, as of the publication date, there is no national data breach notification law that applies to most companies. There are federal statutes that apply to financial institutions, common carriers, health care providers, and vendors of health records. If your organization falls within one of the aforementioned categories, be sure to understand the requirements of the relevant federal law and any additional requirements imposed by state law, as state law may apply in addition to federal law.

While federal data breach notification law is limited in scope, state data breach laws apply whenever a data breach involves records of that state's residents. All 50 states, plus the District of Columbia, Puerto Rico, Guam, and the Virgin Islands, have each enacted their own statutes addressing an organization's notification obligations in the wake of a data breach involving certain types of PII.

The following section first summarizes key information about the federal data breach laws. It then explains pertinent state data

breach law provisions and highlights important areas in which the state laws diverge. In the event of a breach involving records of consumers who live in multiple states, the laws of those states should be reviewed to ensure that the organization is complying with notification requirements.

1. Are there any federal laws that apply to your organization?

While there is currently no national data breach notification law, there may be other federals laws that apply to the organization. Federal law most notably implicates organizations in the health care industry, financial institutions, and common carriers.

HIPAA requires health care providers, health plans, healthcare clearinghouses and certain "business associates"[14] to protect covered health information. Covered entities that fall within HIPAA's scope must notify each impacted individual within 60

---

[14] A "business associate" is defined as "with respect to a covered entity, a person who: (i) [o]n behalf of such covered entity . . . , but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter . . . ; or (ii) [p]rovides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation . . . , management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person." 45 C.F.R.. § 160.103

days after discovering a breach.[15] Notification under HIPAA must be written unless consent for alternative notification has been given. The written notice must include a description of the incident, the type of health information accessed, protective steps impacted individuals should take, any mitigation the organization is undertaking, and contact information for those individuals who wish to learn more.

The Gramm-Leach-Bliley Act ("GLBA") regulates financial institutions' use of consumer nonpublic personal information. In the event of a data breach, if it is found reasonably possible that misuse of compromised personal data will occur, the financial institution should notify its customers. **Tip: The breach notification requirements are found in the 2005 Interagency Guidelines Establishing Information Security Standards.**[16]

Common carriers should be aware of their obligations under the Telecommunications Act of 1996. If a customer's proprietary network information is breached, an organization subject to the Telecommunications Act must notify law enforcement within seven days and, following the law enforcement notification, the organization must notify affected customers.

These federal laws do not supersede state law. Meaning, organizations subject to federal law also must consider the often more stringent state laws at play, although many state laws provide that notification in compliance with HIPAA or the GLBA constitutes proper notice under the state law.

---

[15] 45 CFR § 164.404

[16] https://www.law.cornell.edu/cfr/text/12/appendix-F_to_part_225

2. Do the state laws apply to your organization?

As a general rule, if your organization maintains or transmits PII belonging to citizens of a particular state, you should consult the data breach notification law of that state in the event of a breach. Some states maintain that "any entity" is subject to the data breach notification law, while other states limit applicability only to those entities that "conduct business in the state." Most of the statutes place the onus on the "owner or licensor" to ensure that affected consumers are notified, however, some states (***e.g.,*** Rhode Island and Wisconsin) place that obligation on organizations that simply "maintain" consumer information. As discussed below, even if the breached organization does not own or license the consumer information, most state laws will require that the organization timely notify the data owner(s) of the breach so that they may fulfill their notification obligations.

The notification laws typically apply only to consumers who are residents of the state in question. However, Hawaii, New Hampshire, and North Carolina's statutes do not contain this limitation and apply instead to "affected persons," while Texas' statute specifically applies to Texas residents ***and*** residents of other states.

3. What PII triggers notification?

The statutes generally require notification in the event of breaches involving the following information: the consumer's name in combination with their Social Security number, driver's license number, account number and access code. Some states go even further and require notification in the event other types of information are accessed or acquired. For example, many states (***e.g.,*** Arkansas, Nebraska, Washington and Wisconsin) require notification if biometric data is breached. North Dakota requires notification if the consumer's date of birth

or mother's maiden name are exposed, since this data is often associated with password recovery or identity verification on online accounts. A number of states require notification if certain medical or health information is at issue. Alabama, Arizona, Delaware, Maryland, North Carolina, Montana, and Wyoming have expanded their definitions to include taxpayer identification numbers. Washington recently added student ID number and private key (used for online signatures) to its list of protected information. Some states require notification if military ID and passport numbers are impacted.

Increasingly, states have added the requirement for notification in the event of a breach involving a username or email address in combination with a password or security question and answer that would permit access to an online account. The rationale is that many people use the same username and password across multiple online accounts. Having those credentials stolen in one breach could expose individuals to the risk of having other accounts hacked. Some states, like California and Arizona, permit notification to be electronic for such breaches only. **Tip: While the requirements vary among states, a good rule to follow is "what you do for one, you do for all." In other words, if you have a 50 state breach of usernames and passwords, but not all states technically require notification to affected individuals, it may be insufficient to explain that you did nothing to help the individuals in the non-required state protect themselves from harm because you were not forced to as a matter of law.**

The state statutes provide that a breach of personal information that is publically available does not give rise to a notification requirement. Similarly, the breach of personal information that is encrypted generally does not give rise to notification obligations, because data is assumed to be sufficiently protected from disclosure if accessed in its encrypted form.

Because not every breach of personal information is likely to lead to a risk of harm to the affected person, many states have included a materiality threshold that limits notification only in cases where the breach "compromises confidentiality, integrity, or security." A handful of states do not contain any such limitation, however, and appear to require notification in the event of any breach, regardless of the risk of harm flowing from the breach.

4. How quickly must the organization notify affected consumers?

Most of the state statutes do not strictly define the timing in which notification must occur. Only a few states prescribe specific deadlines (***e.g.,*** Louisiana (60 days), Wisconsin (45 days), and Florida, Colorado, and Washington[17] (30 days)). Generally, the notification must occur in the "most expedient time possible and without unreasonable delay." How this language is interpreted may vary, but as a general rule the organization should endeavor to notify affected consumers within 30-45 days. The triggering point is generally the date on which the organization determined it had a breach or had a reason to believe a breach may have occurred. All states will permit organizations to delay notification if law enforcement determines that notice to individuals would interfere with a criminal investigation. **Tip: As a practical matter, law enforcement will rarely advise that an organization delay notification. If your organization intends to delay notification based on a request by law enforcement, consider obtaining written confirmation of that request to explain any delay at a later time.**

---

[17] Effective March 1, 2020.

5. What information does the consumer notice have to include?

Many state laws do not provide any instruction or requirements concerning the content of a notification, leaving the content to the discretion of the organization. Other states mandate that some or all of the following information be included in the notification letters: (1) a description of the breach; (2) the approximate date of the breach; (3) the type of personal information obtained; (4) contact information for the credit reporting agencies or government agencies; (5) advice to the consumer to report suspected identity theft to law enforcement and/or a reminder to be vigilant about identity theft; and (6) a toll-free number provided by the reporting organization where consumers can call with questions about the breach. However, because there are many deviations from what the states require, each individual statute should be examined in connection with reporting a breach.

California designates a particular format that should be followed. Generally, in multistate breaches, organizations will opt to use the California format even for residents of other states where it is not required.

Massachusetts' statute contains a significant departure from the other states in that it ***prohibits*** an organization from identifying the nature of the breach. Thus, in a nationwide breach, in-house counsel should consider whether Massachusetts residents should receive a slightly modified notification letter compared to the one sent to residents of other states. In addition, Massachusetts and Illinois both prohibit companies from providing in the notice the number of those states' residents impacted by the breach.

6. How must an organization notify affected consumers?

The majority of states require that consumers be notified in writing. Email notice can provide substantial costs savings over mailing written notice, but notification through email is only permitted in approximately one-third of the states and in those states there are restrictions on when email notice is permissible. For example, many states require that the consumer either has consented to receive electronic notices, or that the primary method of communicating with the consumer has been through email, such that the consumer would not be surprised by receiving email notification. Additional states permit email notification if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001, the federal ESIGN Act.

If your organization is considering an electronic notice, you should evaluate the risk that third parties may attempt to create fake electronic messages that appear to originate from your organization (a practice called "spoofing"). These messages can further victimize consumers by having them provide additional personal information (a practice called "phishing"). For example, instances have been reported where individuals send fake notification letters that ask consumers to click on a link that, in turn, downloads malware onto the consumer's computer, or to send PII to a service allegedly providing credit monitoring. As a result of these risks, some companies have chosen not to send electronic messages concerning a security breach. Or some companies make clear in the electronic messages that they do send that the company will never request that consumers transmit additional PII over email or click on a link to obtain credit monitoring. In other situations, companies

have determined that the risk of phishing in their industry is low and have opted (where permitted) to notify consumers by email.

Most states will permit "substitute notification," which is typically some combination of email, posting information about the breach on the organization's website, or notifying the media. However, the circumstances under which such notice is permitted vary widely. Substitute notice generally is permitted only when the notification costs are great or the number of persons to be notified is large; what is considered "large" varies significantly from state to state. For example, Arizona permits substitute notification if the notification cost exceeds $50,000, or the class of persons exceeds 100,000, or if the organization has insufficient contact information for affected consumers. New Jersey (and many other states) will not permit substitute notice unless the cost exceeds $250,000, or the class exceeds 500,000, or if the organization has insufficient contact information for affected consumers.

Many states permit an organization to create its own notification procedures for the treatment of PII if its information security policy complies with the timing requirements under the state law. If notification is done in accordance with the organization's policy, the organization is considered to have complied with the state law.

7. Should an organization ever voluntarily notify consumers of a breach?

In many instances involving a data breach, notice will not be required by any state or federal laws. However, there are many situations in which an organization may choose to voluntarily notify consumers. For example, while a minority of states requires notification for a breach of electronic account user names/email addresses and passwords, if such a breach also

involved consumers in other states, the organization may want to notify all affected persons for consistency.

In addition, as addressed above, breaches often become public through other means (***e.g.***, internet blogs, the media). Self-notifying, even when such notification is not legally required, may help the organization frame the message before the message is framed for it by a third party. Although the organization may face initial criticism for its data security practices, consumers may ultimately appreciate an organization's candor in connection with a breach.

8. Is notification required to any other parties?

Various state statutes also require third-party notification. Some states will require the organization to notify the three major credit reporting agencies in the event of a breach involving a minimum number of affected persons (typically, at least 1,000). The statutes with such a requirement generally do not set forth what information should be provided to the credit reporting agencies other than the timing, distribution, and content of the notices that the organization intends to send to consumers.

In addition, as discussed above, if the organization is not the data "owner," as defined by the various statutes (typically, an organization that maintains or stores, but does not own or license, personal information), then many state statutes will require the organization to notify the data owner of the breach "immediately" or "as soon as possible." Oregon requires data vendors (organizations that process data on another's behalf) to notify the data owner within 10 days of discovering the breach. Once notified, the obligations would then fall to the data owner to comply with the consumer notification requirements of the various statutes. Oregon requires the data vendor to notify the attorney general if the data owner fails to do so.

Many states have a requirement that the state government (usually the Attorney General's office) should be notified of a breach under certain circumstances. Of those states, most require notification in the event of a breach involving any number of persons, while others require that the breach impact a minimum number of residents before state government notification is necessary. For example, New York requires government notification in a breach involving any number, Florida requires government notification when 500 Florida residents are affected, and Arkansas, Hawaii, Missouri, and South Carolina only require state government notification if the breach involves at least 1,000 residents.

For states requiring government notification, the statutes again vary on what information is required to be reported. Most states will require that the reporting organization provide a copy of the consumer breach notification letter, identify the number of residents notified, and the timing of the notification. Some states, e.g., Indiana, North Carolina, and New York, have forms prepared by the state for use in connection with government notice of a breach, and these forms are available online. In the event of a multistate breach, each statute should be carefully examined to ensure full compliance.

9. What types of services should the organization offer to affected consumers?

A growing number of states, e.g., Connecticut, Delaware, and Massachusetts, require that a company provide ID theft-related services if a breach involves Social Security numbers. Massachusetts requires such services be provided for 24 months. Other data breach notification statutes do not require that an organization offer any services to consumers whose information was involved in a breach.

Nonetheless, organizations typically consider whether to voluntarily offer ID theft-related services (***i.e.,*** monitoring a consumer's credit report for suspicious activity), identity restoration services (***i.e.,*** helping a consumer restore their credit or close fraudulently opened accounts), or identity theft insurance (***i.e.,*** defending a consumer if a creditor attempts to collect on a fraudulently opened account and reimbursing a consumer for any lost funds). For those organizations that choose to offer one or more ID theft-related services, they are also faced with the question of how long to offer each of the services; durations typically range from one year to three years. In September 2014, California amended its personal information privacy law to require that businesses that choose to provide identity theft prevention and mitigation services do so for 12 months at no cost to the affected persons.

There are several factors to consider when choosing what (if any) services to offer consumers. In terms of mitigating potential harm, credit monitoring (and to a lesser extent identity restoration services and identity theft insurance) is focused on the prospect that a third party might open a financial account in a consumer's name. Not all breaches involve data that would permit a third party to open a financial account, however. For example, while a breach that involved a consumer's name and credit card number could theoretically lead to unauthorized charges placed on the credit account, name and credit card number alone are insufficient to attempt to open a new financial account, and unauthorized charges on an existing account are unlikely to be identified by credit monitoring.

Although credit monitoring may not be connected to the risks attendant with many breaches, an organization should consider whether a failure to offer the service – even if unconnected to the breach – could be misunderstood by consumers and regulators as a failure by the company to adequately protect

consumers. Conversely, offering such services where the organization views them as unconnected to the risk of harm could be construed in litigation as an admission that the company believes harm is likely to occur.

If your organization chooses to offer credit monitoring, identity restoration services, or ID theft insurance, in-house counsel should carefully consider the vendors that are selected to provide the services and the contractual limitations on those vendors. Specifically, vendors (and by association the breached organizations which retained the vendors) have been criticized for the following:

- Requiring consumers to submit sensitive personal information to the vender in order to enroll in the offered service(s);

- Attempting to "upsell" consumers on additional protection services that are offered by the vendor, but the price of which are not covered by the organization;

- Deceptively advertising or describing the credit monitoring, identity restoration, or ID theft insurance services or products;

- Applying inadequate security to protect the information of consumers who enroll in the credit monitoring, identity restoration, or ID theft insurance products.

F. Communications with Supervisory Authorities and Individuals in the European Union

The GDPR is a bit like the U.S. breach notification laws on steroids. The GDPR applies to establishments in the EU (***e.g.,*** a retailer has stores located in the EU) as well as to companies outside the EU that "offer goods or services" to people located in the EU (***e.g.***, a U.S. company selling tours of New York City to people in France) or to companies that monitor the behavior of people in the EU. If your company is regulated by the GDPR and you suffer a data breach, it is important to understand the ways in which the GDPR differs from U.S. breach notification laws.

First, the definition of "personal data," the EU-equivalent of what the U.S. laws refer to as PII, is much broader. Article 4 states that "'personal data' means any information relating to an identified or identifiable natural person ('data subject')" – and it means ***anything***, including identifiers that you might not expect, like personal IP addresses or business contact information.

Second, the definition of data breach also is broader. Like its U.S. counterparts, the GDPR applies where personal data is accessed by or disclosed to an unauthorized third-party, known as a confidentiality breach.

Unlike its U.S. counterparts, the GDPR also requires notification to impacted individuals if personal data is inadvertently lost or destroyed such that a person may no longer have access to it – referred to as an availability breach. It also applies if personal data is inadvertently altered or modified so that it is no longer accurate – referred to as an integrity breach. As a result, if a situation arises in which data is destroyed or altered, notification may be required pursuant to the GDPR ***even if*** the data was not

accessed or acquired by an unauthorized party – a result that would not be required under current U.S. laws.

If your organization is regulated by the GDPR, you may have notification obligations if you are serving as a processor of personal data for another company, or if you are a joint controller.

While the definitions under the GDPR are more expansive than U.S. law, the GDPR does not require notification in the event of every breach. Instead, notification to the supervisory authorities – the EU regulators – must be made only if the breach results in a risk to the rights and freedoms of individuals. If notification is required, the breach must be reported to the relevant supervisory authorities within 72 hours of becoming aware of it. This is the opposite of U.S. law, which requires regulator notification only if individuals will be notified.

In contrast, in the EU, the standard for notification to the individuals themselves is higher – the breach must result in a "high risk" to the rights and freedoms of individuals, and the 72-hour requirement does not attach to individual notice. Instead, the GDPR recognizes that notification to the individuals likely will take longer, and it requires that communication to impacted individuals should be made as soon as reasonably feasible.

If a company is required under the GDPR to notify individuals of a data breach, the communication should describe in clear and plain terms and in the native language of the recipient the following:

1. A description of the nature of the breach;

2. The name and contact details of a data protection officer or other contact point;

3. A description of the likely consequences of the breach; and

4. A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Should an organization decide notification is not required, the GDPR provides that the breach be documented in the company's records. Since the GDPR took effect on May 25, 2018, supervisory authorities in the various EU member states have seen an influx of breach reporting by companies. While the law is still in its infancy and how regulators will enforce compliance, particularly against companies lacking an EU physical presence remains to be seen, organizations subject to its jurisdiction are well advised to ensure that the GDPR is closely analyzed in the event of a breach.

G. Breaches Outside the US or EU

Other countries are increasingly regulating the use and unauthorized disclosure of PII or personal data. Brazil, for example, recently enacted its own legislation parallel to the GDPR which contains breach notification requirements. Canada recently expanded its data security laws to include additional breach notification requirements. If your organization does business in multiple countries, you should review the laws of those countries and include the timing and notification requirements in your organization's incident response plan.

H. Unique Issues Relating To Payment Card Breaches

Additional considerations should be analyzed when an organization is affected by a breach involving payment card information (***e.g.,*** debit or credit cards). According to one study, the retail, hospitality, food and beverage, and health care industries are most vulnerable to attacks involving payment card information, whether that be through a physical card reader or through e-commerce.[18] If your organization accepts payment cards, and card information is the subject of a data breach, you may have additional obligations to notify your payment processor, merchant bank, or the payment card brands.

Visa and Mastercard cards are processed through a four-party system. Visa and Mastercard enter into licensing arrangements with various financial institutions called "issuing banks" that

---

[18] Trustwave Holdings, Inc., Trustwave Global Security Report (2019) ***available at*** https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/

issue payment cards to cardholders. The issuing bank collects payment from the cardholders through their monthly payment card statements or via withdrawal from their bank account where debit cards are used. Retailers or merchants who accept Visa or Mastercard contract with other financial institutions called "merchant banks." Merchant banks and retailers in turn typically enter into contracts with payment card processors to process the card transaction and collect payment from a cardholder's issuing bank.

In the four-party system, the merchant banks have contracts with Visa or Mastercard and agree to follow Payment Card Industry Data Security Standards (PCI DSS). A merchant bank will typically have a separate contract with a merchant (directly or through a payment processor) that, in turn, requires the merchant to indemnify the merchant bank if there is a data breach and Visa or Mastercard imposes a liability assessment on the bank or processor. Accordingly, an organization impacted by a payment card breach usually is required to notify its merchant bank or payment processor within 24 hours of discovering the breach. The merchant bank is then required to notify Visa or Mastercard.

The Payment Card Industry has set forth a specific set of guidelines that often are incorporated in the various payment card contracts and must be followed in the event of a suspected incident involving payment card data. An organization should review both its contracts with the merchant bank or payment processor and the PCI rules on breach notification to ensure compliance. The PCI rules may require that the merchant retain, at its own cost, a PCI-certified forensic investigator to investigate the breach and determine whether the merchant's security systems were in compliance with PCI requirements. **Tip: An organization may wish to retain, through its legal counsel, a private forensic investigator to do its own**

parallel investigation, since the PCI investigator is required to report its findings to the payment card brands. The private investigator will provide the organization with the ability to contest the PCI investigator's findings.

Discover and American Express transactions are processed through a three-party system. Discover and American Express typically contract directly with a merchant who accepts those cards. In the event of a breach involving those brands, the merchant should consult its contracts with Discover and American Express and any regulations issued by those brands and follow all notification requirements. Generally, notification is required to be made to the brands immediately or within 24 hours.

Merchants should be advised that the brands may request or require prior review of any breach notification letters that will be sent to affected consumers.

CONCLUSION

Planning how your organization will respond to a security breach is essential, but it is manageable. As the data security laws are evolving and changing almost as quickly as the threats to an organization's data, in-house counsel plays a vital role in helping an organization respond quickly and efficiently when a breach occurs.

Bryan Cave Leighton Paisner LLP

With over 1,400 lawyers in 31 offices across North America, Europe, the Middle East and Asia, Bryan Cave Leighton Paisner LLP is a fully integrated global law firm that provides clients with connected legal advice, wherever and whenever they need it. The firm is known for its relationship-driven, collaborative culture, diverse legal experience and industry-shaping innovation and offers clients one of the most active M&A, real estate, financial services, litigation and corporate risk practices in the world.

bclplaw.com