DATA SECURITY BREACHES

INCIDENT PREPAREDNESS AND RESPONSE

Jena Valdetero
David Zetoony
Bryan Cave LLP

Foreword
The Honorable Maureen K. Ohlhausen
Commissioner, Federal Trade Commission

Preface
Lisa Clapes
Vice President, Corporate Counsel & Chief Privacy Officer
Ceridian HCM

WASHINGTON LEGAL FOUNDATION
Washington, D.C.

This Monograph is one of a series of original papers published by the Legal Studies Division of the Washington Legal Foundation. Through this and other publications, WLF seeks to provide the national legal community with legal studies on a variety of timely public policy issues. Additional copies of this Monograph may be obtained by writing to the Publications Department, Washington Legal Foundation, 2009 Massachusetts Avenue, N.W., Washington, D.C. 20036.

Other studies in the WLF Monograph series include:

The View from the Front Lines: Litigation Under the False Claims Act in a New Era of Enforcement by Kristin Graham Koehler and Brian P. Morrissey, Sidley Austin LLP. Foreword by Jay B. Stephens, Raytheon Company. 2013. Library of Congress No. 2013931282

Erasing Intellectual Property: "Plain Packaging for Consumer Products and the Implications for Trademark Rights by Patrick Basham and Dr. John Luik, Democracy Institute. 2011. Library of Congress No. 2011923316.

Litigate the Torts, Not the Mass: A Modest Proposal for Reforming How Mass Torts Are Adjudicated by John H. Beisner and Jessica D. Miller, Skadden, Arps, Slate, Meagher & Flom LLP. Foreword by the late Professor Richard A. Nagareda, Vanderbilt University Law School. 2009. Library of Congress No. 2008936371.

A Framework for Toxic Tort Litigation by Joe G. Hollingsworth and Katharine R. Latimer, Spriggs & Hollingsworth. Foreword by Dorothy P. Watson, Novartis Pharmaceuticals Corporation. 2008. Library of Congress No. 2008923597.

Science Through the Looking Glass: The Manipulation of "Addiction" and its Influence Over Obesity Policy by Dr. John C. Luik. Foreword by Daniel J. Popeo, Washington Legal Foundation. 2007. Library of Congress No. 2007931992.

Waiver Of The Attorney-Client Privilege: A Balanced Approach by The Honorable Dick Thornburgh, Kirkpatrick & Lockhart Preston Gates & Ellis LLP. Foreword by The Honorable John Engler, President and CEO, National Association of Manufacturers. Introduction by Laura Stein, Senior Vice President – General Counsel and Corporate Secretary, The Clorox Company. 2006. Library of Congress No. 2006927395.

Library of Congress Control No. 2014953079

DATA SECURITY BREACHES

INCIDENT PREPAREDNESS AND RESPONSE

Jena Valdetero
David Zetoony
Bryan Cave LLP

Foreword
The Honorable Maureen K. Ohlhausen
Commissioner, Federal Trade Commission

Preface
Lisa Clapes
Vice President, Corporate Counsel & Chief Privacy Officer
Ceridian HCM

WASHINGTON LEGAL FOUNDATION
Washington, D.C.

TABLE OF CONTENTS

ABOUT THE AUTHORS

Jena Valdetero is a partner at the law firm Bryan Cave LLP where she serves as the head of its data breach response team. She has provided counseling to dozens of clients in connection with data privacy and security issues. She is a Certified Information Privacy Professional, U.S. (CIPP/US), by the leading privacy trade organization, the International Association of Privacy Professionals. 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 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 is the author of a leading handbook on data security—the Better Business Bureau's *Data Security Made Simpler*—and the leading quarterly report on data privacy and security class-action litigation. He represents clients from a variety of industries ranging from national department stores to international outsourcers.

FOREWORD

By
The Honorable Maureen K. Ohlhausen
Commissioner, Federal Trade Commission[1]

We live in an era where nearly every business, large or small, has some private data about its customers, and many companies store large amounts of such data. Unfortunately, our world contains those who would act unethically and illegally to access such private information. Security breaches can cost companies tens of millions of dollars in reputational damage, lost business, damage awards, legal fees, and penalties. It is no surprise, then, that companies generally want to keep their consumers' data secure.

At the Federal Trade Commission (FTC), we share the goal of keeping consumer data secure. And we use a number of tools to move toward that goal. For example, we work hard to educate consumers and businesses about safe practices in handling consumer data.[2] We also serve as backstop enforcer to various industry self-regulation efforts.

In addition, the FTC seeks to secure consumer data by enforcing companies' legal obligations to their customers. For example, the Commission's Safeguards Rule[3] imposes data security requirements on financial institutions, and the Fair

[1]Maureen K. Ohlhausen is a Commissioner of the Federal Trade Commission. The views expressed here are her own and do not represent the views of the Commission.

[2]*See, e.g.*, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS, http://www.business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf.

[3]FTC Safeguards Rule, 16 C.F.R. § 314 (2013).

Credit Reporting Act requires credit-reporting agencies to use reasonable procedures to ensure that recipients of sensitive consumer information have a permissible purpose for receiving that information.[4] In addition to these industry-specific laws, we enforce Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer harm.[5] Under these statutes, we have initiated more than fifty data security cases.

The touchstone of the FTC's data security enforcement under Section 5 is reasonableness: a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities. Using this approach, the Commission challenges practices that are unreasonable in light of the full range of circumstances. The FTC recognizes that there is no such thing as perfect security, no one-size-fits-all data security program—and that the mere fact that a breach occurred does not mean that a company has violated the law. Reasonable security requires assessing and addressing risks in a continuous process. Our enforcement typically focuses on instances where there are systemic failures in a company's data security processes rather than on single, standalone problems.

The following WLF Monograph is a useful guide to the role of in-house counsel in the continuous process of data security. Although written by lawyers, the WLF Monograph is not—to the authors' great credit—a legal treatise. Instead, it is a

[4]Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2006).

[5]15 U.S.C. § 45.

practical guide to help in-house counsel understand security incidents and the role of in-house counsel in dealing with such incidents.

The WLF Monograph describes a useful taxonomy of security events, security incidents, and security breaches. It then discusses what issues in-house counsel should consider prior to any incident occurrence. I found the checklists for evaluating cyber security insurance policies, written information security programs (WISPs), and incident response plans to be concrete and particularly useful.

The largest section of the WLF Monograph outlines step-by-step best practices for security incident response. This section is full of practical advice about how investigators of a security incident can effectively work across an organization. For example, one subsection discusses the importance of coordinating with the IT department to preserve evidence while isolating the compromised systems. As the authors point out, investigators may require such evidence to determine if a security incident resulted in a breach. This section also contains a helpful analysis of the key provisions of state data breach notification laws.

Overall, I believe this WLF Monograph will be a useful reference for in-house counsel as they prepare for and encounter security incidents. Businesses will benefit from the advice herein. More importantly, this advice will ultimately benefit the consumers whose data businesses hold in their care. I thank the authors for their hard work in writing this excellent reference.

PREFACE

By
Lisa Clapes*

In December 2009, an unknown party from outside the United States hacked into one of Ceridian's payroll applications and exposed the personal information of a number of individuals. Ceridian quickly notified impacted individuals and took steps to make sure that they were protected from the misuse of the information. Nonetheless, Ceridian has spent the last five years reflecting on the incident and, as always, fine tuning our practices.

As the WLF Monograph describes, there are, inevitably, three universal truths when it comes to data security.

First, in this day and age, all companies are subject to attack—there are no exceptions.

Second, no matter how good a security system is, it would be a mistake to assume immunity. Ceridian has a comprehensive information security program, which is fully documented in writing, and contains administrative, technical, and physical safeguards to help protect the data entrusted to us. After the 2009 breach, Ceridian voluntarily agreed to retain an independent third party to conduct biannual assessments of our security program to verify that it is reasonably designed to protect the security, confidentiality, and integrity of the personal information that we collect. The independent review makes sure that our system keeps up

*Lisa Clapes is Vice President, Corporate Counsel, and Chief Privacy Officer of Ceridian HCM. Ceridian HCM, headquartered in Minneapolis, is a leader in human capital management with offices in the U.S., Canada, and the United Kingdom.

with the latest threat vectors, prevention technologies, and organizational best practices. The result is that our security program is examined and audited, both internally and externally, to a level of scrutiny that exceeds that of many companies in any industry. Nonetheless, as the WLF Monograph explains, regardless of how expertly a security system might guard against all known vulnerabilities and attack vectors (a herculean task in and of itself), it is by definition impossible to guard against vulnerabilities about which nobody is currently aware, such as zero-day exploits.

Third, although criminals are responsible for breaches, as the WLF Monograph describes, the victimized business typically suffers reputational, legal, and other consequences in the aftermath of a breach.

In a world in which attacks are relentless and even the best security systems are not guaranteed to prevent a breach, and in which companies are held to task for the actions of third-party hackers, what ultimately differentiates one company from another is its ability to manage an incident. The WLF Monograph can be an invaluable tool for thinking about how to manage an incident in advance, and an invaluable resource manual for in-house counsel and chief privacy officers as they navigate live incidents.

DATA SECURITY BREACHES:
INCIDENT PREPAREDNESS AND RESPONSE

by
Jena Valdetero
David Zetoony
Bryan Cave LLP

INTRODUCTION

Media reports about data security breaches have become an almost daily occurrence. Increased publicity reflects the simple fact that data breaches have grown in frequency and scope. Although statistics vary, last year there were approximately 1,465 incidents involving data loss and, according to one watchdog group, those incidents impacted over 257 million consumer records.[1] Consumers, regulators, shareholders, and business partners or affiliates are scrutinizing whether organizations that suffer a data security breach had adequate security before the breach occurred, and are critically examining how an organization prepares for, investigates, and responds to a security incident. Instances in which stakeholders believe that the organization's preparation or response was inadequate have led to litigation, regulatory investigation, erosion of customer base,

[1] *See* Privacy Rights Clearinghouse Chronology of Data Breaches, *available at* https://www.privacyrights.org/data-breach (referencing the number of records involved in publicly reported data breaches) (last viewed July 16, 2014); DataLossdb Open Security Foundation, Data Loss Statistics, *available at* http://datalossdb.org/statistics?utf8=%E2%9C%93&timeframe=last_year (referencing data security incidents).

and, increasingly, changes in management.[2] Given this context, it is not surprising that when board members and general counsel are asked "What keeps you up at night?" the answer is frequently: "data security."[3]

In order to effectively respond to a data security incident, in-house counsel must understand what a "security incident" entails, what the organization should do to prepare itself before an 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, and public scrutiny.

This WLF Monograph 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 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 how in-house counsel can 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

[2]*See, e.g.,* Tiffany Hsu, "Target CEO Gregg Steinhafel Steps Down in Wake of Huge Data Breach," L.A. TIMES (May 5, 2014); Danielle Abril, "Sally Beauty to Replace Its CEO, Incurs $1.1M Cost from Data Breach," DALLAS BUS. J. (May 1, 2014).

[3]Data security was the second most common response for both board members and general counsel, after succession planning and regulatory compliance respectively. FTI, *Law in the Boardroom* (2013), *available at* http://www.fticonsulting.com/global2/media/collateral/united-states/law-in-the-boardroom.pdf.

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 refers to a subset of such situations—where there is evidence of an unauthorized "acquisition" of and/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, do not in fact meet the *legal* definition of the term. For the purpose of clarity, this WLF Monograph uses three separate 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 to 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 resets 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 counts as 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."[4] As discussed in this WLF Monograph, security incidents almost always necessitate that an entity conduct a thorough investigation to test the suspicion that personal information was improperly accessed or acquired.

Security incidents impact all types of entities. Two non-profit organizations—Privacy Rights Clearinghouse and the

[4]David Zetoony, ed., Council Of Better Business Bureaus, Data Security Guide: Data Security – Made Simpler: Common Technical and Legal Terms – A Glossary, *available at* http://www.bbb.org/data-security/common-technical-and-legal-terms/overview/.

Open Security Foundation—systematically track publicly reported security incidents and breaches and provide up-to-date reports on evolving trends.[5] According to the latter source, approximately 50% of incidents impact for-profit businesses, 17% impact government agencies, 17% impact medical providers and institutions, 8% impact educational institutions, and 9% impact other types of entities including non-profits.[6]

Security incidents are attributable to a variety of different causes—sometimes referred to as "attack vectors." While approximately 65% are caused by third parties, approximately 25% are a direct result of employees within an organization.[7] Insider-caused incidents are split nearly evenly between those that are accidental (*e.g.,* an employee inadvertently emailing a file that contains sensitive information to the wrong party) and those that are malicious (*e.g.,* an employee stealing customer information). The number of security incidents attributable to employee actions has remained relatively constant over the past ten years,

---

[5]*See* https://www.privacyrights.org/content/about-privacy-rights-clearinghouse and http://www.opensecurityfoundation.org/. In addition, several consulting 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 upon non-public data (*i.e.,* incidents that may not have turned into breaches or that were not publicly reported). *See, e.g.*, Verizon 2014 Data Breach Investigation Report, *available at* http://www.verizonenterprise.com/DBIR/2014/ (last viewed July 17, 2014).

[6]*See* DataLossdb Open Source Foundation, Data Loss Statistics, *available at* http://datalossdb.org/statistics?utf8=%E2%9C%93&timeframe=last_year (referencing data security incidents from 2013). *See also* Verizon 2014 Data Breach Investigations Report.

[7]*See* DataLossdb Open Source Foundation, Data Loss Statistics, *available at* http://datalossdb.org/statistics?utf8=%E2%9C%93&timeframe=last_year (referencing data security incidents from 2013).

whereas the number of third-party attacks—particularly computer hacking, malware, and social engineering—has risen sharply.[8]

C. Security Breaches

As discussed above, a data "security breach" is a legally defined term. The definition varies depending upon the federal or state 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 increased the possibility that a consumer might be harmed by the disclosure. In the laptop example provided above, if an organization determines that the laptop was stolen and it contained unencrypted social security numbers, the incident would also fall under the definition of a "security breach." As discussed below, security breaches almost always dictate that an organization consider the legal requirements of federal and state breach laws.

Data breaches typically impact organizations in a number of ways. Those impacts fall into the general categories summarized below:

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

[8] *See* Verizon 2014 Data Breach Investigation Report, *available at* http://www.verizonenterprise.com/DBIR/2014/ at 9 (last viewed July 17, 2014).

- 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 (*e.g.,* an eCommerce site), removing or decommissioning an affected system may have a direct impact on the organization.

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

- Contractual Costs: An organization may be contractually liable to business partners in the event of a data security breach. For example, a breach involving a retailer's electronic payment system will typically trigger obligations under the retailer's agreements with its merchant bank and/or its payment processor. Those obligations may include, among other things, the assessment of significant financial penalties.

- Notification Costs: If an 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 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 and/or whether an organization properly investigated and responded to it. In addition, some regulatory agencies are empowered to impose civil penalties or monetary fines in the event that they determine an organization's security practices were unreasonable or that an 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: The best available data indicate that approximately 4% of publicly reported data security breaches result in the filing of a federal putative class-action lawsuit. Although most such suits to date have not resulted in a finding of liability, defense costs and settlement costs can be significant.[9]

II.

DATA SECURITY INCIDENT PREPAREDNESS

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

[9]Romanosky, *et al.*, *Empirical Analysis of Data Breach Litigation*, 11(1) J. OF EMPIRICAL LEGAL STUDIES (Mar. 2014) (analyzing 1,772 data breaches reported in the United States and determining that only 65 (3.7%) resulted in federal court litigation).

data and to prevent a breach from occurring. Such steps include instituting written information security programs that describe the security infrastructure of an organization, investing in defensive information technology resources, 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. The new rule of thumb is that it is not a matter of *if*, but rather *when*, a security breach will occur. From that vantage point, preparing in advance for how an organization will respond when a security incident or breach occurs has become essential.

Data security incident preparedness is a process that requires the participation of 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 and/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 and/or provide additional training to improve its response.

In addition to supporting an 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 may create. In-house counsel should also review the incident response plan to make sure that it takes into account 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 an organization's preparation for a possible breach.

A. Cyber Insurance

Only 31% of companies have purchased insurance that is specifically designed to cover part, or all, of the costs of a data security breach ("cyber insurance").[10] Other survey data indicate, however, that the majority of companies that do not have cyber insurance are considering its purchase within the next twenty-four months.[11]

Cyber-insurance policies differ dramatically 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 the organization from potential incident-related cost and liability. Policies may also 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 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

[10]Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis at 22 (May 2014).

[11]*Id.*

continue to align with changes in the legal landscape, coverage trends, and the organization's operations.

The following checklist provides to 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.

Forensic Investigators

□**Coverage**: Does the policy cover the cost of retaining a forensic investigator? If so, does it limit selection to a single investigator, or are there situations in which the policy would permit hiring multiple investigators if needed?

□**Sub-limit**: Does the policy have a sub-limit for forensic investigation-related costs? Is the sub-limit proportionate to the average cost of retaining a forensic consultant to investigate a data security incident? Would the sub-limit be sufficient if more than one forensic consultant must be retained?

□**Sub-Retention**: Does the policy have a sub-retention when hiring an investigator? If so, is the sub-retention well below the average cost of retaining a forensic investigator? If not, does the organization understand that the coverage will only provide protection for catastrophic incidents/breaches?

Consumer Notifications

□**Coverage**: Does the policy cover the cost of issuing notices to consumers? If so, does the coverage give the

organization the right to control how those notices are given (*e.g.,* in paper format versus in electronic format)? Does it require that the organization avail itself of "substitute notice" when permitted by statute? If so, does the organization understand that the policy may not pay for printing and mailing notification letters if the organization decides that issuing notifications in that manner is necessary to help protect the organization's reputation and brand?

□**Exclusions**: Does the policy exclude notifications that are not expressly required under a state data breach notification statute (*e.g.,* "voluntary" notifications)? If so, are there situations in which the organization might decide to issue voluntary notices in order to limit reputational damage or decrease the likelihood of a class-action filing? Does the organization understand that those notices may not be covered under the policy?

□**Sub-limit**: Does the policy have a sub-limit for the total costs in issuing consumer notifications or the total number of consumer notices for which the policy will provide reimbursement? If so, is the sub-limit proportionate to the quantity of consumers about which the organization maintains personal information?

□**Sub-retention**: Does the policy have a sub-retention for either the cost of issuing consumer notifications, or the number of consumer notices that must be paid for by the organization? If so, is the sub-retention well below the total quantity of consumers about which the organization maintains personal information?

Credit-Monitoring-Related Services

□**Coverage**: Does the policy cover the cost of providing credit monitoring (*i.e.,* monitoring consumers' credit reports for suspicious activity), identity restoration services (*i.e.,* helping consumers restore their credit or close fraudulently opened accounts), and identity-theft insurance (*i.e.,* defending consumers if creditors attempt to collect upon fraudulently opened accounts and reimbursing consumers for any lost funds) to consumers who may be impacted by a breach?

□**Exclusions**: Does the policy exclude credit-monitoring-related services where providing them is not "required" by law. If so, given the fact that there are currently no statutes that formally require credit monitoring services to be offered, is anything of value really being provided to the company under the policy?

□**Paneled providers**: Does the policy require the organization to use a certain company to provide credit-monitoring-related services? If so, does the organization have a relationship with a different provider? Does the provider that is listed on the panel have a history of consumer complaints? Does it have a history of alleged unfair or deceptive trade practices? Must the provider, or the organization's insurer, indemnify it for any consumer complaints concerning credit monitoring services that the organization offers?

□**Sub-limit**: Does the policy have a sub-limit for the total cost that it provides for credit monitoring? If so, is the sub-limit proportionate to the average cost of providing credit monitoring multiplied by the quantity of consumers about which the organization maintains personal information?

□**Sub-retention**: Does the policy have a sub-retention? If so, is it well below the average cost of providing credit monitoring multiplied by the quantity of consumers about which the organization maintains personal information?

Regulatory Proceedings

□**Coverage**: Does the policy cover regulatory proceedings that may result from a breach? If so, does the coverage extend to legal fees incurred in a regulatory investigation or regulatory proceeding? Does it also cover the fines or civil penalties that may be assessed as a result of a proceeding?

□**Exclusions**: Does the policy exclude investigations brought by agencies that are likely to investigate the organization? For example, if the organization is under the jurisdiction of the Federal Trade Commission, does the policy exclude investigations brought by the FTC? Does the policy exclude coverage for investigations brought by state regulators under certain types of state statutes (*e.g.,* state consumer protection statutes or state unfair or deceptive trade practices statutes)?

□**Sub-limit**: Is the sub-limit proportionate to the average cost of defending a regulatory investigation and/or the average cost of the fines assessed to other organizations in the same industry?

□**Sub-Retention**: Does the policy have a sub-retention for the cost of a regulatory investigation? If so, is the sub-retention well below the average cost of regulatory penalties and fines? If legal fees incurred in a regulatory investigation are covered, is the sub-limit well below the legal fees that the organization would expect?

Contractual Liabilities

□**Coverage**: Does the policy cover contractual liabilities that result from a data security breach? In particular, 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? These are sometimes referred to as Payment Card Industry (PCI) fines or assessments.

□**Exclusions**: Does the policy exclude any types of contractual liability such as PCI fines or contracts that the organization may have with end-use consumers?

Legal Assistance

□**Coverage**: Does the policy permit the organization to retain an attorney to help the organization investigate and document an incident, retain investigators if needed, review contracts with service providers, identify statutory obligations to notify consumers and regulators, and advise the organization concerning steps that may reduce the likelihood of a class-action lawsuit or regulatory investigation? Does the policy cover legal expenses incurred in defending all types of claims?

□**Exclusions**: Does the policy exclude coverage for lawyers to provide assistance concerning some aspect of a security breach response? For example, does a policy exclude coverage if the organization's attorney attempts to negotiate or settle contractual claims, or has to deal with government regulators? Does the policy exclude claims asserting legal theories that are common in class actions (*e.g.* consumer fraud or deceptive practices claims)?

□**Paneled providers**: Does the policy require that the organization use a specific law firm or provide a panel of firms? Does the organization have relationships with any of the firms that are on the panel? If not, has the organization done due diligence concerning its experience in handling data security breaches? Has it investigated whether the firm has taken legal positions that might benefit the insurer, but be inconsistent with the organization's ability to obtain coverage under the policy?

B. Written Information Security Program

After a security breach occurs, customers, the media, regulators, and other interested parties routinely ask whether the organization took reasonable and appropriate measures to prevent the breach in the first place. In-house counsel should consider, therefore, whether the organization would be able to produce documents that demonstrate that it was attempting to secure the information. Many outside observers will expect that these measures include, at a minimum, a written information security program or "WISP."

The format and contents of a WISP depend greatly on the industry in which an organization operates. Put differently, the WISP of a small non-profit typically looks very different from the WISP of a large, multinational financial institution. Nonetheless, there are areas of commonality. Although in-house counsel should be aware of regulations and standards that apply to an organization's specific 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

C. Incident Response Plan

In addition to the topics discussed above, consider including within the WISP an 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 the other people within the organization with whom they should be coordinating. The plan can also help educate employees concerning what they should and should not do when faced with a security incident, and it 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 counsel draft an incident response plan or evaluate the thoroughness of one that already exists:

□**Definition of Security Event, Incident, and Breach**: Consider explaining the differences between an event, incident, and breach so that everyone in the organization understands the distinctions.

□**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 how an event is escalated to be considered an incident, or a breach, as well as the criteria that govern such a decision. In addition, a plan should specify 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 to conduct the investigation under the auspices of the attorney-client and attorney work product privileges. If so, the plan should make clear that the investigation must operate under the direction of counsel and 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.

□**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.

□**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, etc.

□**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 for 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 feedback might include "lessons learned" from how an incident was handled or ways to prevent an incident from occurring again.

D. Contractual Obligations to Business Partners

In situations in which a security incident involves data that is wholly owned by the organization, there may be few, if any, obligations for the organization to notify business partners or affiliates. Often, however, business partners or affiliates may have an interest in the information impacted. For example, if an incident involves data of another entity for which an organization is performing services, it may have an obligation in its service agreement 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 an organization received from consumers, the organization's agreement with its payment processor or merchant bank may similarly require that it 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 an organization may have to business partners or affiliates. 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 in-house counsel is evaluating an existing response plan, or an organization does not have an incident response plan when an incident is identified, the steps that follow outline best practices that take into account possible legal requirements and obligations. Among other things, these recommendations cover 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 kinds 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 or risk management specialist. 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.

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 protection 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 who 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 information technology ("IT") or human resources ("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.

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 information technology/information services, legal/risk team management, operations, marketing/communications, and human resources (if the breach involves employee misconduct or employees' personally identifiable information). 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 dotted 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. If the IT department of the organization has relatively little experience with investigating security incidents, do not necessarily assume that it 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, for example, 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. 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, or software 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 before any evidence is lost or inadvertently destroyed—and recommend that the organization utilize external resources to help collect and preserve electronic evidence and investigate the incident.

When retaining a forensic investigator, 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. Among other things, 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 (*i.e.,* how information was "exfiltrated"). The investigator may also be able to help in-house counsel coordinate with law enforcement efforts to catch a perpetrator.

When retaining a forensic investigator, remember that it will be given access to the organization's networks and that there is a high likelihood that, if a breach occurred, the investigator may gain access to sensitive personal information as part of its investigation. As a result, counsel should review the agreement between the investigator and the organization carefully to make sure that the investigator agrees to apply the security warranted for the type of information to which it may gain access.

B. Coordination with Data Owners

Organizations are relying increasingly on vendor agreements to carry out various business operations. These agreements may authorize the organization or the vendor to have access to or to 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 likely has a legal obligation to notify its client, who in turn will have an obligation to notify the affected persons.

Therefore, 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 state 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 the costs of notification.

C. Communication to the Public/Media

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

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

As discussed in Section E below, state and federal laws may require an organization to notify consumers and/or the media within a certain time after discovering a breach. There may be significant advantages to notifying consumers as early as is practical for an organization. The sooner consumers 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 victims of identity theft or other fraud. For example, early informed consumers 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 consumers from becoming victims of fraud, they also reduce the likelihood that the consumer will sue an organization for damages allegedly incurred by the breach. Early notification may also reduce the likelihood that regulators will allege that the organization did not comply in a timely fashion with data breach notification laws.

While early notification can be beneficial to consumers and organizations in some situations, premature notification in other situations can harm both interested parties. 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. 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 inaccurate information initially provided by an organization can be both difficult and time consuming, and it can deflect the organization's resources and attention from responding to the breach itself.

There is an additional potential drawback to prematurely notifying consumers of a security breach. If an investigation has not determined how a third party obtained information, the identity of the third party, 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, further threaten the organization's networks, cause the culprit to delete or remove evidence, or cause the culprit to exfiltrate information about additional consumers before the point of infiltration has been identified and remediated.

Once the organization has decided upon 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 two communications channels should be considered:

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

- Social Media: To the extent that an organization desires to disseminate information quickly, it 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. For example, an organization may decide that it is in the best interest of consumers, and the public, to wait until its investigation is complete and the organization is in a position to provide accurate information. However, the media may learn about a breach from a business partner, a government agency, a consumer, or a disgruntled employee. When this occurs, an organization may see information concerning the breach disseminated in the media without its knowledge or input or be asked by the media to comment about the breach. Counsel should be prepared for this to occur and 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 an 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 upon 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 upon 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 creates a potential opportunity for the media to produce 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 the 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, that person 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. Among other things, contacting law enforcement may help stop the criminal behavior or lead to useful information that may assist the organization's investigation of the incident, or the government's prosecution of the culprit. It may also show the public that the organization was diligent in investigating the incident and taking steps to protect consumers.

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 involved the electronic exfiltration of information. For security incidents that involve paper records or known individuals (*e.g.,* employees or former employees), in-house counsel might also consider contacting municipal law enforcement in the jurisdiction in which the individual resides or works.

E. Communication with Affected Consumers

Although Congress has attempted to agree on federal data breach legislation, as of the publication date of this WLF Monograph, there is no national data breach notification law. Instead, 47 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 personally identifiable information ("PII"). The only states without such laws are Alabama, New Mexico, and South Dakota, although their citizens may be covered by the data breach laws of other states.

While the state data breach laws are not uniform, the laws are more similar than not. The following summarizes the key provisions of state data breach notification laws and highlights areas in which 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. Do the state laws apply?

As a general rule, if an organization maintains or transmits personally identifiable information belonging to citizens of a particular state, it 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 of the breach so that it may fulfill its notification obligations. In addition, several states' laws do not apply to organizations that are subject to federal regulation, such as under the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act.

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's statute specifically applies to Texas residents and residents of other states. The language of these statutes arguably would cover notification to residents of the three states that have not yet passed notification laws—Alabama, New Mexico, and South Dakota.

2. What personally identifiable information triggers notification?

The statutes generally require notification in the event of breaches involving the following information: the consumer's name in combination with his or her social security number, driver's license number, account number, or access code. Some states go even further and require notification in the event other types of information are accessed or acquired. For example, Iowa, Nebraska, North Carolina, and Wisconsin all 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. Arkansas, Missouri, Puerto Rico, and Texas

require notification if certain medical or health information is at issue.

California amended its statute in January 2014, and became the first state to require consumer 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. However, California permits notification to be electronic for such breaches only. The electronic notification should direct the person whose personal information has been breached to promptly change his or her password and security question and answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question and answer. To date, Florida has enacted similar changes to its data breach notification statute. Whether other states will follow California and Florida remains to be seen.

The state statutes provide that breach of personal information that is publicly available does not give rise to a notification requirement. Similarly, the breach of personal information that is encrypted 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 to 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.

3. How quickly must the organization notify affected consumers?

Most of the state statutes do not strictly define the timing by which notification must occur. Only a few states prescribe specific deadlines (*e.g.,* Wisconsin (45 days) and Florida (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 the organization to delay notification if law enforcement determines that notice to individuals would interfere with a criminal investigation. If an organization intends to delay notification based upon a request by law enforcement, in-house counsel should consider obtaining written confirmation of that request to explain any delay at a later time.

4. 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 in what the states require, each individual statute should be examined in connection with reporting a breach.

Massachusetts's 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 multi-state breach, in-house counsel should consider whether Massachusetts residents should receive a slightly modified notification letter. In addition, Massachusetts and Illinois both prohibit companies from providing in the notice the number of those states' residents impacted by the breach.

5. How must an organization notify affected consumers?

The majority of states require that consumers be notified in writing. Email notice can provide substantial cost 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 an organization is considering providing email notice, counsel should consider the risk that third parties may attempt to create fake electronic messages that appear to originate from the 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 consumers' computers, or to send personally identifiable information 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 they do send that the company will never request that consumers transmit additional personally identifiable information 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, and/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 and/or the number of persons to be notified is large. 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 sensitive

personal information 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.

6. 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 situations in which an organization may choose to voluntarily notify consumers. For example, although California and Florida currently are the only states in which notification is required for a breach of electronic account usernames/email addresses and passwords, if such a breach also involved consumers in other states, the organization might want to notify all affected persons for consistency's sake.

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.

7. 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 containing 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.

Also, 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 the statutes will require the organization to notify the data owner of the breach "immediately" or "as soon as possible." The obligations would then fall to the data owner to comply with the consumer notification requirements of the various state statutes.

In addition, about one-third of the states have a requirement that the state government (usually the Attorney General's office) must 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 a breach impact a minimum number of residents before state government notification becomes necessary. For example, New York requires government notification in a breach involving any number, while Hawaii, Missouri, and South Carolina only require state government notification if a 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. At least Indiana, North Carolina, and New York all have forms prepared by the state for use in notifying the state government of a breach, and these forms are available online. In the event of a multi-state breach, each

statute should be carefully examined to ensure full compliance.

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

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 offer credit monitoring.

Organizations that choose to offer one or more of these services also face the question how long to offer each service. Durations typically range from one 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. California is the first state to have such a requirement, and other states may follow in its footsteps.

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 on the credit account, a name and credit card number alone are insufficient to attempt to open a new financial account, and

charges on an existing account are unlikely to be spotted by credit monitoring.

Although credit monitoring may not be connected to the risks attendant many breaches, offering credit monitoring in connection with breaches involving sensitive personal information has arguably become an industry standard practice. An organization should thus consider whether a failure to offer the service—even if unconnected to the breach—could be misunderstood by consumers or regulators as a failure by the company to adequately protect consumers.

If an organization chooses to offer credit monitoring, identity restoration services, and/or identify-theft insurance, in-house counsel should carefully consider the vendors that they select to provide the services and the contractual limitations on those vendors. Specifically, vendors (and by extension the breached organizations that retained them) have been criticized for the following:

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

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

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

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

F. Issues Unique to Specific Types of Breaches

1. Payment card breaches

Additional considerations should be analyzed when the organization is affected by a breach involving payment card information (*e.g.,* debit or credit cards). If an organization accepts payment cards, and card information is the subject of a data breach, the organization may have additional obligations to notify its payment processor, merchant bank, and/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 issue payment cards to cardholders. Retailers or merchants who accept Visa or MasterCard contract with other financial institutions called "merchant banks" or payment card processors to process the card transactions and collect payment from a cardholder's issuing bank. 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.

In the four-party system, the merchant banks have contracts with Visa or MasterCard and agree to follow Payment Card Industry Data Security Standards. 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 upon the bank or processor. Accordingly, an organization affected 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 (PCI) has set forth a specific set of guidelines that are often 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. An organization may wish to retain, through its legal counsel, a private forensic investigator to do its own investigation, since the PCI investigator is often required to report its findings to the payment card brands.

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.

2. Breaches involving health information

If an organization handles consumer healthcare data, then it may be subject to the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the event of a breach. Although HIPAA is a federal law, it does not preempt state laws that provide even greater protection of patient information, so state laws may still need to be examined in the event of a breach involving protected health information (PHI).

PHI is defined as any individually identifiable health information that is: transmitted or maintained in any form or medium; is held by a covered entity or its business associate; identifies the individual or offers a reasonable basis for identification; is related to or received by a covered entity or any employer; and relates to a past, present or future physical or mental condition, provision of health care or payment for health care to that individual.

Entities that are directly covered under HIPAA include healthcare providers (*e.g.,* doctors or hospitals) that conduct certain transactions in electronic form, health plans (*e.g.,* health insurance companies), and healthcare clearinghouses (*e.g.,* third-party organizations that host, handle, or process medical information). HIPAA also creates obligations for "business associates." A business associate is any person or organization, other than a member of a covered entity's workforce, which performs services or activities for, or on behalf of, a covered entity, if such services or activities involve the use or disclosure of PHI. For example, business associates can include third-party claims administrators, billing agents, consultants, attorneys or accountants who provide services that involve access to PHI for a covered entity, or a medical record transcriptionist. HIPAA mandates that the covered entity contractually require the

business associate to comply with the privacy and security rules under HIPAA.

The HIPAA Breach Notification Rule[12] requires covered entities to provide notification of a breach involving PHI to affected individuals, the Secretary of the United States Department of Health and Human Services, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate. The timing of the notification to the Secretary depends on the number of persons affected by the breach. If the breach involves 500 or more persons, then the Secretary must be notified without unreasonable delay. For fewer than 500 persons, notification may be made on an annual basis.

Covered entities are also required to have in place written policies and procedures regarding breach notification, to train employees on these policies and procedures, and to develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

3. Breaches involving financial institutions

If the organization is a "financial institution," then the federal Gramm-Leach-Bliley Act (GLBA) imposes certain obligations regarding data privacy and security. The definition of "financial institution" under the GLBA is broad and applies to any U.S. companies that are "significantly engaged" in financial activities. This definition includes entities such as banks, insurance companies, securities firms, check cashing services, mortgage lenders, and more. GLBA authorizes the federal banking agencies, and the FTC (with

[12]45 CFR §§ 164.400-414.

respect to other financial institutions) to implement regulations to "protect against unauthorized access to or use of such records" that could "result in substantial harm or inconvenience to any customer."[13]

Banking entities are subject to the rules provided by the banking agencies under GLBA. Non-banking financial institutions are still subject to GLBA, but they are only required to comply with the statute and those rules promulgated by the FTC pursuant to the GLBA.

On March 29, 2005, the federal banking agencies published the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (the "Interagency Guidance").[14] The Interagency Guidance applies only to banks and directs them to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems."[15]

Among other things, a response program must include a procedure for notifying a bank's primary federal regulator "as soon as possible" when the bank becomes "aware of an incident involving unauthorized access to or use of sensitive customer information."[16] The Interagency Guidance further directs banks to require, by contract, that their service providers notify the bank "as soon as possible of any such

---

[13]15 U.S.C. § 6801(b)(3), 6804(a)(1) (2010).

[14]70 Fed. Reg. 15,736 (Mar. 29, 2005) (codified at 12 C.F.R. pt. 30, 12 C.F.R. pt. 208, 12 C.F.R. pt. 364, 12 C.F.R. pt. 568, and 12 C.F.R. 570).

[15]70 Fed. Reg. at 15,752.

[16] *Id*. at 15,740.

incident" to enable the bank to "expeditiously implement its response program."[17]

In addition to notifying its primary regulator, the Interagency Guidance also urges a bank to notify its customers in connection with those incidents where the bank determines that "misuse" of customer information "has occurred or is reasonably possible."[18] The Interagency Guidance provides banks with a minimum standard to follow when determining whether notifying customers of an incident is "warranted."[19] According to the Interagency Guidance, customer notification should occur following an "incident involving the unauthorized access or use of the customer's information" when a bank determines that "misuse" of customer information is "reasonably possible."[20] Although the Interagency Guidance does not define what situations constitute a "reasonable possibility" of misuse, it makes clear that "an institution need not notify customers if it reasonably concludes that misuse of the information is unlikely to occur."[21] The banking agencies also warn banks against notifying consumers when "misuse of information is unlikely" as such notification may cause consumers to be "alarmed needlessly."[22]

Unlike the banking agencies, the FTC has not promulgated a formal rule, regulation, or guidance that requires a financial institution under its jurisdiction to notify

---

[17] *Id*. at 15,739.

[18] *Id*. at 15,743.

[19] *Ibid*.

[20] *Id*. at 15,752.

[21] *Id*. at 15,743.

[22] *Id*. at 15,749.

either a business partner or a consumer in the event of an incident which involves the unauthorized access of information. However, as a general rule, non-banking financial institutions should consider notifying business partners and consumers in accordance with the Interagency Guidance.

CONCLUSION

Planning for how an organization will respond to a data security breach is essential—it is not a matter of if one will occur, but when. As the data security laws are evolving and changing almost as quickly as the threats to an organization's data, in-house counsel play a vital role in helping an organization respond quickly and efficiently when a breach occurs.

WASHINGTON LEGAL FOUNDATION

The Washington Legal Foundation was established in 1977 as a nonpartisan public interest law institution. Over the past 38 years, WLF has established itself as America's premier public interest law firm and policy center devoted to preserving and defending the nation's free enterprise system. WLF's litigation and educational activities directly target the forums where legal policies are made today: the judiciary, regulatory agencies, and the court of public opinion.

WLF's mission is to preserve and defend America's free enterprise system from excessive government intrusion through litigating and advocating in support of free market principles, limited and accountable government, individual and business civil liberties, and the rule of law.

To receive information about previous Washington Legal Foundation publications, contact Glenn G. Lammi, Chief Counsel, Legal Studies Division. Materials on WLF's other legal programs and activities may be obtained by contacting Constance C. Larcher, Chief Executive Officer, Washington Legal Foundation, 2009 Massachusetts Avenue, N.W., Washington, D.C. 20036.

WLF's LEGAL STUDIES DIVISION

The Washington Legal Foundation (WLF) established its Legal Studies Division to address cutting-edge legal issues by publishing substantive, credible publications targeted at educating policy makers, judges, the media, and other key legal policy audiences.

WLF's Legal Studies Division has deliberately adopted a unique approach that sets it apart from other policy centers.

First, Legal Studies deals almost exclusively with legal policy questions as they relate to the principles of free enterprise, legal and judicial restraint, and America's economic and national security.

Second, its publications focus on a highly select legal policy-making audience. Legal Studies aggressively markets its publications to: federal and state judges and their clerks; members of the United States Congress and their counsel; government attorneys; business leaders and corporate general counsel; law school professors and students; influential legal journalists; and major print and media commentators.

Third, Legal Studies possesses the flexibility and credibility to involve talented individuals—from law students and professors to federal judges and senior partners in established law firms—in its work.

The key to WLF's Legal Studies publications is the production of a variety of readable and challenging commentaries with a distinctly commonsense viewpoint rarely reflected in academic law reviews or specialized legal trade journals. Each publication is written to reach an intelligent reader who has no use for academic jargon.