ONCE MORE UNTO THE BREACH: HOW COUNSEL SHOULD HELP CLIENTS PREPARE FOR AND RESPOND TO DATA INCIDENTS

7/01/2016

Reprinted from California Busines Law Practitioner, copyright 2016 by the Regents of

AUTHORS

Sharon R. Klein
Partner | 949.567.3506

Alex C. Nisenbaum
Associate | 949.567.3511

NEWS view all

7/12/2016
Jan P. Levine Quoted in The Legal Intelligencer Article, 'Judge Approves $8.4M Settlement in Egg Class Action'

7/12/2016
Todd B. Reinstein Quoted in Bloomberg Article, 'Wells Fargo's Partial Tax Victory May Spur Billions in Refunds'

PUBLICATIONS view all

7/14/2016
Federal Circuit Finds That Use of a Contract Manufacturer Does Not Trigger the On-Sale Bar Provision

7/08/2016
Materiality Is the New Condition of Payment:

The statistics are staggering: In the last 4 years, the California Office of the Attorney General (COAG) received reports of 657 data breaches affecting 49 million records. In 2015 alone, 24 million records of Californians were affected by reported data breaches—that's three out of five Californians—according to the COAG's February 2016 Data Breach Report. California Data Breach Report (Feb. 2016), available at https://oag.ca.gov/breachreport2016 (COAG 2016 Breach Report).

Statistics like these show that data breaches can and will affect any organization. Today, it is not "if" but "when" your client will be the victim of a data breach. The legal and business consequences in terms of remedial costs, litigation, regulatory enforcement, and reputational harm have compelled businesses to focus on data privacy and security preparedness. The continued emergence of data as one of the most highly valued assets of the digital economy lends urgency to these preparations. Businesses increasingly are using the cloud—transferring data over vulnerable network connections and engaging in data analytics—and using targeted marketing and mobile and social media to increase a company's brand and reach.

Despite the growing risks and many high-profile breaches, there are still businesses that remain woefully underprepared. In a recent BDO survey of corporate directors, 55 percent of directors stated their company either did not have, or they were not sure whether their company had, an incident response plan in place. 2015 BDO Board Survey (Oct. 2015), available at https://www.bdo.com/getattachment/71efe245-f2b7–4106-bc25-c76b3d1d3244/attachment.aspx. Businesses that are unsure of whether they are prepared to handle data breaches and ongoing compliance with privacy and data security issues increasingly need guidance from legal counsel on the scope of their obligations with respect to cybersecurity.

Preparation is key. Although an organization may contact its legal counsel for the first time on data breach issues in the midst of an ongoing incident, a counsel's role in mitigating risk associated with these issues should begin well before an incident occurs. Applicable law and regulatory guidance make clear that an organization's responsibility for the privacy and security of data does not begin with discovery of a data incident. Rather, organizations that collect personal information have a legal responsibility to take reasonable steps to safeguard such information in their possession, and regulators are fining companies if proper measures have not been taken to prevent risk, not merely because a breach has occurred.

California law requires that a business "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect personal information from unauthorized access, destruction, use, modification, or disclosure." CC §1798.81.5(b). Other states have similar requirements. For example, Massachusetts requires organizations to implement and maintain a comprehensive written information security program. 201 Mass Code Regs §17.00 (2009). Federal

The Implied False Certification Theory After Escobar

EVENTS view all

July 18-20, 2016
Opal Financial Group, Family Office & Private Wealth Management Forum: The Race for Returns

July 20-21, 2016
2016 New York Venture Summit

WEBINARS view all

7/20/2016
Independent Contractor Classification: What to Do and Not Do After Uber

7/29/2016
The Role of Indemnity and Insurance in Business Litigation (Mechanicsburg, Simulcasts and Webcast)

PODCASTS view all

6/02/2016
Evolution of Blockchain for Investment Management Companies and Hedge Funds

6/01/2016
Exploring the Large Role of Successor Liability in Bankruptcy Cases

BLOGS view all

7/09/2016
Status Quo At The PTAB for Now: Supreme Court Makes No Changes to IPR Practice

7/06/2016
Court of Federal Claims Rules Contracting Officer's Failure to Exercise Independent Business Judgment Renders Partial Termination for Conveniencea an Abuse of Discretion and Breach, but Holds Subsequent Termination for Cause of Remainder of Contract to Be Appropriate

laws, such as the Gramm-Leach-Bliley Act (GLBA) (Pub L 106–102, 113 Stat 1338) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub L 104–191, 110 Stat 1936), mandate general security requirements for financial services organizations and health care organizations, respectively. In addition, the Federal Trade Commission (FTC) has pursued a number of enforcement actions alleging "unfair" trade practices under section 5 of the Federal Trade Commission Act (FTC Act) (15 USC §45) against companies for failure to employ adequate cybersecurity safeguards. See, e.g., *FTC v Wyndham Worldwide Corp.* (3d Cir 2015) 799 F3d 236. Accordingly, organizations cannot ignore their responsibility to appropriately address the privacy and security of sensitive personal information.

This article outlines an organization's legal responsibilities with respect to cyber risk, suggests how legal counsel can better prepare clients to mitigate risks before and during a data incident, and reviews the legal obligations and issues that counsel must address with a client in navigating a data breach.

The article begins by addressing data security-related issues on which legal counsel should advise an organization before any data incident. These matters include advising the client's directors and management on their responsibilities to provide appropriate oversight and direction of an organization's cybersecurity program, implementing appropriate training programs for the client's personnel, helping to manage data security issues in an organization's supply chain, assisting the client organization in establishing and testing an incident response plan, and reviewing insurance issues. The article then discusses legal requirements that counsel should help a client navigate in the event a security incident results in a reportable data breach, including California and other state and federal breach notification laws and best practices for the maintenance of attorney-client privilege and work product protections for data breach investigations. Finally, the article summarizes potential liability for noncompliance with privacy and security laws.

Counseling the Client Before the Breach

Board Duties

Regulators and the courts have repeatedly reminded us that cybersecurity is a business issue and not merely an IT issue, and that it must be dealt with as part of the overall management of an organization. Commissioner Luis A. Aguilar of the Securities and Exchange Commission (SEC) has warned directors that "boards that choose to ignore, or minimize the importance of cybersecurity oversight responsibility, do so at their own peril." Aguilar, *Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus*, Remarks at the "Cyber Risks and the Boardroom" Conference (June 10, 2014), available at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

As a business issue, the executives responsible for managing the organization play a critical role in determining whether the appropriate time, money, and resources are being expended to address cybersecurity issues. Indeed, top-down guidance within the organization is not only critical from an operational perspective; leaders may also

have legal duties to their organizations to address cybersecurity issues. As a result, counsel should prepare client organizations for a data breach by providing advice to directors and executives about how to comply with their fiduciary responsibilities in the realm of cybersecurity.

Corporate directors owe the corporations they manage fiduciary duties of good faith, care, and loyalty. To fulfill these fiduciary obligations, corporate directors are required to perform their duties as a director "in the best interests of the corporation and its shareholders and with such care, including reasonable inquiry, as an ordinarily prudent person in a like position would use under similar circumstances." Corp C §309. Directors are generally safe from judicial scrutiny of their management decisions due to the application of the business judgment rule, which in California is codified in Corp C §309. *Will v Engebretson* (Cal App 1989) 213 CA3d 1033, 1040. To take advantage of the business judgment rule shield, however, directors must exercise appropriate oversight of their organization's cybersecurity program. This oversight duty does not require that directors undertake day-to-day management of cybersecurity issues, but it does demand that directors and others in corporate leadership positions put in place reporting and control systems regarding cybersecurity. Counsel should advise the board and executives on the evaluation, selection, and implementation of appropriate cybersecurity oversight mechanisms and help corporate directors fulfill their fiduciary duties before a breach occurs.

Counsel should review cybersecurity oversight mechanisms that may already be in place at the client organization, analyze the gap between current policies and best practices, and assist the board and executives in establishing other mechanisms to develop a comprehensive enterprise risk management program. Every organization is unique and the mechanisms chosen should be tailored to the needs of the particular organization. The cybersecurity program must be integrated into the fabric of the organizational processes or risk being ignored, which itself could lead to liability. For example, under HIPAA, having a compliance program that is not implemented exposes clients to liability for willful neglect, which may subject organizations and their directors, officers and employees to civil and criminal liability. See 42 USC §1320d–5.

Operational mechanisms to help ensure that the board has access to appropriate information to quantify and mitigate risk and that infrastructure is in place to execute an enterprise-wide cybersecurity risk management plan can include

- Regularly devoting time in board meetings to review cybersecurity issues and listen to presentations from management responsible for cybersecurity at the organization, and documenting these activities in minutes;
- Appointing a chief information security, privacy, or similar officer to have accountability for, and report to the board on, cybersecurity issues; and
- Assigning a board audit committee with responsibility for cybersecurity issues and requiring the committee to report regularly to the board in person and in writing.

See Klein & Nuñéz, *Cybersecurity: Could It Be Your Next Fiduciary Duty?* (Middle Market Growth, May 2014), available at

http://www.pepperlaw.com/publications/cybersecurity-could-it-be-your-nextfiduciary-duty-2014–05–01/.

Boards should ensure that adequate resources and money are devoted to remediate identified deficiencies, consistent with the level of risk and organizational resources and priorities. Boards should also monitor the effectiveness of cybersecurity risk management plans through ongoing internal and external monitoring of the organization's cybersecurity controls.

Documented board attention to cybersecurity issues can be helpful in shielding corporate directors from shareholder derivative suits. For example, in a derivative suit against board members of Wyndham Worldwide Corporation, a federal district court in New Jersey noted that directors had discussed cybersecurity issues at 14 meetings and Wyndham's audit committee discussed the same issues in at least 16 committee meetings. As a result, the court determined that the Wyndham board had investigated adequately and had a clear understanding of the relevant issues when the board rejected the plaintiff's demand that the corporation bring a lawsuit based on data breaches suffered by Wyndham. See *Palkon v Holmes* (D NJ, Oct. 20, 2014, No. 2:14-cv-01234) 2014 US Dist Lexis 148799.

A Holistic Operational Approach

Although organizational preparation for a data breach may start at the top with management oversight, adequate preparation for a breach requires a holistic view that should also involve bottom-up efforts to train personnel and instill a culture of security at the organization. People, not technology, still remain one of the most commonly exploited cyber vulnerabilities. Together, errors by authorized users, such as employees and service providers, and misuse of access privileges by authorized users accounted for 24 percent of breaches reported to the COAG from 2012 to 2015. See COAG 2016 Data Breach Report. Phishing and social engineering ruses, and simple mistakes made by employees and vendors with access to personal information, commonly result in expensive breaches. Counsel should advise and assist their clients to establish annual security and privacy training programs for organization personnel. Depending on the needs of the organization, the training programs can include general privacy and security compliance training for all personnel, as well as specialized training for individuals in functional groups that face unique or heightened privacy and cybersecurity compliance issues, such as customer service, sales and marketing, and human resources. Counsel should assist in identifying legal obligations and cybersecurity needs specific to these groups and tailor training programs for them.

A holistic view that devotes attention to organizational preparation and establishes policies and procedures to minimize the risk that personal data could be compromised is consistent with regulatory guidance in this area by the FTC—which advocates privacy and security by design within an organization. See FTC Commissioner Edith Ramirez's *Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission*, Remarks at the Privacy by Design Conference (June 13, 2012), available at

https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacyframework-u.s.federal-trade-commission/120613privacydesign.pdf.

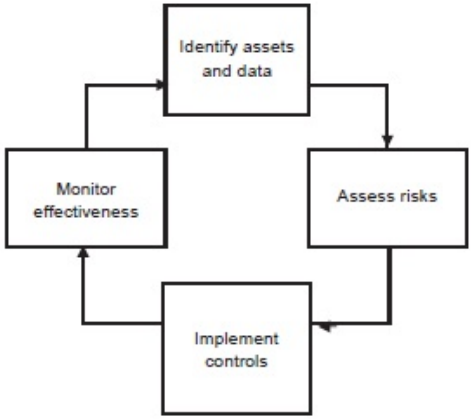
In June 2015, the FTC released *Start with Security: A Guide for Business* (available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf), which distills lessons learned from more than 50 cybersecurity-related enforcement actions by the FTC. The guidance provides ten principles to help ensure compliance with the FTC Act when an organization uses personal information in its business.

Principles from the FTC's Start with Security guidance:

1. Start with security.
2. Control access to data sensibly.
3. Require secure passwords and authentication.
4. Store sensitive personal information securely and protect it during transmission.
5. Segment your network and monitor who's trying to get in and out.
6. Secure remote access to your network.
7. Apply sound security practices when developing new products.
8. Make sure your service providers implement reasonable security measures.
9. Put procedures in place to keep your security current and address vulnerabilities that may arise.
10. Secure paper, physical media, and devices.

A fundamental principle of the FTC framework is that organizations must factor security into decision-making in every department of the organization's business and that organizations must make conscious data decisions every step of the way. For example, counsel should be involved early to analyze privacy and security risks in new product development, from registration screens to data capture and database storage. According to the FTC guidance, it is important to maintain privacy and security of personal information throughout the life cycle of data—collection, use, transmission, storage, and destruction. Data of the typical organization passes through many hands, from internal users to external service providers. Counsel for the organization must therefore have a firm grasp of assets and data, including the location of sensitive data, its transmission routes and its destinations, the risks to which the data is subject, and the controls required to protect data as it flows within and outside of the organization.

This holistic approach is stressed in the COAG 2016 Data Breach Report, which notes that information security is a process that requires a risk management approach, with basic steps informing and reinforcing each other: identifying assets and data to be protected, assessing the risks to that data, implementing security controls, and monitoring the effectiveness of those controls.



Source: COAG 2016 Data Breach Report.

The COAG also advocates the use by organizations of authoritative, comprehensive security standards to achieve an appropriate standard of care for personal information. Specifically, COAG guidance states that the 20 controls in the Center for Internet Security's Critical Security Controls (CIS Top 20), available at https://www.cisecurity.org/critical-controls.cfm, identify a "minimum level of information security that all organizations that collect personal information should meet" and further provide that an organization's "failure to implement relevant controls constitutes a lack of reasonable security." COAG 2016 Data Breach Report. The CIS Top 20 are listed in the table below:

CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7	E-mail and Web Browser Protection
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocols, and Services
CSC 10	Data Recovery Capability
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC	Boundary Defense

12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 15	Wireless Access Control
CSC 16	Account Monitoring and Control
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18	Application Software Security
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

Other common industry-accepted security standards that may be employed by an organization, such as the National Institute of Standards and Technology (NIST) Special Publication 800–53, the International Organization for Standardization's ISO 27002, and the Payment Card Industry Data Security Standards (PCI DSS), provide for types of controls similar to the CIS Top 20.

Supply Chain Issues and Third-Party Cyber Risk

Organizations often entrust third-party vendors with sensitive personal information. This creates data privacy and security supply chain issues that can potentially compromise the data. Legal counsel can play an integral role in managing these supply chain issues by helping to conduct appropriate due diligence review of vendors and ensuring that each vendor contract appropriately addresses privacy and security issues so that the confidentiality, integrity, and availability of the personal information entrusted to the vendor organization remains intact.

Before contracting, counsel should make sure that the client understands a vendor's cybersecurity practices, which can be achieved through appropriate due diligence. Counsel should review the vendor's data security-related policies, procedures, and other controls and should facilitate the proper level of review by the client to ensure that the vendor's policies and procedures are consistent with the client's requirements. Often, this can be accomplished by reviewing the results of independent third-party audits of the vendor's internal controls related to data processing, such as a Service Organization Control (SOC) 2 report (see http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC2Report.aspx). In addition, any vendor that handles sensitive personal information should perform internal audits and risk assessments in the ordinary course of its business and make the results or summaries available to customers annually and on request.

Clients in regulated industries may be required to contractually bind their vendors to specific privacy and security requirements. Vendor compliance with these requirements is meant to ensure that vendors are not the weak link in the chain,

exposing the regulated company to compliance risk. For health care entities subject to HIPAA, these agreements are called business associate agreements. Even in the absence of a special regulatory regime, regulators have made clear that companies that outsource data security functions to third parties can still be liable in enforcement actions in the event their vendors fail to provide adequate security. See *In re GMR Transcription Servs., Inc.* (FTC, Aug. 14, 2014, No. C-4482), available at https://www.ftc.gov/enforcement/casesproceedings/122–3095/gmr-transcription-servicesinc-matter; *In re Upromise, Inc.* (FTC, Mar. 27, 2012, No. C-4351), available at https://www.ftc.gov/enforcement/cases-proceedings/102–3116/upromiseinc.

When reviewing contracts, it is extremely important to determine the vendor's contractual commitments with regard to data privacy and security. At a minimum, agreements should address the issues below in an appropriate manner given the sensitivity of the data at issue. In addition to these issues, counsel should advise their clients to consider what steps may be appropriate to shift risk through the use of cyber insurance and the limitations of liability and indemnities in the contract. Vendor contracts should

- Commit the vendor to maintain and enforce reasonable administrative, technical, and physical safeguards appropriate to the sensitivity of the personal information being processed;
- Maintain client control over sensitive personal information by specifying that the client organization owns the data and prohibiting the vendor from using the data for any purpose other than to provide services to the client (to prevent a vendor from using personal data in unexpected ways for its own profit);
- Appropriately address integration with the organization's incident response plan by obligating the vendor to share breach-related evidence from the organization's cloud provider's environment;
- To the extent possible, make the responsible vendor pay for first-party costs (e.g., forensics, credit monitoring, remediation, and notification) as well as third-party costs (damages to the victim associated with a data breach caused by the vendor);
- Make sure that the vendor can meet the organization's data and document retention requirements, including those related to any "litigation hold"; and
- Require the vendor to return or destroy personal data at the end of the agreement.

Incident Response Plan

Adequate preparation for a security incident requires the development and testing of an incident response plan well before an incident occurs. Privacy counsel can play an essential role in developing and testing such a plan. At a minimum, counsel should read and understand the organization's incident response plan before being called on to assist in responding to a security incident.

The incident response plan should identify the internal interdisciplinary incident response team and any third parties that an organization has selected to assist in the event of an incident, such as computer forensics, public relations specialists, and outside counsel. The plan should provide a flexible approach for categorizing security events and responding appropriately, from identification and assessment to recovery

and resumption of normal operations. The plan should also identify which disaster recovery and business continuity plans are triggered.

Counsel should participate with the client in regular testing of the organization's incident response plan. Counsel and client should hold a dry-run exercise by selecting a hypothetical scenario to run through with all key players in the data breach response, including the internal incident response team and third parties such as outside privacy counsel and forensic specialist firms. The response plan should be well documented, and a roster of participants in the exercise and awareness training should be maintained. The plan should be reviewed annually and should be updated and informed by the client's experience in privacy and security incidents. The team should exchange all phone numbers and other contact information, and counsel should be involved in communications to provide attorney-client privilege protections.

Insurance

Cyber insurance plays a key role in an organization's overall strategy to mitigate risks related to data incidents. Although an in-depth discussion of insurance issues is beyond the scope of this article, counsel should be aware that traditional insurance policies have over time come to include limitations and exclusions to coverage that may preclude recovery in the event of a data incident. Even when cyber insurance is obtained, it is incumbent on the organization to make sure that the coverage is broad enough to address the risks that the organization is trying to insure against. Coverage for potential liability to third parties can generally be obtained, including coverage for costs related to defense, judgments and settlements, regulatory investigations, fines and penalties, noncompliance with the Payment Card Industry Data Security Standard (PCI DSS), and crisis management expenses, such as breach notification costs, forensic investigations, credit monitoring, and public relations specialists.

Counsel should review the state of the client organization's cyber insurance to assist in identifying coverage gaps that may be important to address given the nature of the client's business. When obtaining cyber insurance, counsel should collaborate with the organization's information technology professionals and compliance experts. Use of experienced insurance coverage counsel is also advisable; cyber insurance policies are negotiable in the current state of the market, and an in-depth understanding of the nuances of insurance coverage law can help avoid costly missteps in policy language.

Counseling the Client During a Breach

State Breach Notification Laws

When a security incident occurs, an organization needs knowledgeable privacy counsel to help guide it through compliance with its obligations under the various state data breach notification laws. In addition to understanding the timing and content of notices, counsel must assess whether a breach notice should be sent at all. Many security incidents do not require breach notification.

For example, in California, unauthorized disclosure of a credit card number would not trigger a breach notification unless a PIN or other security code, access code, or password that would permit access to an individual's financial account was also disclosed. See CC §1798.82(h)(1)(C). Given that litigation can ensue within 24 hours of a breach notice, the decision to issue a breach notice is as important as what to include and to whom the notice should be sent. California's general data breach law is codified at CC §1798.82. California also has a data breach law specific to breaches of medical information applicable to licensed health facilities, codified at Health & S C §1280.15. This article focusses on California's general data breach law but also provides an overview of breach notification obligations under specialized regulatory regimes, including health care.

Forty-seven states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification laws. Only Alabama, New Mexico, and South Dakota have no data breach legislation. The notification triggers and other aspects of the data breach notification laws can vary, creating the potential for multiple obligations for an organization that is required to provide notice. To ensure that the organization can meet its obligations under each of the applicable laws, counsel must help determine whether obligations to notify individuals and regulatory agencies are triggered, how long the organization has to provide notice, and what information is required in the notice.

Notification to Individuals

Who Is Required to Notify?

Data breach notification laws place the burden to notify affected individuals on the organization that owns or licenses the data. California and other state laws do not define the terms "owns" or "licenses," but the California Office of Privacy Protection (COPP) states that, for purposes of California's breach law, the term "data owner" means "the individual or organization with primary responsibility for determining the purpose and function of a record system." COPP, Recommended Practices on Notice of Security Breach Involving Personal Information (Jan. 2012), available at http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/recom_breach_prac.pdf. Service providers or other organizations that maintain data they do not own are responsible for notifying the data owner (but not affected individuals) of a reportable breach.

Unauthorized Access to Personal Information

Although precise legal requirements differ, data breach notification laws typically require that a data owner organization notify individuals when there has been unauthorized access to the individuals' unencrypted personal information. Depending on the applicable state or federal law, personal information is generally defined as a person's name together with one or more of that person's Social Security number, driver's license number, or financial information, such as an account number or credit or debit card number. See, e.g., CC §1798.82(h). Many states have included additional data elements in their definitions of "personal information," including health information, biometric data, date of birth, and mother's maiden name, to name a few.

See, e.g., CC §1798.82(h)(1)(D) (medical information).

California defines "personal information" as either (1) an individual's first name or first initial and last name in combination with any one or more of the following data elements: Social Security number; driver's license number or California identification card number; account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information; health insurance information; or information or data collected through the use or operation of an automated license plate recognition system; or (2) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. CC §1798.82(h).

Encrypted or Redacted Personal Information

Many breach notification laws, including California's, do not require notification if compromised data is encrypted, providing organizations with an incentive to implement robust encryption to protect personal information. See, e.g., CC §1798.82(h)(1). Some states also do not require notification if information is redacted. See, e.g., Mich Comp Laws §§445.63–445.72. Under California law, an organization is not required to notify individuals if either the individual's name or one of the enumerated data elements is encrypted. CC §1798.82(h)(1). Although the California statute does not reference encryption with respect to an individual's user name or e-mail address in combination with a password or security question and answer, notification duties with respect to that type of information are only triggered if the compromised data would "permit access to an online account." CC §1798.82(h)(2). Since properly encrypted data would not permit access, California law impliedly does not require notice if such data elements are encrypted.

Amendments to California's data breach notification law in 2015 define the term "encrypted" to mean "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security." CC §1798.82(h)(4). Use of proprietary cryptographic technologies no longer satisfies the "encrypted" standard. Counsel should advise clients to document the industry-accepted technology the client chooses to use with respect to the personal information that it processes.

Harm Thresholds

California and some other state breach notification laws require that organizations provide notice to any individual whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, 36 of 47 state breach laws (but not California's) contain harm thresholds. Under these laws, unauthorized access by itself does not trigger a notification obligation unless the organization determines that there is a reasonable likelihood that the unauthorized access would result in harm to the affected individuals. See, e.g., Ohio Rev Code Ann

§1349.19.

If a breach involves data of a resident of a state with a harm threshold law, counsel or experts may be required to work with the organization to conduct a risk assessment to determine whether the threshold has been met. In conducting such an assessment, counsel may follow a framework similar to that provided under the Final Omnibus HIPAA Rule (Final Rule) promulgated by the U.S. Department of Health and Human Services (HHS). See Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed Reg 5566 (Jan. 25, 2013) (codified at 45 CFR pts 160, 164). Under the Final Rule, one of the criteria that must be met for an incident to constitute a reportable breach is that there is more than a low probability that "protected health information" has been compromised. See 78 Fed Reg 5566, 5642.

The Final Rule provides four factors to consider in an organization's risk assessment that counsel may wish to evaluate if faced with a harm threshold statute: (1) the nature and extent of the personal information involved; (2) the person to whom the unauthorized disclosure was made; (3) whether personal information was actually acquired or viewed; and (4) the extent to which the risk to the personal information has been mitigated. 78 Fed Reg 5566, 5695. Of course, as stated above, California and many other states do not provide for a harm threshold. Consequently, if a breach involves the data of residents of states that lack a harm trigger as well as states that provide for a harm trigger, an organization may reasonably decide to notify all affected individuals, regardless of the results of a risk assessment, for customer relations purposes.

Notification and Timing Requirements

Each state law describes how organizations must give notice to affected individuals. Typically, laws (1) require written notice, (2) allow electronic notice in limited circumstances, and (3) allow substitute notice (usually consisting of e-mail notice, conspicuous posting on the home page of the organization's website, and notification to statewide media, e.g., newspapers and television) if (a) notifying individuals will exceed a specified cost threshold, (b) the number of individuals affected by the breach exceeds a certain number, or (c) the organization does not have sufficient contact information to provide notice.

California law allows notice to be provided by written notice; by electronic notice if such notice is consistent with the federal Electronic Signatures in Global and National Commerce Act (E-Sign) (15 USC §§7001–7031); and by substitute notice if the organization demonstrates that the cost of providing notice would exceed $250,000, that the affected class of subject persons to be notified exceeds 500,000, or that the person or business does not have sufficient contact information. Similar to other state statutes, substitute notice must consist of e-mail notice, conspicuous posting on the home page of the organization's website for a minimum of 30 days, and notification to major statewide media. CC §1798.82(j).

Several breach notification laws, including California's, include specific content requirements for notice to individuals. In 2015, California amended the breach notice format required under California law. As of January 1, 2016, California law requires data breach notices to be titled "Notice of Data Breach" and to follow a standard format, in which required content is organized under the headings "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." It also provides a model breach notice form that affected organizations may use to notify data breach victims. CC §1798.82(d). Organizations are required to include specific information in the notification, including a general description of the breach, the approximate date of the breach, and the types of personal information that were affected by the breach. CC §1798.82(d)(2). California law is typical in the types of information it requires to be included in the notice, although atypical in the detailed notice format requirements.

Requirements under each state data breach notification law differ, so each state's applicable law should be consulted when crafting breach notifications to ensure the notice complies with each state's requirements. In addition, published guidance from state attorneys general may include specific recommendations concerning actions to take and information to provide in a notice to individuals. For example, the COAG 2016 Data Breach Report recommends that an organization's data breach notice prominently encourage individuals affected by a breach of Social Security numbers or driver's license numbers to place a fraud alert on their credit files. Third-party vendors and knowledgeable privacy counsel assisting with the preparation of notices in various jurisdictions will be able to identify applicable jurisdictional differences to build into the notices.

Timing of Notification to Individuals

State breach laws, including California's, generally require data owners to provide notice of a breach to affected individuals "in the most expedient time possible and without unreasonable delay." CC §1798.82(a). A few state breach laws require notification to affected individuals within 30 or 45 days of discovery of the incident giving rise to the breach. See, e.g., Wis Stat §134.98(3)(a); Fla Stat §501.171(3)(a). California's data breach law specific to licensed health facilities requires clinics, health facilities, home health agencies, and hospices to report breaches of patient information to patients and the California Department of Public Health within 15 business days after detection of the breach, unless the notice would impede a law enforcement investigation. Health & S C §1280.15. Given the detail required by the notification requirements, providing notification within such timeframes can be a significant challenge. Clients often want to provide notice immediately, but it is advisable to gather all facts first to ensure that the notice provides the most accurate picture of the incident and to minimize the likelihood of having to reissue notices on discovery of new information.

In California and nearly all other jurisdictions, organizations that own or license the data subject to the breach are permitted to delay notification (1) to comply with a request for delay by law enforcement authorities, (2) to restore the security of the affected system, or (3) to determine the scope of the breach. See, e.g., CC

§1798.82(a), (c). However, California law requires that service providers must notify the owner or licensee of the data "immediately" following discovery of the acquisition of the data by an unauthorized person. CC §1798.82(b). Counsel for service-provider organizations that process personal information of California residents on behalf of other organizations should therefore be aware that the law does not give a service-provider organization leeway with respect to its obligation to report a breach to the owner or licensor of the data.

California law does not contain a hard-and-fast deadline for owners and licensors by which notice must be provided to affected individuals. Consequently, what constitutes the "most expedient time possible" and "without unreasonable delay" under CC §1798.82(a) is a fact-specific inquiry based on the nature of each breach. In 2014, a California court dismissed claims against Sony relating to a breach of its Sony PlayStation Network for failure to state a claim because the plaintiffs had not substantiated an injury attributable to the fact that Sony took 10 days to notify claimants after Sony became aware of the breach. See *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.* (SD Cal 2014) 996 F Supp 2d 942, 965. Also in 2014, Kaiser Foundation Health Plan, Inc. agreed to pay $150,000 to settle claims by the COAG that Kaiser's notification to its employees of unauthorized access to their personal information 6 months after it first learned of the breach constituted an unreasonable delay. The 6-month period included 4 months of forensic examination in an attempt to determine the scope of the breach. See *People v Kaiser Found. Health Plan, Inc*. (Super Ct, Alameda Cty, Jan. 24, 2014, No. RG14711370) (unpublished order). Thus, while immediate notice may not be required, organizations must balance their own efforts to determine exactly what happened with what notification period is reasonable to protect individuals affected by the breach.

Other Breach Notification Laws and Requirements

To determine the full scope of an organization's compliance responsibilities, counsel must understand whether any special regulatory regimes apply to the client. Numerous industry-focused federal laws govern data breaches. For example, the GLBA applies to financial institutions (see 15 USC §§6801–6809); HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) (Pub L 111–5, 123 Stat 115) apply to the health care industry; and the Family Educational Rights and Privacy Act (FERPA) (20 USC §1232g) applies to educational institutions. Any of these special regulatory regimes could affect an organization's obligations under state data breach laws. For example, California and many other states exempt covered entities from compliance with California data breach notice requirements if the covered entity has complied with its notification requirements under HIPAA. CC §1798.82(e). Further, as stated above, licensed health facilities in California are subject to separate data breach notification requirements under Health & S C §1280.15.

Gramm-Leach-Bliley Act

The GLBA, among other things, requires "financial institutions" to develop, implement, and maintain administrative, technical, and physical safeguards to protect the

security, integrity, and confidentiality of "nonpublic personal information." 15 USC §6801(a). The GLBA guidelines provide that when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customers as soon as possible. See 12 CFR pt 364, App A. This analysis is similar to the analysis required under state data breach laws that contain a harm threshold.

HIPAA and the HITECH Act

HIPAA and the HITECH Act set forth privacy and security protections required for the health care industry. Breach notification requirements for "covered entities" and "business associates" subject to HIPAA (see 45 CFR §160.103) are provided in HIPAA's breach notification rule. See 45 CFR pt 164. The breach notification rule requires covered entities to provide notification for breaches of unsecured or unencrypted protected health information to the affected individuals, HHS, and major print or broadcast media for breaches affecting more than 500 residents of a state or jurisdiction. 45 CFR §§164.404, 164.406, 164.408.

Family Educational Rights and Privacy Act

FERPA applies to any public or private elementary, secondary, or post-secondary school and any state or local education agency that receives federal funds. See 34 CFR §99.1. FERPA does not contain specific breach notification requirements. Rather, it protects the confidentiality of education records by requiring documentation of each disclosure. The federal regulations, nonetheless, encourage direct notification if, for example, the compromised data includes student Social Security numbers or other identifying information that could lead to identity theft. See 34 CFR pt 99. Similarly, FERPA does not require that an institution notify the Family Policy Compliance Office of the U.S. Department of Education in the event of a data breach. However, it is nonetheless generally considered a best practice to do so.

Notification to Regulators, Law Enforcement, and Others

In addition to notifying affected individuals and consumer reporting agencies, numerous state breach laws may also require affected entities to notify state attorneys general or other state regulators of an incident. Under these laws, the obligation to notify state regulators typically belongs to the entity that owns or licenses the data. In certain states, service providers must cooperate with data owners during the notification process. California requires organizations to notify the Attorney General (by submitting to the Attorney General an electronic copy of the individual breach notification letter, excluding any personally identifiable information) if the organization is notifying more than 500 California residents. CC §1798.82(f). As in the case of notification to individuals, timing requirements for required notifications differ across jurisdictions. At the extreme, Puerto Rico law requires that companies inform Puerto Rico's Department of Consumer Affairs within 10 days after a violation

of a system's security has been detected. The Department of Consumer Affairs is obligated to make a public announcement related to the incident within 24 hours of being notified. PR Laws Ann, tit 10, §§4051—4055. Such compressed timing could affect an organization's legal and business strategies following a breach. Counsel must review regulatory notification thresholds and timing requirements in each jurisdiction in which affected individuals reside.

It is also important to identify appropriate law enforcement contacts to notify regarding security incidents that may involve illegal activities. Counsel should be involved in making the assessment of whether law enforcement should be notified and should establish relationships with appropriate law enforcement contacts before an incident occurs to facilitate communications in the event of an incident. From a practical perspective, counsel should provide advice on how and when to notify regulators and law enforcement. In the case of a major breach, discussions with and notice to regulators should generally precede notice to individual victims. In addition, it is critical to have a consistent description of the facts and to arm customer support personnel with appropriate responses to questions about the breach.

Organizations may also have contractual obligations to notify third parties, such as insurers or contracting partners. A client should notify its insurance carrier in accordance with policy requirements. Failure to provide prompt notice could be used by the insurer as part of a basis to deny the claim. Counsel should also assist the client in the review of any contractual obligations it may have to business partners to provide notification in the event of a data breach. For example, merchants that process payment card data are obliged to notify payment card issuers in the event of a data breach.

Attorney-Client Privilege and Work Product Protection

In addition to providing organizations with guidance on the legal and regulatory minefield of laws governing data privacy and security, the retention of counsel to address a data breach provides an organization with the added benefit of preserving confidential communications and strategy discussions on legal matters related to a breach.

Attorney-Client Privilege

In general, a communication between a client and attorney is protected by the attorney-client privilege if the communication is confidential and for the purpose of securing or obtaining legal advice. Fisher v U.S. (1976) 425 US 391, 403. The attorney-client privilege line, however, becomes murky when communications may have business as well as legal purposes, which may occur when in-house counsel is involved. In these cases, courts will look to the dominant purpose of the communication to determine whether it was for a legal purpose rather than a business purpose. See *Soltani-Rastegar v Superior Court* (1989) 208 CA3d 424, 427. When in-house counsel has both legal and business responsibilities, the line between the two can become blurred and a court may be less inclined to find an attorney-client privilege.

Given the potential uncertainty regarding application of the attorney-client privilege in a corporate setting, outside counsel should be retained to direct the breach investigation for the purpose of gathering the information necessary to provide legal advice to the organization. In that way, to maximize the chances that communications regarding the investigation will be privileged, the organization can avail itself of the simpler test for privilege: whether the communication between the client and attorney was confidential and for the purpose of obtaining legal advice.

Before or, if necessary, during a breach, counsel should engage third-party vendors and coordinate the breach response from the organization's personnel and vendors so that the efforts of all parties are focused on ensuring that counsel can provide appropriate legal advice to enable privilege protection for breach investigation communications. Members of the response team must be educated by counsel on basic guidelines for communications to help keep them privileged. For example, communications should stay within the circle of the breach response team to maintain confidentiality, and all communications should be marked as "attorney-client privileged." Education of the team on these basic points should be a part of counsel's role before a breach in preparing the organization to respond, but counsel should also be alert for communications that do not fall in line with best practices during the fast-paced breach response. If necessary, counsel should step in quickly to ensure that behavior that could threaten the ability to claim attorney-client privilege is immediately corrected.

Work Product Doctrine

The work product doctrine is another tool that can protect documents that are prepared as part of the investigation of a data breach. Federal Rule of Civil Procedure 26(b)(3) states:

> Ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent).

If such documents are requested during discovery, an organization must show that the documents it is attempting to shield from discovery through the work product doctrine were prepared in anticipation of litigation. The work product doctrine clearly applies to documents created by investigators working for attorneys if the documents were created in anticipation of litigation. *U.S. v Nobles* (1975) 422 US 225, 239. Conversely, documents created as part of routine business or investigations will not receive the benefit of work product protection. See *2,022 Ranch, LLC v Superior Court* (2003) 113 CA4th 1377, 1390, disapproved on other grounds in *Costco Wholesale Corp. v Superior Court* (2009) 47 C4th 725. For example, if an organization's information technology staff is investigating the breach to determine the extent of any compromise of the organization's systems without the involvement of counsel, the organization may not be able to protect the results of the investigation from discovery under the work product doctrine.

Consequently, outside counsel should engage consultants such as forensic specialists to assist in the data breach investigation. When outside counsel hires third-party experts to assist in an investigation, courts will generally extend work product protection to the documents created by that third party as part of the investigation. See *U.S. v Torf (In re Grand Jury Subpoena)* (9th Cir 2003) 357 F3d 900, 907. When it is necessary for in-house counsel to hire third-party consultants to assist in a data breach investigation, the organization should state as part of the terms of the engagement that the third party has been hired in anticipation of litigation related to the data breach.

The recent class action litigation related to the Target Corporation breach, which involved financial information of nearly 40 million consumers, provides a good blueprint for structuring a data breach investigation in a way that helps preserve the attorney-client privilege and work product doctrine for investigation-related communications and materials. In that case, the plaintiffs sought to compel production of documents related to the organization's investigation of the data breach. The documents were created by a data breach task force that was established at the request of the company's in-house and outside counsel "so that the task force could educate Target's attorneys about aspects of the breach and counsel could provide Target with informed legal advice." *In re Target Corp. Customer Data Sec. Breach Litig.* (D Minn, Oct. 23, 2015, MDL No. 14–2522 PAM/JJK) at 2 (unpublished order) (Target Unpublished Order). The task force engaged two teams from Verizon to investigate the data breach. One Verizon team was engaged by Target's outside counsel to "enable counsel to provide legal advice to Target, including legal advice in anticipation of litigation and regulatory inquiries." Target Unpublished Order at 3. The other Verizon team conducted a separate investigation on behalf of several credit card brands. The Verizon teams did not communicate with each other about the attorney-led investigation. The court found that this two-track investigation was structured in a way that properly shielded most of the information that was the subject of the discovery request. Target Unpublished Order at 5.

Finally, as with any litigation, a party has a duty to preserve reasonably accessible information. Litigants are required to initiate a legal hold when litigation is reasonably anticipated. Organizations should reasonably anticipate that they will be involved in litigation related to the breach on discovery. Accordingly, when a data breach occurs, organizations should take care to preserve and collect evidence as soon as practicable in accordance with the organization's litigation hold policy. Counsel should document the actions taken by the organization in response to a breach to evidence compliance with the organization's discovery obligations.

Liability for Noncompliance

Potential costs to a client organization for failure to comply with its obligation to maintain reasonable security safeguards can be substantial. Civil actions can be a significant source of potential liability following a breach, and civil suits by consumers, notably class actions, are nearly always filed immediately after a large data breach. Thanks to the U.S. Supreme Court decision in *Clapper v Amnesty Int'l USA* (2013) ___US ___, 133 S Ct 1138, plaintiffs face challenges in establishing

standing in such cases because of the difficulty of showing actual injury, but success is not unheard of. Class action plaintiffs in the Target breach litigation were found by the court to have standing to sue. See *In re Target Corp. Customer Data Sec. Breach Litig.* (D Minn 2015) 309 FRD 482. That ruling quickly led to a $10 million settlement of the case. California residents that are injured by an organization's violation of California's requirement to implement and maintain reasonable security procedures or a violation California's data breach notification law may sue for damages and injunctive relief, raising the specter of such civil suits in California. See CC §1798.84.

Given an opportunity based on the type of data at issue, plaintiffs may avoid issues in establishing actual injury and standing under laws that provide statutory damages for data incidents. The Video Privacy Protection Act of 1988 (VPPA) (18 USC §2710) is a favorite vehicle for plaintiffs for this reason. The VPPA prohibits a video tape service provider (which can broadly include providers of video content over the Internet) from knowingly disclosing information identifying an individual as having requested or obtained specific video materials or services. It creates a private right of action with liquidated damages available for aggrieved consumers for VPPA violations. 18 USC §2710. In the event a law such as the VPPA is invoked, disentangling the organization from the lawsuit may be more difficult than prevailing on standing issues. Moreover, case law regarding standing issues is in flux. The U.S. Supreme Court is currently considering whether congressional authorization of a private right of action based on a technical statutory violation may confer standing on a plaintiff who has suffered no concrete harm (see *Spokeo, Inc. v Robins* (US, Apr 27, 2015, No. 13–1339) 2015 US Lexis 2947 (granting cert)), and the U.S. Court of Appeals for the Seventh Circuit ruled recently that the risk of future injury related to a data breach is sufficient to survive the pleadings stage (see *Remijas v Neiman Marcus Group LLC* (7th Cir 2015) 794 F3d 688). The shifting legal landscape on standing could have a significant impact on potential liability in the event of a data incident.

Organizations can also be subject to enforcement actions by federal and state regulators. In the event of a breach at a health care organization, HHS can bring an enforcement action if it finds that the organization has violated HIPAA. WellPoint, Inc., a managed care company now known as Anthem, Inc., settled alleged HIPAA violations for $1.7 million in 2013, and HHS imposed a $4.3 million civil penalty for HIPAA violations on Cignet Health of Prince George's County, Maryland, in 2011.

The FTC can also bring actions to prosecute deceptive and unfair trade practices against companies that do not adhere to their stated privacy and security standards or do not provide adequate security. In an enforcement action against a repeat offender, LifeLock Inc., the FTC fined the company $100 million not for a data breach, but for violating a previous FTC order to secure customer information and stop deceptive advertising. See *FTC v LifeLock Inc.* (D Ariz, Jan. 4, 2016, No. CV-10–00530-PHX-JJT) 2016 US Dist Lexis 17973. In addition to monetary penalties, FTC enforcement actions typically result in 20-year consent decrees, under which organizations must regularly monitor and obtain independent assessments of their privacy practices. Monitoring and assessment activities can be incredibly expensive over such a long period.

State attorneys general can also bring enforcement actions that may result in heavy penalties. The COAG has not been shy in bringing privacy enforcement actions. For example, in 2013, Citibank, N.A. agreed to pay a $420,000 penalty under a stipulated final judgment arising out of a breach of its Citibank Online website resulting from a known technical vulnerability that affected more than 80,000 California account holders. *People v Citibank, N.A.* (Cal Super Ct, Aug. 29, 2013, No. RG13693591) (unpublished order).

Derivative suits brought by shareholders alleging a breach of fiduciary duty by officers and directors are also becoming increasingly common for public companies that find themselves the subject of data breaches. However, the *Wyndham* case, discussed above, shows that plaintiffs may have difficulty succeeding if the board exercises appropriate care and due diligence. In addition to *Wyndham*, breach of fiduciary duty lawsuits have been brought in connection with the Target and Home Depot data breaches.

Conclusion

Businesses have long understood that the technical aspects of cybersecurity need the attention of dedicated IT and security professionals. The same holds true for the legal aspects of cybersecurity. Experienced legal counsel are needed to prepare for and to help prevent data incidents. Experienced counsel are also needed to ensure that any response to a breach not only meets all legal and regulatory requirements, but also best positions the client to weather the perfect storm of litigation, reputational harm, and other business impacts resulting from a breach.

The material in this publication was created as of the date set forth above and is based on laws, court decisions, administrative rulings and congressional materials that existed at that time, and should not be construed as legal advice or legal opinions on specific facts. The information in this publication is not intended to create, and the transmission and receipt of it does not constitute, a lawyer-client relationship.