

BREACH RESPONSE CHECKLIST

1. ENGAGE YOUR IN-HOUSE AND OUTSIDE COUNSEL

- Counsel will play an important role following any data incident, including maintaining the confidentiality of the investigation, protecting applicable internal communications under the attorney-client privilege and work product protections, and anticipating litigation and other legal risks.
- Counsel will also assist in identifying your legal obligations following any data incident, including any notification requirements.

2. NOTIFY YOUR INSURANCE BROKER AND/OR CYBER-INSURANCE CARRIER, IF YOU HAVE ONE

- Involve your insurance manager to assist with the communications to your cyber-insurance carrier. Insurance will have their own questions and requirements and it is important to have your representative provide accurate and timely information as necessary.

3. BEGIN EXECUTION OF YOUR DATA INCIDENT RESPONSE PLAN, IF YOU HAVE ONE

- Assemble your pre-identified incident response team, including your incident response team leader and leaders from management, IT, human resources, and public relations teams.
- Remember that data incidents may compromise communications within the organization. Be prepared by having contingency plans in place that account for such possibilities, including laptops not connected to the network and a secure communication method.

4. INVESTIGATE THE INCIDENT

- At the direction of legal counsel, your appointed incident response team member should identify and collect information about the incident, including interviewing involved personnel and documenting the forensic position of the organization (e.g., was data viewed, modified, or stolen; what personal information was compromised; what measures are necessary to restore the system).

BREACH RESPONSE CHECKLIST CONTINUED

5. STOP ANY ADDITIONAL LOSS AND PREVENT FURTHER EXPOSURES

- Mitigate your risks by determining whether you have any other security gaps or risks, or whether other systems are under threat of immediate danger.

6. CONSIDER, WITH LEGAL COUNSEL, WHETHER LAW ENFORCEMENT NEEDS TO BE NOTIFIED

- As of 2018, all 50 states have breach notification laws and certain states *require* notification of law enforcement when there is a security breach.

7. ENGAGE YOUR CRISIS MANAGEMENT TEAM

- Once you have sufficient information about the incident, deploy your communications team to control internal and external messaging.
- Internal and external communications should be clear, concise, and consistent.

8. ANALYZE THE LEGAL IMPLICATIONS OF THE INCIDENT

- Review any relevant company agreements, including website privacy policies, to determine if the organization owes notification or other obligations to any third-party with respect the data impacted.
- Determine the location of the customers, employees, and/or systems affected by the incident to determine impact and involvement of various jurisdictional laws.

9. LEARN FROM THE INCIDENT

- Data incidents expose the vulnerabilities in an organization's computer systems. Those vulnerabilities can be addressed to prevent the systems from being exploited in a similar manner in the future.
- Address any weaknesses in your incident response plan.

TOP TIPS FOR THE CYBERSECURITY OF DATA

With the rapid and significant changes surrounding the protection of data and consumer privacy, including the EU's General Data Protection Regulation (GDPR) and California's new privacy law, the California Consumer Privacy Act of 2018 set to take effect January 1, 2020, it is important to take stock and review your data protection practices frequently. Here are a few "top tips" and best practices for considering privacy issues within your organization and for maintaining a robust cybersecurity plan in an effort to keep pace with the evolving threat and legal landscape.

EDUCATE YOUR STAFF

By far the weakest link in any organization's chain, human error or malfeasance is often cited as the cause of the majority of data incidents and the biggest threat to everyday cybersecurity. Annual cybersecurity training will help your employees understand their role in protecting your business from cybersecurity threats and also demonstrate to your employees your commitment to protecting data.

RESTRICT ACCESS TO DATA

If an employee does not have to use sensitive information as part of their job, there's no need for them to have access to it. Implementing access controls strengthens your data protection and is an important cybersecurity tool. Effective access controls can be put into place with separate user accounts that grant a user privileges based on their job needs.

ENCRYPT DATA

Encryption is one of the most effective and straightforward tools for protecting data. By encrypting data, you make it more difficult for attackers to read information even if they gain access to the data. Generally, data is most at risk when it is being moved from one location to the next so encrypting data while it is both in-motion and at-rest is critical. Don't forget to also encrypt data on mobile devices, whether that is a company-issued smartphone or laptop.

CONDUCT REGULAR SECURITY RISK ASSESSMENTS

Proactive privacy and security risk assessments can help identify vulnerabilities and weaknesses in your system before they become a problem. Regular risk assessments can also create an audit trail that may be helpful in identifying the cause or other valuable details surrounding a data incident after it occurs.

BACKUP TO A SECURE, OFFSITE LOCATION

Data backups to a secure, offsite location are important to avoid significant business interruption in the event of a data incident. Ensure a good backup strategy is in place, including controls for data encryption and access and ongoing data management, to make sure your data backups are effective and secured.

EVALUATE THE CYBERSECURITY POSTURE OF YOUR VENDORS

Do not ignore the importance of frequently (and carefully) evaluating the cybersecurity posture of your vendors and third-party business associates. Their vulnerabilities may eventually become your liabilities.



Cyber Incident Reporting

A Unified Message for Reporting to the Federal Government

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber attacks that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This fact sheet explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

How to Report Cyber Incidents to the Federal Government

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, and any of the federal agencies listed in the table on page two. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident to an appropriate federal point of contact.

Types of Federal Incident Response

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: Threat Response and Asset Response. Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity. Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to



systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community.

Irrespective of the type of incident or its corresponding response, Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Key Federal Points of Contact	
Threat Response	Asset Response
<p>Federal Bureau of Investigation (FBI)</p> <p>FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field</p> <p>Internet Crime Complaint Center (IC3): http://www.ic3.gov</p> <p><i>Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.</i></p> <p><i>Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.</i></p>	<p>National Cybersecurity and Communications Integration Center (NCCIC)</p> <p>NCCIC: (888) 282-0870 or NCCIC@hq.dhs.gov</p> <p>United States Computer Emergency Readiness Team: http://www.us-cert.gov</p> <p><i>Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.</i></p>
<p>National Cyber Investigative Joint Task Force</p> <p>NCIJTF CyWatch 24/7 Command Center: (855) 292-3937 or cywatch@ic.fbi.gov</p> <p><i>Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.</i></p>	
<p>United States Secret Service</p> <p>Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): http://www.secretservice.gov/contact/field-offices</p> <p><i>Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information</i></p>	
<p>United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI)</p> <p>HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or https://www.ice.gov/webform/hsi-tip-form</p> <p>HSI Field Offices: https://www.ice.gov/contact/hsi</p> <p>HSI Cyber Crimes Center: https://www.ice.gov/cyber-crimes</p> <p><i>Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.</i></p>	
If there is an immediate threat to public health or safety, the public should always call 911.	

Attorney Client Privilege and Work Product During a Cyber Breach

By Carole J. Buckner, Partner and General Counsel, Procopio, Cory, Hargreaves & Savitch, LLP

When a data breach occurs, counsel can advise on a wide range of issues from customer notification to remediation to regulatory requirements. Because class action litigation and regulatory scrutiny can follow a data breach, understanding and properly addressing attorney client privilege and attorney work product are critical from the outset. Companies should structure the data breach team to protect privilege and work product in connection with implementation of a response. Meetings and documentation should be implemented in a manner that will establish and maintain privilege. All members of the data breach team and company management should be trained as to how to preserve both privilege and work product. This article addresses many of the important nuances, including lessons learned from prominent data breach litigation.

ATTORNEY CLIENT PRIVILEGE

The attorney client privilege protects confidential communications made during an attorney client relationship from disclosure. (Cal. Ev. Code § 954.) Confidential communications are defined as those between client and lawyer in the course of an attorney client relationship, transmitted by means which disclose the information to no third persons other than those who are present to further the interest of the client in the consultation or those who are reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted. (Cal. Ev. Code § 952.) Disclosure of information to those reasonably necessary to accomplish the purpose of the representation does not constitute a waiver. (Cal. Ev. Code § 912.)

Federal attorney client privilege in the corporate setting protects communications with employees and corporate counsel in order to obtain information not otherwise available to upper management, where the employee is communicating with an attorney at the direction or a superior in order to secure legal advice for the company, if the subject matter of the communication falls within the duties of the employee and the communication is intended to be confidential. (*Upjohn Co. v. United States*, 449 U.S. 383 (1981).) In California, the dominant purpose test is used to determine whether a corporate employee is making the communication at the request of the employer, and to examine the intent of the employer and employee. (*D.I. Chadbourne v. Sup. Ct.*, 60 Cal.2d 723 (1964).) In determining whether any particular communication is privileged, the number of hands through which it passed is also relevant. (*Id.*)

WORK PRODUCT

If a particular document is not covered by the attorney client privilege, it may still be protected by the work product doctrine. (*Hickman v. Taylor*, 329 U.S. 495 (1947); Fed Rule Civ. P. 26 (documents and tangible things prepared in anticipation of litigation or for trial); Fed. R. Crim. P. 16.) California work product protection is broader in scope, and may protect recordings and notes regarding witness interviews even if

they are not created in anticipation of litigation. (Cal. Code Civ. P. 2018.030; *Coito v. Sup. Ct.*, 54 Cal.4th 480 (2012).)

LEGAL OR BUSINESS ADVICE?

An important consideration in determining whether a particular communication is privileged involves whether the dominant purpose was to give legal advice or business advice. Generally, the attorney client privilege is not applicable where the attorney merely acts as a negotiator or to provide business advice. (*Aetna Cas. & Sur. Co. v. Sup. Ct.*, 153 Cal. App. 3d 467 (1984).) Court will look at whether the communication was made in furtherance of that attorney client relationship, while taking into consideration that an attorney may be hired to address business affairs, but also give legal advice during the course of the representation, and that such advice should be protected notwithstanding the original purpose for which the attorney was employed. (*Kaiser Foundation Hospitals v. Sup. Ct.*, 66 Cal. App. 4th 1217 (1998).) Sending a carbon copy (or “cc”) of an otherwise non-privileged communication to an attorney does not necessarily render the communication privileged. (See, e.g., *In re Google, Inc.*, 462 Fed. Appx 975 (Fed. Cir. 2012).)

INTERNATIONAL PRIVILEGE

In-house attorneys operating in an international setting need to bear in mind that while U.S. courts generally extend privilege protection to foreign attorneys, some courts recognize foreign privilege law, such as the law of the European Union, and do not extend privilege protection to communications between companies and their in-house attorneys. (*Akzo Nobel Chem. Ltd. V. European Comm’n*, Case C-550/07 P, 26 Law. Man. Prof. Conduct 584 (Euro. Ct. Justice, Sept. 14, 2010).)

OUTSIDE COUNSEL

In-house counsel often provide both legal and business advice. Outside counsel in contrast, predominantly provide legal advice. Hiring outside counsel at the inception can protect against the argument that in-house counsel’s advice predominantly involved business advice and therefore was not privileged. This can be particularly important in international investigations given that non-U.S. privilege will not apply to protect communications between the company and in-house counsel in some countries.

DUAL INVESTIGATIONS

One approach is to establish dual investigations as Target did in connection with its payment card data breach. One team worked on the business response, focusing on operational concerns, while a second team directed by Target’s counsel directed a response task force. (*In re Target Corp. Customer Data Security Breach Litig.*, MDL NO. 14-2522 (D. Minn. Oct. 23, 2015).) To optimize application of the privilege, the work should be directed by legal counsel, and the key objective should be to render legal advice. In addition, outside consultants should be engaged by counsel and work at the direction of counsel. (*Id.* At 1-2.) Counsel should remind employees and consultants of the confidentiality and privilege applicable to communications under the direction of counsel for the purpose of rendering legal advice.

In the Target data breach, Target retained Verizon to investigate the data breach. Two separate teams were established both at Target and at Verizon. The plaintiffs argued that communications between the Target task force and Verizon were not privileged and were not protected by the work product doctrine, because Target would have had to investigate and address the data breach regardless of any litigation. Target asserted that the task force was not engaged in an ordinary course of business investigation of the data breach. Rather Target asserted that Verizon had been engaged to educate the task force run by Target's in-house counsel and Target's outside counsel about aspects of the breach to enable counsel to provide informed legal advice, in part to defend against multiple class action lawsuits filed against Target. The court conducted an in camera review.

One set of documents in question involved email updates from the CEO to the Target board of directors in the aftermath of the data breach. The court ordered such communications produced because they did not involve any confidential attorney client communications or contain requests for legal advice nor provide legal advice. (*Id.* at 3.)

As to documents related to the work of the task force focused not on remediation but on informing Target's in-house and outside counsel about the breach, for the purpose of obtaining legal advice and preparing to defend the class action litigation, the court found Target met its burden of demonstrating these documents were protected by attorney client privilege and the work product doctrine. (*Id.* at 3-4.)

EMAIL

In order to be protected by attorney client privilege, email communications with counsel must request or provide legal advice. (*Premora II*, at *3.) Factual discussions exchanged with counsel are not protected from discovery by the attorney client privilege, unless the facts are being transmitted to counsel in order to provide legal representation. (*Id.*)

PRESS RELEASES

In general, courts are divided regarding whether attorney client privilege covers communications between counsel and a public relations consultant. In California, there is no public relations privilege. (*Behunin v. Sup. Ct.*, 9 Cal. App. 5th 833 (2017) (holding that communications with public relations consultant were not covered by the attorney client privilege where the disclosures were not reasonably necessary for the client's representation in the litigation).) The issue is whether the communication is necessary for the client to obtain informed legal advice, which may be evaluated by an in camera review after the privilege is claimed. The more integrated the public relations consultant is with development of legal strategy, effectively becoming and "agent" of the attorney, the more likely the privilege will cover communications between the two. In such a situation, there will be an expectation of confidentiality as well as necessity of disclosure to the third party in order to obtain informed legal advice. Some cases refer to the necessity element as requiring more than just convenience, requiring near indispensability. Other cases apply a test asking whether the public relations consultant was the "functional equivalent of an employee of the client." (*U.S. v. Chen*, 99 F.3d 1495, 1500 (9th Cir. 1996) (requiring a detailed factual showing of a close working relationship with the company's principals on matters critical to the company's position in litigation, and possession of

information possessed by no one else in the company).) These considerations should be balanced in entering into the engagement agreement with and utilizing the public relations consultant.

Federal common law on attorney client privilege differs from California law because the privilege is broader and there is no requirement of a finding that the communication was reasonably necessary for the attorney to provide legal advice. In any event, a fact specific inquiry will be required.

One case addresses the application of the privilege to communications with a public relations consultant during a data breach investigation. To the extent that those are not drafted by or sent to counsel, even if they incorporate the advice of counsel, a court may find that they are not protected by the attorney client privilege. (*In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230 (D. Or. 2017).) In addition, documents not prepared by or sent to counsel, even if prepared at the request of counsel by employees and third party vendors, will not be privileged if they are not prepared because of litigation. (*Id.* at 1242.) The court will look at whether the primary purpose of such communications is to address the data breach, a business function, or to obtain legal advice. (*Id.* at 1243.) However, communications sent to and from legal counsel seeking or providing actual legal advice or the possible legal consequences of a proposed text are privileged. (*Id.*)

PUBLIC RELATIONS AND INTERNAL COMMUNICATIONS

A public relations consultant is a key member of the team that will address a data breach. Copying an attorney on communications involving a public relations consultant discussing published articles about the data breach may or may not be privileged. If the discussion involves seeking legal advice about how a particular article may impact the company or litigation, or how, from a legal perspective, the company should comment on the article, it is privileged. (*Premera*, 2019 U.S. Dist. LEXIS 20279 *11 (*Premera II*); citing *Premera I*, 296 F.Supp. 3d At 1244.) If, however, the discussion involves merely the facts of the article, or how others are responding to the article, without a request for legal advice, or the provision of legal advice, merely including attorneys on the email does not render the email privileged. (*Id.*)

Internal communications between company executives and counsel regarding an article being drafted by the company are more likely to be privileged because they are more likely to involve requests for legal advice where the company's executives may be asking for legal advice as to how to minimize legal exposure, and/or the impact on the company's risk of liability.

In responding to a data breach internal communications will also be generated, which may include scripts prepared by outside counsel and in-house counsel, FAQs, responses to regulators and notices to consumers. Where drafts of such documents contain edit by counsel, a privilege designation is appropriate. (*Premera II*, at *6.)

COMMUNICATIONS RE: CONSUMER NOTIFICATIONS

Communications with outside counsel concerning consumer notifications are privileged if they are requesting or providing legal advice. This is the case even if counsel is not providing a redline version. This

will include documents circulated in order to provide legal counsel to the company in drafting notification letters. Such communications may also qualify for protection under the work product doctrine.

DATA BREACH CONSULTANT'S WORK

Discovery disputes over draft and final reports of consultants can develop. In the *Premera* matter the forensic consultant produced a Remediation Report and an Intrusion Report. The consultant was first hired by the company. After discovery of a breach, the consultant's statement of work was amended to provide that outside counsel would supervise the consultant's work. *Premera* argued that the subsequent reports were privileged and protected as work product. However the court found that the flaw in *Premera's* argument was that the consultant was hired to perform a scope of work for *Premera*, not for outside counsel, and noted that the scope of work did not change after the consultant was directed to report to outside counsel and label the reports privilege. (*Premera*, at 1245.)

The court distinguished the *Target* data breach because there was only one investigation in the *Premera* matter. The court also distinguished the *Experian* data breach in which outside counsel was hired by the company, and outside counsel had hired the consultant. Ultimately, the *Premera* court held that changing the supervision, without changing the scope of work, was not sufficient to render the later communications privileged and protected by the work product doctrine. However, the court did allow work product protection for documents generated by the forensic consultant working with outside counsel to the extent that they contained legal advice or mental impressions of counsel.

In *In re Experian Data Breach Litig.*, 2017 U.S. Dist. LEXIS 162891, the company's announcement of a data breach was followed by the filing of a class action. The company hired outside legal counsel and outside legal counsel hired the outside forensic consultant to investigate and provide information to legal counsel in order to allow legal counsel to provide legal advice to the company. The consultant provided a report not to the company, but to outside counsel only, who then shared the report with in-house counsel, all designed to facilitate the legal advice by outside counsel.

Importantly, the full report was not shared with the company's incident response team. When the class action plaintiffs sought the report in discovery, the court held that the documents were protected by the work product doctrine because the report was prepared in anticipation of litigation, even though that was not the company's only purpose. The court also rejected the argument that the hardship exception to the work product doctrine applied to allow plaintiff's discovery of the report, because plaintiffs had the exact same access to mirrored images of the servers as the consultant had.

Consultants should be hired and supervised by outside counsel, not by the incident response team, and not by the information security department. The consultant's statement of work should provide that the consultant will report to counsel pursuant to the scope of work set forth in the agreement, and that the consultant is being hired to assist counsel with providing legal advice. While it may be a better approach to have separate teams of consultants should conduct separate investigations as in the *Target* case, this may not always be possible due to expense.

COMMUNICATIONS REGARDING REMEDIATION

While remediation is a business function, communications with counsel are privileged if they actually contain legal advice or requests for legal advice, or where factual information is being provided to counsel for the purpose of allowing counsel to provide legal advice. As to remediation information provided by third parties, the privilege will apply only if the same criteria are applicable. (*Premera II*, at *XX; *Genesco, Inc. v. Visa U.S.A., Inc.*, No. 3:13-CV-00202 (M.D. Tenn. Mar 25, 2015).)

COMMON INTEREST?

It is important to consider the consequences of sharing information in connection with a cyber breach. In the *Experian* case the company had shared the forensic report with a co-defendant's counsel. The plaintiffs in the class action sought the report on the ground that the disclosure waived the work product doctrine. Ultimately, the court ruled that the sharing of the report with the co-defendant's attorneys under a joint defense agreement in redacted form did not result in a waiver of the work product doctrine. An effective joint defense agreement requires that the interests of the parties be aligned. Although a written common interest agreement is not required, having such an agreement would allow the parties to control specific aspects of the agreement, including remedies for breach of such an agreement.

THIRD PARTY VENDORS

Other third party vendors will be scrutinized by the court to determine whether they are providing non-legal business functions, or services related to litigation, such as electronic discovery related services, which would be protected. (*Premera*, at 1246-47.)

WAIVER

Under California law, voluntary disclosure of the contents of otherwise privileged communications constitutes a waiver of the privilege as to all communications on the same subject matter. (*Weil v. Investment, Research and Mgmt, Inc.*, 647 F.2d 18, 24 (9th Cir. 1981).)

In addition, the company may decide that it is advantageous to waive privilege and work product in favor of disclosing communications. This possible avenue should be kept in mind in the course of the data breach investigation as the data breach team is communicating.

CONCLUSION

Companies handling a data breach must address multiple considerations in order to preserve attorney client privilege and work product if litigation ensues. Thinking through and planning for the myriad issues before hand is an important part of planning and executing a competent response.

ETHICAL ROADMAP FOR DATA BREACH OR CYBERATTACK

By Procopio Partner and General Counsel Carole J. Buckner

ABA Formal Opinion 483 provides a roadmap regarding a lawyer's ethical obligations following a cyberattack or data breach involving confidential client information, where such information is misappropriated, destroyed or otherwise compromised, or where the data event impairs the lawyer's ability to perform client services. The ethical obligations of lawyers following a data breach depend on the lawyer's role, level of authority, and responsibility in the operation of a law firm.

All lawyers have duty of competence in understanding technology under Rule 1.1. (This refers to the ABA Model Rules of Professional Conduct.) Under Rules 5.1 and 5.3, lawyers with managerial authority must adopt reasonable measures to safeguard and monitor the security of electronically stored client information. A data breach does not necessarily mean that an ethical violation has occurred, given the ingenuity of cyber criminals. An ethical violation occurs only when an attorney fails to "undertake reasonable efforts to avoid data loss or to detect cyber intrusion, and that lack of reasonable effort is the cause of the breach." (ABA Formal Op. 483, 6.)

Once a breach occurs, a lawyer must act both promptly and reasonably to intervene to stop the breach and to mitigate damages. Having an incident response plan in place is key to addressing the situation in a coordinated manner to identify intrusion, assess the scope, determine whether data is accessed and/or compromised, quarantine threats and prevent exfiltration, and finally, restore the firm's network. (Id.) Having a predetermined team in place with a process ready to go is recommended, with either the lawyer taking necessary steps, if competent, or engaging qualified experts. After a breach, a lawyer should evaluate what steps should be taken to avoid a reoccurrence.

Mitigating a data breach involves a post-breach investigation to determine what occurred in terms of any data intrusion and loss. This allows the lawyer to address the duty of confidentiality under Rule 1.6. The Committee points out that this "is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable." (Id. at 9.) The Opinion also references the ABA Cybersecurity Handbook as to the emerging standard requiring an ongoing risk assessment and mitigation process. Whether to disclose to law enforcement may depend on the client's objections, risks to clients, and whether a report would aid in recovery of stolen information.

Finally, the Opinion addresses the nuances of client notification. Current clients must be advised of a data breach under Rule 1.4 if the breach involves material client confidential information. The notice must be sufficient to allow a client to decide what to do, if anything. As to former clients, while there is a duty to protect confidential information, there is no blackletter ethics rule requiring notification; however lawyers should consider other applicable law, particularly if personally identifiable information is involved. Lawyers should also follow a document retention policy that reduces the amount of information retained that relates to former clients.

This article was originally published November 26, 2018 in the San Diego County Bar Association Ethics in Brief blog (<https://www.sdcb.org/index.cfm?pg=Ethics-in-Brief-2018-1203>)



PROCOPIO
1117 S California Ave
Suite 200
Palo Alto, CA 94304
T. 650.645.9000
F. 619.235.0398

MINDY M. MORTON
mindy.morton@procopio.com

DEL MAR HEIGHTS
LAS VEGAS
PHOENIX
SAN DIEGO
SILICON VALLEY

April 10, 2019

VIA E-MAIL
ATTORNEY-CLIENT PRIVILEGED

Very Important Client

Re: Letter of Engagement

Dear Jane,

We are pleased that you have selected Procopio, Cory, Hargreaves & Savitch LLP (the "Firm") to serve as counsel for Very Important Client (the "Company"). We submit for the Company's approval the following provisions governing our engagement, as well as the additional provisions set forth in the enclosed "General Terms of Engagement" (the "General Terms"). Please note that to the extent there are inconsistencies between this letter and the General Terms, this letter will govern. If you have any questions about any of these provisions, or if you would like to discuss possible modifications, please contact me.

1. Identity of Client; Scope of Representation. The Firm's client, for purposes of this representation, and any additional services provided as contemplated by this agreement, is the Company, and not any of its incorporators, promoters, organizers, shareholders, partners, members, directors, officers, employees, subsidiaries, parents, other affiliates or insurers. This means we will not have a conflict of interest if we represent other clients of the Firm in matters in which those other clients are adverse to parties having any of the specified relationships with the Company.

The Company has engaged the Firm to advise and represent it in connection with an investigation regarding a data breach. If the Company requests, and we agree to provide, services with respect to additional matters, the terms of this letter and of the General Terms will apply to those additional services, unless superseded by another written agreement between us.

procopio.com

2. Fees and Expenses. Our fees will be based primarily on the amount of time spent by our lawyers, paralegals and other timekeepers on the Company's behalf. At present it is anticipated that Mindy Morton will be the attorney primarily responsible for the Company's matters; Ms. Morton's current hourly billing rate is \$____.

In addition to our fees, we will be entitled to payment or reimbursement for costs and expenses as set forth in the General Terms.

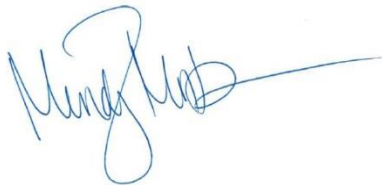
If you have any questions or concerns about any of our statements for fees and expenses, please contact me promptly so that we can discuss your questions or concerns, and I can respond appropriately.

3. Staffing. Although Mr. Femrite will be primarily responsible for this engagement, various portions of the work may be delegated to other partners of the Firm, associate, staff and of counsel lawyers, paralegals and other timekeepers as the Firm deems appropriate in the circumstances.

If the foregoing reflects your understanding of the terms and conditions of our representation, please indicate the Company's acceptance by executing a copy of this letter in the space provided below and returning it to our office. The individual signing this agreement on behalf of the Company represents and warrants that he or she has all requisite authority to bind the Company to the terms of this agreement.

We are pleased to have this opportunity to be of service and to work with the Company.

Very truly yours,



Mindy M. Morton

Attachment

Agreed to and accepted:

Date: _____

Very Important Client

By: _____

Name

Printed: _____

Title: _____

General Terms of Engagement

Thank you for selecting Procopio, Cory, Hargreaves & Savitch LLP (the “Firm”) to represent you. These General Terms of Engagement will apply to the relationship between the Firm and you, except as modified by the Letter of Engagement or other written agreement between you and the Firm. Experience has shown that the attorney-client relationship works best when there is a mutual understanding between the Firm and its client regarding the terms of that relationship. We encourage you to discuss with us any questions you may have at any time concerning these terms.

1. **Identity of Client.** The Firm undertakes to represent only the persons and entities it has expressly agreed to represent and has acknowledged or identified as its clients. If there is a Letter of Engagement or other agreement regarding representation, the Firm’s only client or clients in the matter to which the representation relates are the persons or entities identified as such in that Letter of Engagement or other agreement. A client’s incorporators, promoters, organizers, shareholders, partners, members, directors, officers, employees, subsidiaries, parents, other affiliates, family members, related interests, or insurers are referred to herein collectively as the client’s “Affiliates”. In agreeing to represent a client, the Firm does not undertake to represent any of that client’s Affiliates, and, unless otherwise expressly agreed by the Firm in writing, the client’s Affiliates will not be clients of the Firm.

2. **Communications.** Communications between you and the Firm may be made in person, via telephone, including via mobile phone, via facsimile or via electronic mail, and you hereby authorize communication by all such means. Please understand that electronic communication is not an absolutely secure method of communication. You acknowledge and accept the risks inherent in such communication and authorize the Firm to use electronic communication means to communicate with you or others necessary to effectively represent you. If there are certain documents with respect to which you wish to maintain absolute confidentiality, it is imperative that you advise the Firm in writing not to send those documents via electronic communications, and the Firm will comply with your request. At no time should you communicate with the Firm utilizing technology provided by your employer, nor should you communicate with us on any shared device that belongs to any third party or entity. Finally, do not communicate about any matter which is the subject of the Firm’s representation on social media (Facebook, Twitter, Tumblr, Flickr, Skype and the like). Communications and information shared on social media are not private.

3. **Engagement of the Firm.** You understand that no particular result, compensation or recovery is, or can be, guaranteed or promised by the Firm in rendering legal services requested by you for any particular matter. The Firm undertakes only to render legal services requested by you and accepted by the Firm. It is understood that you are not relying on the Firm for business, investment or accounting decisions or to investigate the character or credit of persons with whom you may be dealing.

4. **Post-Engagement Matters.** You have engaged the Firm to provide legal services in connection with the specific matter described in the Letter of Engagement. After completion of the matter, changes may occur in applicable laws or regulations that could have an impact on your future rights and liabilities. Unless you engage the Firm to provide additional advice on issues arising from the matter, the Firm has no continuing obligation to advise you with respect to future developments. This also includes any continuing obligation, whether during or after our engagement, to monitor future filings that may be necessary, including, but not limited to, filings of annual reports and returns, filings under the Uniform Commercial Code (including a Continuation Statement with respect to any UCC-1 Financing Statement), renewals of judgments, and renewals of patents or trademarks.

5. **Fees.** Unless a separate Alternative Fee Agreement is approved in writing by you and the Firm, the Firm's compensation for legal services rendered for your matters ("Fees") will not be a fixed amount but rather will be an amount based primarily upon the time devoted to your matters, including, but not limited to, consultations, correspondence, meetings, telephone calls, negotiations, factual investigations and analyses, legal research and analyses, document preparation and revision, court appearances, travel on your behalf and all other work related to your matters. The hourly billing rates of the Firm's lawyers and paralegals vary depending upon their experience, and the Firm's total fees vary depending upon the novelty and difficulty of the questions involved, the skill required to perform the legal service properly, the skill and experience of opposing counsel, the responsibilities assumed, the time limitations imposed by you or the circumstances, the seriousness of the consequences, the results obtained and other considerations permitted or required by applicable Rules of Professional Conduct. The Firm's hourly rates are subject to change periodically, usually on January 1. The Firm may utilize the services of independent contract attorneys on your matters and may charge you more than the Firm pays such attorneys for their services. You are responsible for, and will pay, all Fees. In certain litigation matters, the court has the power to order that your fees are to be reimbursed, in whole or in part, by the other party; however, you are responsible for all Fees without regard to the amount of any fee award by the court and without regard to whether those Fees are ultimately reimbursed to you by the other party.

6. **Costs and Expenses.** In addition to our Fees, the Firm will be entitled to payment or reimbursement for costs and expenses incurred in performing our services, including, but not limited to, photocopying, messenger and delivery service, computerized research, outside research and document retrieval services, travel (including mileage, parking, airfare, lodging, meals and ground transportation), communication expenses (e.g., international long distance telephone charges, telecopy charges), clerical overtime, court costs, filing fees and fees of other third parties consulted by the Firm in the course of its representation of you. Some of these charges may include a mark-up for overhead and administration. Electronically Stored Information (ESI) processing conducted as a necessary part of the Firm's representation of you will be billed to you as a Cost. The Firm maintains its own in-house ESI Data Processing Center. In some instances, ESI processing may be outsourced to a qualified ESI processing vendor. In such instances, you, and not the Firm, shall be responsible for the timely payment of invoices received from such outside vendor. The Firm reserves the right to require you to (i) engage or pay directly any third party consultant, expert witness, vendor or other party engaged on your behalf, (ii) pay all outside costs directly to the vendor and/or (iii) provide Firm a cash deposit for Costs to be incurred.

7. **Credit Reports.** By entering into the Letter of Engagement, you authorize the Firm to obtain consumer and commercial credit reports as it deems appropriate.

8. **Deposit for Fees and Costs and Expenses.** You may be required to deposit with the Firm an initial deposit to be applied automatically to pay Fees and Costs incurred on your behalf. This deposit does not represent an estimate of anticipated Fees and Costs. The Firm reserves the right at any time to require that the deposit be replenished or that a new deposit in an amount determined by the Firm be made to apply against future Fees and Costs, which additional deposit may be in an amount the Firm then estimates may be necessary to complete the representation. Any unused portion of your initial or additional deposit will be returned upon completion or termination of the Firm's services. Any deposit made by you shall be deposited into the Firm's general trust account. Under applicable law, interest on attorneys' trust accounts for clients is payable to a State fund for legal services to the indigent, unless clients specifically elect separate trust accounts. If you desire to have your deposit placed in a trust account with interest payable to you, you must so advise the Firm and provide to the Firm your taxpayer identification number on a W-9 form. The Firm's trust accounts are held in approved financial institutions and bear interest at the bank's rates for this type of account. The bank, however, is subject to change at the Firm's

discretion. Your execution of our Letter of Engagement constitutes your consent to the deposit of your initial deposit and any subsequent deposits by you into one of the Firm's trust accounts in a financial institution.

9. **Third-Party Payment of Fees and Costs.** You may arrange for a third-party to be responsible for payment of Fees and Costs that will become due hereunder. However, if the third-party fails for any reason to pay the Firm's statements as they become due, you will remain responsible for payment of such. Please understand that the attorney/client relationship will exist only between the Firm and you and that the third-party will have no right to information regarding your matter nor any right to direct the Firm in providing the services herein unless specifically approved by you. Your execution of the Letter of Engagement shall constitute your acknowledgment that you have been fully advised of this arrangement and have consented to such. You should also understand that if you arrange for a third-party to be responsible for payment of Fees and Costs, then the Firm is authorized to direct its invoices to said third-party, and you acknowledge that said invoices may contain confidential or privileged information regarding the Firm's representation of you.

10. **Monthly Statements.** Unless a different billing cycle is approved by the Firm in writing, the Firm generally will issue its statements for Fees and Costs on a monthly basis. The amounts due as stated on the Firm's statements shall be deemed to be correct, conclusive and binding on you unless you notify the Firm in writing within thirty (30) days from the date of the particular invoice that you dispute such charge. The Firm's statements are due and payable upon receipt. All Fees and Costs unpaid for more than thirty (30) days bear interest at the rate of twelve percent (12%) per annum on the unpaid amount. If you fail to pay the Firm's statements within thirty (30) days of the statement date, the Firm reserves the right to require an additional deposit in an amount determined by the Firm or to terminate representation. In addition, in the event you fail to pay the Firm's statements within thirty (30) days of the statement date, the Firm reserves the right to require a current financial statement from you and further reserves the right immediately to cease advancing any Costs on your behalf with respect to the matters in which the Firm represents you.

11. **Estimates.** Although the Firm may from time to time, for your convenience, provide estimates of fees or expenses that we anticipate will be incurred, these estimates are subject to unforeseen circumstances and are by their nature inexact. As a result, the actual fees and expenses most likely will be more or less than the Firm's estimate. No fee estimate shall be deemed or construed to establish a fixed, maximum or minimum fee, and the Firm will not otherwise be bound by any estimates, unless expressly otherwise provided by written agreement with you. You shall pay the Firm's fees and costs actually billed to you regardless of any estimate.

12. **Preservation of Evidence.** In the event you are retaining the services of the Firm for purposes of representation in a litigation or arbitration matter or in a matter in which you may make a claim against a third party or a third party may make a claim against you, it is imperative that you secure and maintain all documents, both written and electronic, including emails and voicemails, which may be relevant to the claim or potential claim. Preservation extends not only to your office computers, but also to cloud storage locations, personal computers, laptops, smartphones and home computers on which information relevant to the claim or potential claim may be present. Preservation also extends to any information which you may have posted on any social media website; you may not alter or delete any such information. It is imperative that you confer with the Firm attorney responsible for your matter immediately concerning preservation and possible collection of all potentially relevant documents and information and that a "Litigation Hold" be properly maintained until the representation has been concluded.

13. **Arbitration and Waiver of Jury Trial.**

a. Any dispute between you and the Firm arising out of, or relating to, the Letter of Engagement or any services rendered pursuant to such, including, without limitation, claims of malpractice, errors or omissions, negligence, breach of contract, or any other claim of any kind regardless of the facts or legal theories, shall be finally and exclusively settled by mandatory binding arbitration in San Diego, California, before an arbitrator selected from and administered by the San Diego office of Judicate West in accordance with Judicate West's then existing rules of practice and procedure. Such arbitration shall be conducted in accordance with California Code of Civil Procedure § 1282 *et seq.*, including, but not limited to, Section 1283.05, with each party to bear its own costs and attorneys' fees and disbursements. Such arbitration shall be conducted before a single arbitrator. The arbitrator shall have no authority to rescind, reform or modify the Letter of Engagement. The arbitrator shall be exclusively authorized to determine whether the provisions of this section apply to a dispute in which case the provisions of this section shall provide the exclusive means for obtaining relief for any claim arising out of or relating to such a dispute. The arbitrator shall not have the power to commit errors of law or legal reasoning, and the award may be vacated or corrected on appeal to a court of competent jurisdiction, for any such error. A judgment on a binding arbitration award may be entered in the Superior Court for the County of San Diego, State of California.

b. Notwithstanding the binding arbitration agreement set forth in subparagraph (a) above, in the event of a fee dispute between the Firm and you, you are entitled to participate in fee arbitration through the San Diego County Bar Association, pursuant to Business & Professions Code §§ 6200-6206. In the event you elect not to participate in fee arbitration pursuant to the Business & Professions Code, the Firm and you will resolve the fee dispute pursuant to the binding arbitration agreement set forth in subparagraph (a) above. If you do elect to participate in such a fee arbitration but reject an award issued therein by, among other things, requesting a trial *de novo*, the trial *de novo* will consist of a binding arbitration conducted pursuant to the agreement set forth in subparagraph (a) above.

c. You and the Firm mutually acknowledge that, by this agreement to arbitrate, you and the Firm each irrevocably waive the right to a court or a jury trial.

d. You have the right to consult with separate legal counsel at any time as to any matter, including whether to enter into the Letter of Engagement and to consent to this agreement to arbitrate.

14. **Termination.** You have the right to discharge the Firm at any time upon advance written notice to the Firm. The Firm reserves the right to withdraw as legal counsel to you at any time upon written notice to you. If the Firm withdraws or is terminated, the following provisions shall govern the rights and duties of Client and the Firm:

- a. The Firm will reasonably cooperate with you to retain other counsel;
- b. You will provide all consents reasonably necessary to effect such withdrawal or termination;
- c. Files for the matter shall be made available to you;
- d. You shall pay to the Firm all costs incurred by the Firm to provide said files to you or to your new counsel, including costs of labor, time and out-of-pocket expenses associated with copying, retrieving and processing your files, in both paper and electronic form; and

e. You shall pay promptly upon receipt of an invoice thereafter all Fees and Costs incurred prior to termination.

Please note that in the event the Firm has provided no legal services to you for a period of twelve (12) consecutive months, the representation of you in the matter in which you engaged the Firm shall be deemed concluded and the attorney-client relationship between you and the Firm shall be deemed terminated.

15. **Retention of Files.** After the Firm's services conclude, the Firm will, upon your request, and at your cost, deliver files for your matters to you, along with any funds or property of yours in the Firm's possession. If you request delivery of your files, you agree to pay all costs of labor, time and out-of-pocket costs associated with copying, retrieving and processing such files in both paper and electronic form. If you do not request the file for your matter, the Firm will retain it, either in its original form or on microfilm, microfiche, disk or electronically for a period of ten (10) years after conclusion of the representation in the matter. The Firm undertakes no obligation to retain electronic mail or voicemail. If you do not request delivery of the file for the matter before the end of the ten-year period, the Firm will have no further obligation to retain the file and may, at its discretion, destroy it without further notice to you. At any point during the ten-year period, you may request delivery of the file. The Firm reserves the right to purge from your file at any time attorney notes, research memoranda and other work product of Firm attorneys.

16. **Insurance.** If you have insurance, there may be policy provisions that provide coverage for potential liability and/or attorneys' fees and costs applicable to the legal services to be rendered. It is your responsibility to advise the Firm whether any such insurance exists. The Firm maintains errors and omissions insurance coverage.

17. **Promotional and Publicity.** You agree that the Firm may identify you as a client of the Firm on its website, in marketing materials and to third parties. You hereby grant to the Firm the right and license to use, copy and publish your company name and logo on the Firm's website and in newspapers, journals, other media and/or marketing materials describing the Firm's services for the purpose of identifying you as a client of the Firm. In addition, after public announcement of any material transaction consummated with its assistance, the Firm may include your name and a description of the services provided on its website and in marketing materials which shall refer solely to publicly available information regarding the transaction. Such information may also be disclosed to current or prospective clients of the Firm and to other third parties.

18. **General.** No change, waiver or modification of any of the terms of these General Terms of Engagement or the Letter of Engagement shall be effective unless confirmed in writing and executed by the Firm. The Letter of Engagement and these General Terms of Engagement set forth the entire agreement between the Firm and you concerning your engagement of the Firm. The Firm has not made any representations or promises (including binding estimates of Fees or Costs) to you. If any provision of the Letter of Engagement or of these General Terms of Engagement is invalidated by a final judgment, the remaining provisions shall remain in full force and effect. The Letter of Engagement and these General Terms of Engagement are binding on the respective successors and assigns of the Firm and you.



Sabrina Fève joined the San Diego US Attorney's Office in 2007, after spending several years practicing civil litigation in San Francisco. Since 2009, she has worked in the National Security and Cybercrime Section, where she serves as the Computer Hacking and Intellectual Property Coordinator, the National Security Cybercrime Specialist, and the Identity Theft Coordinator. In addition to overseeing cybercrime and national security investigations in San Diego, Sabrina also represents the Department of Justice on the National Institute of Standards and Technology's Digital Evidence Subcommittee, which is tasked with crafting forensic standards for the collection and use of electronic evidence.

Contact Info:

Sabrina Fève
619.546.6786 (direct)
sabrina.feve@usdoj.gov



Tim Hamon is a Senior Forensics Examiner for the FBI, assigned to San Diego's Regional Computer Forensics Laboratory (RCFL). Since 2001, he has conducted hundreds of computer examinations, testified dozens of times, designed, researched and tested tools used by the FBI's computer forensics program, and created the FBI's digital forensic fundamentals training curriculum.

Since 2008, Mr. Hamon has been assigned to San Diego's criminal cyber squad where he conducts cyber-specific forensic examinations and provides technical expertise and analysis for criminal cyber cases.

Mr. Hamon has a master's degree in software engineering and teaches digital forensics at the FBI academy.

Contact Info:

Tim Hamon
858.320.8375 (direct)
858.583.3423 (mobile)
thamon@rcfl.gov



MARTY LORENZO

**Vice President Legal Affairs and Assistant Corporate Secretary
Petco**

Marty is a forward-thinking servant leader who solves complex problems and leads cross-disciplinary teams. He integrates the sound judgment of a proven legal advisor, the strategic outlook of an entrepreneur, and the results-oriented discipline of a senior military professional. As Vice President Legal Affairs at Petco, he collaborates with other senior executives and heads of business units to develop and execute innovative, efficient and cost-effective strategies. Marty is the lead lawyer on mergers and acquisitions, joint ventures, and business development projects. He manages complex litigation and advises on corporate governance matters. Marty has responsibility for the team that provides legal support to Petco's real estate business and he is lead counsel to Petco's growing pet health services business, including expansion of veterinary hospitals. Marty is Petco's lead attorney on privacy matters and co-leads the Chapter on Data Privacy, Security and Controls.

Prior to joining Petco, Marty had a long career in private practice with Am Law 100 firms representing international companies and boards of directors from the United States, Singapore, Australia, Germany and the Philippines. His practice covered a wide variety of business issues and strategic transactions such as mergers and acquisitions, capital formation and securities offerings, international expansion, technology licensing and corporate governance. Marty regularly served as outside general counsel for many of his clients across various industries. He provided leadership on product development, human resource management, budget and finance matters, joint ventures and intellectual property strategy.

Marty is a combat veteran who served in Operations Desert Shield/Storm and Operations Enduring/Iraqi Freedom and he is a Major in the U.S. Marine Corps Reserves. Marty is an Executive Sponsor of Petco's Military and Veteran Resource Group.

Marty earned his B.A. *cum laude* from the University of San Diego and his J.D. from the University of San Diego School of Law.