2016 CLM Annual Conference
April 6-8, 2016
Orlando, FL

Stop Writing Exhibits For Data-Breach Plaintiffs

I. Importance and Challenges of Preserving Privilege

A. Importance

The importance of preserving the attorney-client privilege is difficult to overemphasize. This is particularly true in connection with preserving the attorney-client privilege over communications regarding data breaches, which may result in significant – and perhaps material or even debilitating – fines, penalties, costs, and damages.

1. Need To Be Candid About Risks

Businesses need to be clear-eyed and candid about their cybersecurity risks, both before and after a breach or incident. There is no way to prepare adequately for a breach or incident without identifying, communicating about, and addressing the true risks. This is not the time to be Pollyannaish or even mildly optimistic. Technological and legal risks abound, and accurate risk assessments are a critical component of a meaningful cybersecurity program. Moreover, it may seem tautological, but businesses cannot address their risks after a breach or incident without knowing what those risks truly are.

2. Need To Protect Against Disclosure

Candid communications often (indeed, necessarily) will be less than complimentary regarding cyber readiness. Every business has multiple technological and legal points of vulnerability, and frequently there are palpable gaps between the current state of affairs and real cybersecurity preparedness. When these gaps are memorialized in documents – whether emails, memos, policies, plans, tests, or otherwise – those documents become potentially devastating weaponry when secured and used by plaintiffs and/or regulators. It is vital, therefore, to protect these documents from potential disclosure in the course of prospective litigation or regulatory investigations. And protecting these documents from disclosure requires careful planning and communications management *before* they are written and transmitted.

B. Challenges

1. Burdens of Establishing the Attorney-Client Privilege

It is axiomatic that the party asserting the privilege bears the burden of establishing its applicability. Although the law differs among the states, and between state and federal courts, the attorney-client privilege typically applies only if the communication was: (a) between attorney and client, and (b) for purposes of seeking or rendering legal advice.

Most communications serve a dual purpose, particularly those to or from inside counsel, who frequently wear multiple hats and advise clients on business as well as legal matters. For those mixed-purpose communications, the majority rule provides that the privilege applies only if their "primary purpose" was the provision of legal (rather than business) advice.

The "primary purpose" of a communication often is difficult to discern, let alone prove to a judge. This is particularly true with regard to communications regarding pre-breach preparations and post-breach investigations and mitigation measures. These areas encompass multiple tasks that span the spectrum between legal and business matters, with many tasks involving mixed legal-business issues that fall into the vast gray area of that spectrum.

Further complicating matters is the difficulty of establishing the attorney-client privilege in the context of corporate communications. Whose employees' communications, after all, are entitled to the privilege? Courts take varying approach in addressing this inquiry. Some courts follow the "control group" test, which extends the privilege only to those employees who exercise decision-making authority and/or control. Other courts, including federal courts (following the seminar *Upjohn* decision by the U.S. Supreme Court), extend the privilege broadly to all employees whose communications fall within the subject matter and scope of their employment responsibilities.

Another layer of complexity is the challenge of avoiding waiver. It is commonly held that the corporation, not the employees or the corporation's attorney, holds the privilege. Hence only the corporation can waive it. However, a communication may lose its privileged status if an employee distributes it beyond the group of appropriate recipients (*e.g.*, the control group, if that test applies, or to someone whose job responsibilities do not necessitate being in the communications loop).

2. Burdens of Establishing The Work-Product Doctrine

The work-product doctrine may protect communications after a breach, when litigation is reasonably foreseeable if not frequently inevitable. Like the attorney-client communication privilege, however, the work-product doctrine is difficult to assert and sustain, and it depends on creating and managing the information carefully.

The black-letter rule is that the work-product doctrine protects information that is prepared in anticipation of litigation or for trial. That said, there are variations of the doctrine among the states, so insurers and insureds need to be cognizant of the specific applicable rules and case law. The doctrine protects information created by the attorney, or by another at the attorney's direction, which itself may be difficult to establish if the attorney's directive was not clear and definitive before the information was generated.

Also like the attorney-client privilege, there are substantial challenges if the attorney was acting in a dual-role capacity, as in-house counsel often does. Perhaps, for example, information was generated for purposes of regulatory compliance, and/or to avoid (rather than defend) litigation or regulatory action. Such dual-purpose information often falls outside the protective ambit of the work-product doctrine.

The underlying theme is that attorneys must create and manage their communications and other information very carefully in order to enhance the prospects of protecting them from disclosure. Outside counsel must be involved in order to establish that the communications and information directly related to the provision of legal advice and/or the defense of prospective or actual litigation. Then the communications and information must be managed so as to reduce the ever-looming risks of waiver.

II. Preserving the Privilege Pre-Breach

Most businesses recognize the critical importance of attempting to reduce their risks and potential exposure before they suffer data breaches or incidents. As with most other risks, preventive measures are critically important. Such measures may not succeed in avoiding intentional intrusions or negligent releases of data, but they may reduce the magnitude of the data losses as well as the potential exposure in damages, penalties, and reputational harm.

A strong risk-prevention program should have expansive technological, procedural, and legal components. Each business holding or transmitting sensitive data, for example, needs to undertake a comprehensive vulnerability assessment, implement technological security controls to anticipate and detect intrusions, build a solid risk-management program, craft a broad yet enterprise-specific incident-response plan, undertake realistic table-top exercises to test that plan, develop security policies that cover all potential points of intrusion, and train employees on those policies.

To the extent possible, moreover, all of these measures need to be undertaken with the protections of the attorney-client communications privilege. Each of these initiatives necessarily generates candid and often-critical communications and information about the gaps in a business's cyber-readiness. If these communications and information are not protected, therefore, they may become top exhibits for an adversary in a lawsuit or regulatory inquiry.

A. Assessing Risks

Breaches or incidents often are the impetus for businesses to focus closely on their legal exposure. By that time, however, the objective is to minimize or mitigate the damages. It makes much more sense, for both insurers and insureds, to examine legal compliance before the damage is done through a data breach or incident. The analogy to other insured risks is simple yet probative. Better to focus on fire readiness before the fire, on health before the illness, on protective contractual provisions before a breach. And assessing compliance with legal mandates is necessary in order to identify and implement the necessary preventive measures.

But risks assessments, by their very nature, highlight deficiencies in a business's cybersecurity readiness. Accordingly, outside counsel should be involved at the outset – initiating the risk assessment for purposes of assisting counsel in the provision of legal advice, managing communications about the assessment so that they flow through outside counsel and across the proper channels of appropriate recipients, and ensuring that employees are maintaining the information so as to reduce the risks of potential waiver.

B. Implementing Protective Measures

1. Cyber Insurance

Cyber insurance is a prevalent part of the risk-reduction landscape. The insurance-application process, however, may be the first time that a business does a deep-dive into its cyber-readiness. Accordingly, outside counsel should be involved in that process, helping the business undertake and complete the insurance-application process. All of these communications, of course, cannot be protected by the privilege, particularly anything that it shared with the insurance company, such as the application itself. Nevertheless, outside counsel may help prevent the disclosure of potentially harmful communications and information sparked by the process of acquiring cyber insurance.

2. Cyber Policies

Strong data-security policies are the backbone of any breach-readiness plan. These policies should encompass the multitude of ways that data is received, accessed, stored, transmitted, and used across the entire enterprise. Policies, for example, should cover internal and remote access, passwords, encryption, email usage and storage, mobile devices in and outside the workplace, network security, physical security, legal compliance (and its many facets), monitoring and logging, and many other areas depending on the business and the data it touches. Each business is unique in all of these respects, and the policies should be crafted and fine-tuned accordingly. Given the complexities, generic policies represent, at best, a start.

Outside counsel should be directly involved in the process of drafting and revising

these policies, so as to enhance the prospects of protecting those materials from subsequent disclosure. Otherwise, a plaintiff or regulator may have access to the policies' lifecycles, with the ability to critique – with the benefit of hindsight – the various manners in which the policies could or should have been crafted better or differently. It is highly advisable to utilize the attorney-client communication privilege to prevent prospective adversaries from engaging in such Monday-morning quarterbacking.

3. Incident-Response Plans

The same principles hold true for incident-response plans, which should be tailored to each business's particular structure, data, and legal duties. The plans are roadmaps for acting quickly and effectively in the event of a potential breach and incident. As such, these plans should carefully delineate who gets involved and when, what steps must be taken to investigate and address the potential breach or incident (particularly in the critical early stages), and how information is to be communicated internally and externally. One central commonality is that all of these plans should involve outside counsel, often labeled as a "breach coach," to coordinate and quarterback the response to maximize the protection of information where appropriate under the attorney-client privilege and work-product doctrine.

As with policies that are not communicated and understood, incident-response plans have little or no efficacy if they are not used and tested before a real breach or incident. Businesses should deploy realistic table-top exercises to rehearse the appropriate response to various foreseeable breaches or incidents. It is far preferable to identify and plugs gaps in the plan during a hypothetical exercise than fall through them when it really counts.

All of these tasks will generate documents and information that may become powerful fodder for an adversary. Again, therefore, outside counsel should initiate, coordinate, and manage the development and testing of incident-response plans.

4. Other Steps To Foster Enterprise-Wide Security Culture

The underlying theme of all of these preventive measures is to foster a true security culture across the entire enterprise. There are many additional ways to create that atmosphere. Corporate executives should be leading the charge, and they should be active and visible sponsors of preventive measures across the organization. The same is true for outside counsel, who should work with these executives so as to help protect the resulting documents and information from potential disclosure to prospective adversaries.

III. Preserving the Privilege Post-Breach (20 minutes)

A. Internal Investigations

Promptly upon discovering a potential data breach or incident, a critical first step is to initiate an investigation. The central objectives are to determine the nature and scope of the intrusion or loss, and to take tangible measures to stop or at least mitigate the resulting harm. The incident-response plan, in fact, is the roadmap for meeting these objectives. Once these objectives are satisfied, additional investigatory measures will be necessary in order to develop and implement strengthened data protections, communicate with regulators and other interested constituencies, and prepare for potential litigation in administrative tribunals and courts.

It also is well-recognized that businesses need to protect their communications as much as possible during these investigations. It is in everyone's interest to communicate openly and critically, and the incentives to do so are directly related to the extent to which those communications are protected from disclosure to regulators and the outside world generally.

Outside counsel, therefore, typically are involved as "breach coaches" to quarterback the investigations and protect associated communications, to the extent legally possible, under the rubrics of the attorney-client privilege and work-product doctrine. Courts generally recognize the privileged and protected nature of these communications when requested and/or directed by outside counsel for purposes of assessing legal risks and counseling on legal issues. By contrast, courts exhibit increased skepticism when adjudicating privilege assertions over communications that did not involve counsel, or even those that involved in-house counsel (whose communications are more easily characterized as undertaken for business purposes rather than legal advice).

Merely involving outside counsel is necessary but not sufficient. Outside counsel needs to initiate the process by making clear – in writing – that the investigation is undertaken for purposes of assisting counsel in the provision of legal advice as well as the defense of litigation. In addition, outside counsel must coordinate and manage all consequent communications, which should run to and through outside counsel. All communications and information also must be labeled, to the extent possible, as attorney-client privileged and/or attorney work product.

Outside counsel also must quarterback the engagement of, and communications with, third parties whose work is central to any meaningful investigation, such as the data-forensics firm which is retained to investigate the magnitude and scope of the breach or incident. This initiative requires outside counsel to execute engagement letters with

the third-parties, and those letters should make abundantly clear that those parties are engaged for purposes of assisting counsel to provide legal advice and defend against potential (if not pending) claims.

It is impossible, of course, to protect all investigatory documents and information from disclosure under the attorney-client privilege and/or work-product doctrine. Not everything is created and generated to aid counsel or defend against litigation. Rather, much work is focused on the business needs of addressing and remediating a breach. However, it is incumbent on a business to isolate and protect the communications and information that bear directly on the legal vulnerabilities and exposure caused by a breach or incident, and to involve outside counsel so that those communications and information receive the greatest potential level of protection from disclosure. Those are the communications and information that a prospective adversary will find most useful and powerful, and they should receive the greatest protective attention and focus.

B. Notification Compliance

One of the most urgent post-breach tasks involves compliance with applicable notification laws of all states. 47 states have such laws, which vary in multiple respects, including the data they cover, the time within which notification must be provided, the content of the mandatory notification, and the fines or penalties for non-compliance. Yet businesses must comply with all such laws in every state where affected persons reside.

These tasks may seem obvious, but even the most sophisticated businesses are getting into hot water for alleged failures to do so, such as the recent example of Anthem, which received a public rebuke by ten state attorneys general for, to borrow a phrase from *Cool Hand Luke*, a "failure to communicate."

Outside counsel must be involved from the outset in developing and implementing a notification plan. While plaintiffs and regulators clearly may (and often invariably will) challenge the adequacy of a business's notification efforts, the strategic decision-making that led to those efforts should be protected from disclosure. Yet that may be difficult, if not impossible, if outside counsel was not directly involved in developing, implementing, and managing the communications regarding that plan.

C. Litigation or Regulatory Investigations

It goes without saying that outside counsel must lead the charge in any post-breach litigation or regulatory investigations. Despite its obviousness, this principle sometimes does not receive the attention that it deserves. If outside counsel is not

involved and attentive, employees may generate communications and information that are not protected by the attorney-client privilege or work-product doctrine, including communications and information that may be directly pertinent to (and very helpful to the adversary in) the underlying case. Accordingly, outside counsel should make clear – in litigation-hold notices and other internal memoranda – that employees should avoid any written communications (including of course emails) regarding the case, and that employees should communicate only as specifically requested by outside counsel.

D. Incorporating Lessons Learned

There are many lessons learned after a breach or incident, and they should be incorporated into the fabric of a business's pre-breach preparations. Outside counsel also should be involved in this process, which is part and parcel of the provision of legal advice and guidance. If these efforts are done without outside counsel's involvement, and outside the scope of the attorney-client communication privilege, they may become helpful to a prospective adversary. After all, it is powerful to criticize a business for failing to understand and appreciate a risk about which it knew (or should have known), and for failing to fix a deficiency that it knew (or should have known) needed fixing.

E. Case Study: The Target Litigation

The notorious Target case provides an excellent case study for the importance and challenges of preventing the disclosure of post-breach documents through the attorney-client privilege and work-product doctrine. On October 23, 2015, a federal magistrate judge sided with Target and protected the vast majority of its post-breach investigatory documents, many of which were generated by its "Data Breach Task Force." Fortunately for Target, this group was created at the request of Target's outside counsel for purposes of assisting them in understanding and addressing Target's legal risks.

Specifically, the magistrate judge held that Target established "that the work of the data breach task force was focused not on remediation of the breach, as plaintiffs contend, but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice and prepare to defend the company in litigation that was already pending and was reasonably expected to follow."

This result was not accidental. Target's outside counsel did the necessary work to establish the requisite foundation to protect the privileged and protected nature of these communications. Both insurers and insurers should take heed to follow similar steps and ensure that investigatory communications occur under a protective privileged umbrella.