Data Breaches: The Attorney-Client Privilege and the Work Product Doctrine

MARGARET A. DALE AND YASMIN M. EMRANI, PROSKAUER ROSE LLP, WITH PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

A Practice Note discussing the steps organizations should take to shield documents and communications from disclosure following a data breach under the attorney-client privilege and the work product doctrine. The Note discusses engaging counsel to lead data breach investigations, training employees and management, tracking litigation, retaining third parties, implementing a dual-track investigation, and using joint defense agreements.

Plaintiffs are increasingly filing class actions against companies that have suffered data breaches, especially those affecting personal information. Regulatory inquires often follow. Litigants typically seek a broad range of documents in discovery about data breaches, including forensic reports, analyses, and communications.

Organizations facing a data breach must understand how to shield from discovery documents protected by the attorney-client privilege and the work product doctrine. Simple missteps can easily destroy or waive these protections, for example, if organizations:

- Share protected information with third parties to whom counsel do not need to provide legal advice.
- Combine protected information with communications reflecting ordinary business advice.
- Do not properly retain and supervise third parties, such as computer forensics and other service providers, to investigate the data breach.

This Note describes the steps organizations can take to preserve the attorney-client privilege and work product protection for communications made or documents created after a data breach.

ATTORNEY-CLIENT PRIVILEGE

The attorney-client privilege protects confidential communications between attorneys and their clients that relate to the request for, or rendering of, legal advice. Several types of communications meet this standard, including:

- A client's request for legal advice from a lawyer.
- A client's communication to a lawyer of facts the lawyer needs to give advice.
- A lawyer's request for facts that the lawyer needs to give legal advice.
- A lawyer's legal advice.

The US Supreme Court in *Upjohn Co. v. United States* recognized that the attorney-client privilege applies to communications between corporate counsel and a corporation's employees when:

- Employees communicate with counsel at the direction of their corporate superiors.
- Employees communicate with counsel to:
  - secure legal advice for the corporation; or
  - provide facts that the lawyer needs to give the corporation legal advice.
- Employees are sufficiently aware that counsel or their agent is questioning them so that the corporation may obtain legal advice.
- The communication concerns matters within the scope of the employees' corporate duties.
- The communication is confidential.

(449 U.S. 383, 390-97 (1981).)

Courts have held that the privilege also extends to:

- Communications between corporate counsel and former employees, if the discussion relates to the former employee's conduct and knowledge gained during employment (*In re Gen. Motors LLC Ignition Switch Litig.*, 80 F. Supp. 3d 521, 526 (S.D.N.Y. 2015)).
- Counsel's communications with agents and consultants whom counsel retain to help provide legal advice to the client (*United States v. Kovel*, 296 F.2d 918, 921 (2d Cir. 1961)).

For more information on the scope of the attorney-client privilege, see Practice Note, Attorney-Client Privilege: Scope of Protection (7-502-9405).

WORK PRODUCT DOCTRINE

The work product doctrine protects from disclosure to third parties documents and tangible things prepared in anticipation of litigation or trial by or for another party or its representative (FRCP 26(b)(3)(A)). The work product doctrine protects documents prepared in anticipation of litigation by:

- The client.
- The client's attorney.
- Agents and consultants for the client and the attorney.
- Experts retained by the client or the attorney.

When determining whether the work product doctrine applies, courts interpret "anticipation of litigation" to mean that a document:

- Was created because of anticipated litigation.
- Would not have been created in substantially similar form but for the prospect of that litigation.

(*In re Grand Jury Subpoena*, 357 F.3d 900, 908 (9th Cir. 2004).)

For more information on the work product doctrine, see Practice Notes, Work Product Doctrine: Protected Information (6-504-4171) and Work Product Doctrine: Basic Principles (8-504-4165).

TYPES OF WORK PRODUCT

The two types of work product recognized by US law are:

- **Fact work product.** Examples of documents deserving fact work product protection include:
  - a lawyer's time slips and billing records;
  - a litigant's list of confidential witnesses;
  - pictures of a pertinent place;
  - a company's litigation hold notice;
  - documents containing logistical information, such as deposition dates; and
  - general factual chronologies.
- **Opinion work product.** Documents that constitute opinion work product include those that contain an attorney's or other party representative's:
  - mental impressions;
  - conclusions;
  - opinions; or
  - legal theories.

(FRCP 26(b)(3)(B).)

Courts generally provide almost absolute protection to opinion work product, holding that the requesting party can discover it only in extraordinary circumstances (see *In re Cendant Corp. Sec. Litig.*, 343 F.3d 658, 664 (3d Cir. 2003) (collecting cases)).

However, a requesting party can overcome fact work product protection if it shows both:

- A substantial need for the fact work product materials.
- That it cannot obtain a substantial equivalent of the materials by any other means without undue hardship.

(FRCP 26(b)(3)(A)(ii).)

For more on the difference between fact work product and opinion work product, see Practice Note, Work Product Doctrine: Protected Information (6-504-4171).

WAIVING THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK PRODUCT PROTECTION

Disclosing privileged communications to anyone outside the company typically waives attorney-client privilege protection unless the disclosure of privileged information is to a third party retained to help provide legal advice.

The work product doctrine is not as fragile as the attorney-client privilege because disclosing work product to those outside the company does not automatically waive this protection. Instead, courts typically find that an organization's disclosure to third parties only waives the work product protection if the organization discloses information to adversaries or third parties that might share the work product with adversaries.

For more information on waiving the attorney-privilege and the work product protection, see Practice Notes, Attorney-Client Privilege: Waiving the Privilege (0-503-1204) and Work Product Doctrine: Waiving the Work Product Protection (0-504-4174).

PRESERVING THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK PRODUCT DOCTRINE AFTER A DATA BREACH

Organizations facing a data breach should take steps to shield from disclosure documents and communications protected by the attorney-client privilege and the work product doctrine. Organizations should consider:

- Engaging counsel at the outset to lead the investigation (see Engage Counsel to Lead the Investigation).
- Training company management and employees on how to protect the attorney-client privilege and the work product doctrine (see Train Company Management and Employees).
- Tracking and documenting when the organization reasonably anticipates litigation (see Know When the Organization Reasonably Anticipates Litigation).
- Having counsel retain and supervise third parties performing services relating to the data breach (see Engage Counsel to Retain and Supervise Third Parties).
- Implementing a dual-track investigation (see Consider Dual-Track Investigations).
- Entering into joint defense agreements (see Explore Common Interest and Joint Defense Agreements).
- Identifying non-US legal privileges for global data breaches (see Identify Non-US Legal Privileges).

Organizations should consider including these steps in their data breach response plans. For more information on developing data breach response plans and a template plan, see Developing

a Cyber Incident Response Plan Checklist and Standard Document, Cyber Incident Response Plan (IRP) (w-005-0419).

ENGAGE COUNSEL TO LEAD THE INVESTIGATION

Organizations often cannot reasonably determine the likelihood of litigation or regulatory actions immediately following a data breach. They must first investigate to understand the breach's magnitude and impact. Organizations should involve counsel immediately following a data breach to help shield investigation-related and other protected documents from disclosure in any future litigation.

Counsel should supervise every aspect of the data breach investigation to demonstrate the investigation's legal nature. Organizations typically analyze the scope and impact of a breach by, for example:

- Reviewing system logs for evidence of unauthorized access.
- Limiting access to the affected system.
- Analyzing the types of data affected and disclosed.
- Determining whether other systems are under threat of immediate or future danger.
- Gathering other information about the data breach.
- Collecting details about the compromised data.

Counsel should demonstrate their supervisory role by, for example:

- Instructing individuals on the actions to perform following a data breach, even if some tasks involve technical or operational details.
- Documenting clearly that they need the individuals to perform the requested actions to provide legal advice to the organization.
- Training all employees working on the data breach investigation on how to protect the attorney-client privilege and the work product doctrine (see Train Company Management and Employees).

If counsel ask a non-attorney to interview employees about the data breach, counsel should document each request and make clear that counsel made the request so that they can provide legal advice to the organization (see *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754, 758 (D.C. Cir. 2014) (holding that the attorney-client privilege protects communications made by and to non-attorneys serving as agents of attorneys in internal investigations)).

Benefits of Involving Outside Counsel

Organizations may not want to incur the expense of retaining outside counsel following a data breach until they learn the breach's scope and impact. However, relying solely on in-house counsel to lead a data breach investigation may risk discovery of protected information.

In-house lawyers often function in dual roles by providing clients with both business and legal advice. Organizations therefore may face more difficulty showing that in-house counsel communications deserve privilege protection than showing that communications of outside lawyers who predominantly provide legal advice deserve protection. Involving outside lawyers in corporate investigations can make it easier for organizations to:

- Demonstrate that the company's need for legal advice rather than non-legal business or other advice primarily motivated the communication.
- Support a work product argument, especially if the company only involves outside counsel in matters that might reasonably result in litigation, rather than in ordinary business matters.
- Protect communications and documents in global investigations because non-US privilege law may not protect communications to and from in-house counsel (see Identify Non-US Legal Privileges).

In-house counsel should work with management immediately following a data breach to decide whether the company should retain outside counsel to conduct or assist in the investigation. Organizations may also consider including a protocol on when to obtain outside counsel in their data breach response plan and retaining (or at least identifying) appropriate counsel before a breach occurs.

TRAIN COMPANY MANAGEMENT AND EMPLOYEES

Counsel must explain to employees and management working on any data breach investigation that all of their communications are potentially discoverable. Counsel should train individuals to:

- Include counsel on all communications concerning the data breach (although that does not guarantee that a court will deem the communication privileged).
- Avoid any unnecessary written communications. For necessary written communications, individuals should:
  - be careful what they write; and
  - assume that any of their writings will become public.
- Avoid speculating on reasons for the data breach or making conclusions in writing.
- Document investigation-related business matters separately from legal matters. Separating legal and business matters helps to reduce the likelihood that a court will find that the motivation behind creating the documents was for business reasons, not for legal advice or litigation.
- Date documents to assist in any later claim of privilege or work product protection.
- Mark documents as "Protected by the Attorney-Client Privilege," "Prepared at the Direction of a Lawyer," or "Prepared in Anticipation of Litigation" when appropriate. However, counsel should help employees and management understand that overusing these markings can:
  - dilute a legitimate claim of privilege or work product protection; and
  - increase the cost of a document review.
- Avoid sharing privileged communications with anyone outside the company and even those inside the company beyond those who need to know the information. Companies may consider using security controls to limit access to certain information to authorized individuals.

Counsel should also train employees and management to state in any investigation-related writing the bases for any protections. For example, individuals:

- Seeking legal advice should explain in the body of the document or in the transmittal document that they need legal advice.
- Preparing a list of witnesses for counsel should indicate that they prepared the list in anticipation of litigation.

Stating the bases for protection in the writing itself:

- Supports attorney-client privilege and work product protection claims.
- Reduces the need for affidavits explaining the purpose of the communications or documents.

KNOW WHEN THE ORGANIZATION REASONABLY ANTICIPATES LITIGATION

Organizations learn information about data breaches during their investigations that can help them assess whether they should reasonably anticipate litigation or regulatory actions for work product purposes. Factors that often influence whether an organization should anticipate litigation or a regulatory investigation include:

- The number of records stolen.
- The sensitivity of the compromised data.
- The likely unauthorized use of or access to the compromised data.
- The likelihood of harm to individuals (see Data Breach Notification Laws: State Q&A Tool).
- The novelty of the method used to infiltrate a network.
- Business disruption resulting from the data breach.
- The organization's negligence in not detecting or preventing the data breach, or gaps in its information security practices (see Common Gaps in Information Security Compliance Checklist (3-501-5491)).
- The amount of press or social media attention resulting from the data breach.
- Whether the organization has suffered prior data breaches and, if so, whether the press reported on those breaches.
- Whether the organization issued potentially false or misleading statements:
  - in public filings on its information security and cyber security risks; or
  - to customers regarding its information security and cyber security practices.
- The organization's failure to timely notify affected individuals under relevant federal or state laws.

Once an organization reasonably anticipates litigation, it should instruct all employees to mark documents "Prepared in Anticipation of Litigation" and not share protected documents with third parties. Organizations should also document when they anticipated litigation and the basis for that decision in case their analysis is later challenged.

When an organization reasonably anticipates litigation for work product protection, it should start preserving any potentially relevant documents for the litigation. For more information on preserving data following a data breach, see Practice Note, Preserving Data After a Data Breach (W-005-3417).

ENGAGE COUNSEL TO RETAIN AND SUPERVISE THIRD PARTIES

Investigating the technical aspects of a data breach may require the expertise of computer forensic analysts and other outside experts. The attorney-client privilege and the work product doctrine may protect communications and documents exchanged with third parties if an organization can show that it retained the third party:

- To provide legal advice to the organization.
- In anticipation of litigation.

If a litigant challenges whether communications with third parties deserve attorney-client privilege or work product protection, organizations have the burden of showing that privilege or protection applies. To help show that privilege or work product protection applies, organizations can structure their third-party engagements by:

- Having counsel retain the third parties.
- Documenting in retainer agreements that counsel hired the third parties to help counsel provide legal advice in anticipation of litigation.
- Having counsel direct and supervise the third parties' work.

Genesco, Inc. v. Visa U.S.A., Inc. demonstrates the importance of having in-house counsel hire and work with third-party consultants following a data breach (302 F.R.D. 168 (M.D. Tenn. 2014)). Genesco's general counsel retained a computer security consultant, Stroz Friedberg, to help the company investigate a data breach. In litigation following the breach, Genesco withheld documents and communications about Stroz Friedberg's investigation under the attorney-client privilege and the work product doctrine. Visa asked the court to order production of these documents.

The *Genesco* court found that the attorney-client privilege and the work product doctrine applied to communications between Genesco's general counsel and Stroz Friedberg because:

- Genesco's general counsel showed through an affidavit and other documents that he retained Stroz Friedberg as an agent in anticipation of litigation so that the general counsel could provide legal advice with Stroz Friedberg's help.
- The language in the Stroz Friedberg retainer agreement stated that Genesco's counsel hired the firm in anticipation of litigation.

(See 302 F.R.D. at 193; see also *In re Target Corp. Customer Data Sec. Breach Litig.*, 2015 WL 6777384, at *1-2 (D. Minn. Oct. 23, 2015) (noting that Target submitted declarations and exhibits to substantiate that counsel retained a team from an outside company in anticipation of litigation to help provide legal advice).)

The more details organizations can present to the court demonstrating that the attorney-client privilege or the work product doctrine applies, the more likely it is that a court will uphold the privilege or protection.

CONSIDER DUAL-TRACK INVESTIGATIONS

Litigants often challenge claims of attorney-client privilege or work product protection for withheld data breach-related investigative reports and underlying documents, claiming that:

- The investigative report contains factual findings made to provide business rather than legal recommendations.
- The organization investigated the breach for reasons other than obtaining legal advice or in anticipation of litigation, including:
  - legal or regulatory requirements;
  - contractual obligations;
  - corporate policy requirements; or
  - for ordinary course of business purposes.

(See, for example, *In re Target*, 2015 WL 6777384, at *1 (rejecting the argument that Target would have had to investigate and fix the data breach regardless of any litigation); *Genesco*, 302 F.R.D. at 194 (ordering the production of documents and communications reflecting remedial measures Genesco took in response to an investigative report contractually mandated by Visa); *Kellogg Brown & Root*, 756 F.3d at 760-61 (rejecting the argument that the attorney-client privilege did not protect internal investigation undertaken under regulatory law and corporate policy).)

To shield these documents from disclosure, organizations should consider setting up a dual-track investigation with separate teams to:

- Conduct an ordinary course of business, non-privileged investigation.
- Provide the organization with legal advice and protect the organization's interests in litigation.

Target Investigation

Target's dual-track investigation following its massive data breach demonstrates how counsel can protect from disclosure information created for an investigation under the attorney-client privilege and the work product doctrine (see Legal Update, Target Agrees to Settle Additional Data Breach Claims for Almost $39.4 Million (w-001-0217)).

In *In re Target*, the company's outside counsel engaged Verizon Business Network Services to conduct a technical investigation that it described to the court as "enabl[ing] counsel to provide legal advice to Target, including legal advice in anticipation of litigation and regulatory inquiries" (2015 WL 6777384, at *1). Another team from Verizon conducted a separate non-privileged investigation into the data breach on behalf of several credit card brands as the Payment Card Industry Data Security Standard often requires (see *In re Target*, 2015 WL 6777384, at *2; see also Practice Note, PCI DSS Compliance (8-608-7192)). The two teams did not communicate with one another about the attorney-directed investigation (*In re Target*, 2015 WL 6777384, at *2).

In litigation, Target withheld documents that came from the attorney-directed team as privileged. The plaintiffs asked the court to order production of the documents, arguing that these documents were not privileged because Target would have had to investigate and fix the data breach regardless of any potential litigation. (*In re Target*, 2015 WL 6777384, at *1.)

After *in camera* review, the court found that the attorney-client privilege and the work product doctrine protected communications and documents relating to the attorney-directed investigation because the purpose of that investigation was to advise counsel in anticipation of litigation (*In re Target*, 2015 WL 6777384, at *1).

The court relied heavily on the declarations of Target's in-house counsel and other exhibits to make its ruling (*In re Target*, 2015 WL 6777384, at *1 (citing declarations)).

Decide in Advance How to Structure Investigations

In re Target demonstrates that organizations need to prepare for how they will structure data breach investigations. Target protected from disclosure a significant part of its data breach investigation because it had considered the long-term implications of a data breach investigation at the outset.

A dual-track investigation may not be the appropriate response to every data security breach because it involves a substantial amount of time, planning, and resources. However, organizations should have a plan in place before a data breach regarding whether and under what circumstances they will implement a dual-track investigation.

EXPLORE COMMON INTEREST AND JOINT DEFENSE AGREEMENTS

Multiple parties may play a role in data breach investigations. For example, a third-party vendor that handles data for an organization may suffer a breach of its systems that affects the organization. In cases involving multiple parties, organizations should consider using the common interest doctrine to shield documents from disclosure.

The common interest doctrine, also called the joint defense doctrine, allows separately represented parties with common legal interests to share information with each other and their respective attorneys without destroying the attorney-client privilege or the work product doctrine. Courts generally require parties seeking to rely on the common interest doctrine to:

- Satisfy the requirements of either the attorney-client privilege or the work product doctrine.
- Have interests that are:
  - nearly identical; and
  - legal in nature.
- Have made the communications or have created the documents to further that common interest.

The parties generally do not have to enter into a written agreement for the common interest doctrine to apply. However, organizations that enter into a common interest or joint defense agreement can contractually agree on the scope of their common interest, including, for example:

- The duration of the agreement.
- Remedies for a participant's violation of the agreement.

For more information on drafting a joint defense agreement, see Standard Document, Joint Defense and Confidentiality Agreement (2-501-9461).

IDENTIFY NON-US LEGAL PRIVILEGES

Organizations responding to a global data breach may need to apply different privilege and work product rules, depending on the country involved. For example, in many EU countries, the attorney-client

privilege does not protect communications to and from in-house lawyers (see Article, Akzo Nobel judgment: European Court continues to deny legal privilege to in-house lawyers (0-378-7983)).

Counsel should conduct additional research if a data breach investigation involves any overseas communications or documents to ensure that the organization protects discovery under non-US privilege rules and laws. For more information on the varying privilege rules outside the US, see Practice Note, A world tour of the rules of privilege (9-205-5802).