

The Sedona Conference Draft  
Commentary on Application of  
Attorney-Client Privilege and  
Work-Product Protection to  
Documents and Communications  
Generated in the Cybersecurity  
Context, Second Edition  
(April 2022)

---





**The Sedona Conference  
Draft Commentary on Application of Attorney-Client  
Privilege and Work-Product Protection to  
Documents and Communications Generated in  
the Cybersecurity Context, Second Edition  
(April 2022)**

**Drafting Team Members:**

Kate Baxter-Kauf (Drafting Team Co-Leader)

David Cohen (Drafting Team Co-Leader)

Mathea Bulander

Kelly Iverson

Anderson Lunsford

Douglas McNamara

Kelly Ruane Melchiondo

Daniel Robinson

Sara Romine

Caitlin Saladrigas

Ronni Solomon

Jud Welle

Ruth Promislow (Steering Committee Liaison)

Jonathan Wilan (Steering Committee Liaison)



The Sedona Draft Conference Commentary  
on Application of Attorney-Client Privilege  
and Work-Product Protection  
to Documents and Communications  
Generated in the Cybersecurity Context, Second Edition

April 2022 Version for Review and Comment by Working Group 11

*\*Changes made to first edition are reflected in redline in this version\**

This *Commentary* evaluates the application of the attorney-client privilege and work-product protection to documents and communications that an organization generates in the cybersecurity context. The goal of the *Commentary* is to address the absence of “settled law” on this topic by assessing (1) how the courts have and can be expected to decide, and what organizational practices will be important to a court’s decision regarding, whether the attorney-client privilege or work-product protection applies to documents and communications generated in the cybersecurity context; and (2) how the development of the law in this area should be informed not just by established attorney-client privilege and work-product protection legal principles, but also by the policy rationales underlying the attorney-client privilege and work-product protection generally and those unique to the cybersecurity context.

Part A of the *Commentary* elaborates on the *Commentary*’s purpose (as summarized above) and sets forth its target audience. Part B sets forth the legal principles generally applicable to claims of attorney-client privilege and work-product protection. Part C uses the general principles set forth in Part B and other relevant legal sources to evaluate how the courts have and can be expected to decide, and what organizational practices will be important to a court’s decision regarding, whether the attorney-client privilege or work-product protection applies to various types of documents and communications that an organization generates in the cybersecurity context. Section 1 of Part D examines whether and to what extent the results suggested in Part C are consistent with the policy rationales underlying the attorney-client privilege and work-product protection generally and those unique to the cybersecurity context. Section 2 of Part D considers various proposals for adapting existing attorney-client privilege and work-product protection law, or developing entirely new protections, for documents and communications that an organization generates in the cybersecurity context, and the tradeoffs those proposals present.

Style Definition	... [60]
Style Definition	... [59]
Style Definition	... [58]
Style Definition	... [57]
Style Definition	... [56]
Style Definition	... [55]
Style Definition	... [54]
Style Definition	... [53]
Style Definition	... [52]
Style Definition	... [51]
Style Definition	... [50]
Style Definition	... [49]
Style Definition	... [48]
Style Definition	... [47]
Style Definition	... [46]
Style Definition	... [45]
Style Definition	... [44]
Style Definition	... [43]
Style Definition	... [42]
Style Definition	... [41]
Style Definition	... [40]
Style Definition	... [39]
Style Definition	... [38]
Style Definition	... [37]
Style Definition	... [36]
Style Definition	... [35]
Style Definition	... [34]
Style Definition	... [33]
Style Definition	... [32]
Style Definition	... [31]
Style Definition	... [30]
Style Definition	... [29]
Style Definition	... [28]
Style Definition	... [27]
Style Definition	... [26]
Style Definition	... [25]
Style Definition	... [24]
Style Definition	... [23]
Style Definition	... [22]
Style Definition	... [21]
Style Definition	... [20]
Style Definition	... [19]
Style Definition	... [18]
Style Definition	... [17]
Style Definition	... [16]
Style Definition	... [15]
Style Definition	... [14]
Style Definition	... [13]
Style Definition	... [12]
Style Definition	... [11]
Style Definition	... [10]
Style Definition	... [9]
Style Definition	... [8]



## A. PURPOSE AND TARGET AUDIENCE

With cybercrime on the rise, cybersecurity breaches have become more frequent, and organizations have increasingly found themselves subject to litigation and/or regulatory investigations by reason of having experienced such breaches. In such litigation and/or regulatory investigations, it is often (if not always) the case that the organization has created documents and/or engaged in communications that contain information about the organization's cybersecurity practices that are therefore relevant to the litigation or investigation. Examples include pre-breach documents and communications such as assessments of the organization's information security posture (e.g., technical and gap assessments), table-top exercise results, internal audit reports, reports to third parties (e.g., clients or insurers), or post-hoc analyses of prior incidents. Relevant cybersecurity-related documents and communications also are regularly generated by an organization after it suffers a cybersecurity breach, as it conducts a forensic investigation of the breach, assesses its information security posture, remediates the circumstances that may have enabled the breach to occur, and/or communicates with third parties (e.g., law enforcement, insurers, vendors, clients, or public relations firms) regarding the breach.

Such documents and communications are often highly relevant to litigation or regulatory investigations over a breach because they pertain to issues such as (1) whether the organization's cybersecurity practices, or its oversight of third parties' (e.g., vendors') cybersecurity practices, complied with any applicable legal requirements; (2) whether the organization made deceptive statements regarding its cybersecurity practices that might provide a basis for misrepresentation-based claims; and/or (3) whether the organization provided legally sufficient notice to external parties regarding the breach. Accordingly, such documents and communications are likely to be helpful to plaintiffs and regulators in trying to prove their claims in any breach-related litigation or regulatory investigations, and potentially damaging to the breached organization's legal defenses to such claims. As a result, the breached organization may desire to shield such documents and communications from discovery under the attorney-client privilege or as protected trial preparation "work product" (such protection being referred to both colloquially and in this *Commentary* as "work-product protection"), whereas plaintiffs and regulators may desire to overcome any such assertion of attorney-client privilege or work-product protection.

Because cybersecurity law is remains in its infancy, there are only a few limited judicial decisions in the cybersecurity area that even address, and certainly there is no "settled law" in the cybersecurity area that establishes, when, if ever, a breached organization's pre- and post-breach cybersecurity-related documents and communications (collectively, CI) can be protected from discovery under the attorney-client privilege or the work-product protection. Moreover, because CI tends to be unique to the cybersecurity context, or at least not regularly encountered in litigation generally, the applicability of the

Formatted: English (United States)

Formatted: Outline numbered + Level: 1 + Numbering Style: A, B, C, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5", No page break before, Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Normal



attorney-client privilege and the work-product protection to CI has received little if any judicial attention *outside* the cybersecurity area.<sup>1</sup> Cybersecurity lawyers and judges handling cybersecurity cases are therefore currently operating with only minimal guidance in considering whether and to what extent CI qualifies for the attorney-client privilege or the work-product protection.

The *Commentary* seeks to address the absence of settled law in this area by providing cybersecurity lawyers (whether they are private practitioners, in-house organizational attorneys, or government regulators) and judges with: (i) an evaluation of how the courts have extrapolated and can be expected to extrapolate general principles of attorney-client privilege and work-product protection law into the context of CI; and (ii) guidelines as to what practices by the organization in question the courts can be expected to consider as important in deciding whether an organization's CI<sup>2</sup> can be protected from discovery under the attorney-client privilege or the work-product protection.<sup>3</sup> The *Commentary* also seeks to help move the law forward by providing practitioners (faced with advocating for and against the discoverability of CI), judges (faced with rendering decisions on its discoverability), and legislators (seeking to create law on its discoverability) with an

<sup>1</sup> For instance, while there is substantial case law on the applicability of the attorney-client privilege and work-product protection to documents like financial reports and product safety investigations, courts have had little occasion to rule on whether CI such as penetration test reports or data-breach forensic investigations qualifies for either protection.

<sup>2</sup> The *Commentary* focuses on attorney-client privilege and work-product protection claims that an organization might assert as to *its own* CI, rather than attorney-client privilege and work-product protection claims that such an organization's adversaries might assert as to *their* documents and communications.

<sup>3</sup> The *Commentary* focuses on attorney-client privilege and work-product protection law, as opposed to other privileges and protections that might potentially apply to CI, but recognizes that other privileges and protections may potentially be applicable to CI and/or may have underlying policy rationales that bear upon the propriety of according attorney-client privilege and/or work-product protection to CI. In addition, while private lawsuits and regulatory investigations regarding cybersecurity breaches occur inside and outside of the United States, and accordingly, data security lawyers have an interest in both the U.S. and the non-U.S. legal standards governing attorney-client privilege and work-product protection claims that might be made as to CI, the *Commentary* focuses solely on the U.S. legal standards. In this regard, it bears noting that many of the cybersecurity decisions discussed in Part C below, while brought in federal court, were decided under state attorney-client privilege law pursuant to Federal Rule of Evidence 501, because the court's jurisdiction rested on diversity of citizenship. However, none of those decisions are at odds with any of the general governing principles of attorney-client privilege law discussed in Part B.1 below or turned on the attorney-client privilege law of the state in question being at odds with one or more of those general governing principles. Accordingly, while differences do exist in various states' attorney-client privilege laws, none of those differences are relevant to the discussion in Parts C and D below regarding the application of attorney-client privilege law to CI. Similarly, while differences also exist in various states' laws regarding work-product protection and waiver of privilege, none of those differences are relevant to the discussion in Parts C and D below regarding the application of those laws to CI.

Formatted: Font: 10 pt, Font color: Black

Formatted: Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



assessment of the arguments for and against having the discoverability of CI be determined under general principles of attorney-client privilege and work-product protection law, as opposed to modifying those principles in the context of CI to create more or less protection of CI from discovery than otherwise would be provided under the attorney-client privilege and the work-product protection. Finally, the *Commentary* considers various proposals for adapting existing attorney-client privilege and work-product protection law, or developing entirely new protections, in the CI context. To this end, the *Commentary* calls for enacting a qualified—but not an absolute—stand-alone cybersecurity privilege under which CI would enjoy some measure of protection against discoverability, whether or not lawyers were sufficiently involved in its creation to qualify the CI in question for the attorney-client privilege and/or the work-product protection. The *Commentary* also calls for all U.S. jurisdictions to recognize a “no waiver” doctrine that provides a data holder’s disclosure of CI to law enforcement would not waive any privilege or protection that might otherwise be claimed in future civil litigation.

Formatted: Highlight

## B. GENERAL GOVERNING PRINCIPLES

This Part of the *Commentary* summarizes the general principles of attorney-client privilege and work-product protection law most relevant to the application of the attorney-client privilege and the work-product protection to CI. This Part is therefore not intended as a generalized primer on attorney-client privilege and work-product protection law. Part B.1 sets forth the relevant general principles of attorney-client privilege law; Part B.2 sets forth the relevant general principles of work-product protection law; and Part B.3 sets forth the relevant general principles regarding waiver of attorney-client privilege and work-product protection.

Formatted: English (United States)

Formatted: Outline numbered + Level: 1 + Numbering Style: A, B, C, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5", No page break before, Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

### 1. The Attorney-Client Privilege

The attorney-client privilege generally protects a communication made in confidence for the “predominant purpose” of obtaining legal advice from a lawyer.<sup>4</sup> The privilege protects communications, including observations of the client’s communicative acts (such as the client revealing a hidden scar or submitting to a medical examination by a doctor enlisted by the attorney), but does not permit a party to resist disclosure of the facts underlying the communications to the extent they are discoverable separate from

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5", Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

<sup>4</sup> *In re County of Erie*, 473 F.3d 413, 419–20 (2d Cir. 2007); *United States v. Kovel*, 296 F.2d 918, 922 (2d Cir. 1961). Courts sometimes alternatively use the phrase “primary purpose” or “dominant purpose” in this context, acknowledging that it has the same meaning as “predominant purpose.” See, e.g., *In re County of Erie*, 473 F.3d at 420 (citing *In re Buspirone Antitrust Litig.*, 211 F.R.D. 249, 252–53 (S.D.N.Y. 2002); *U.S. Postal Serv. v. Phelps Dodge Refining Corp.*, 852 F. Supp. 156, 163 (E.D.N.Y. 1994).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



the communications.<sup>5</sup> The privilege’s “purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice.”<sup>6</sup> “[L]ike any other testimonial privilege,” however, “this rule contravenes the fundamental principle that the public has a right to every man’s evidence,” and therefore courts “construe it narrowly to serve its purposes.”<sup>7</sup>

In the corporate context, confidential communications between corporate employees and counsel for the predominant purpose of assisting counsel in rendering legal advice to the company are protected by the attorney-client privilege.<sup>8</sup> The majority of courts today employ a “functionality” or “subject-matter” test that extends the attorney-client privilege to include a company lawyer’s communications with any corporate employee as long as the communication relates to the subject matter for which the company is seeking legal representation.<sup>9</sup> Courts generally have held under both federal common law and state law<sup>10</sup> that this includes not just communications with actual employees, but also with independent contractors who are the “functional equivalent” of an employee.<sup>11</sup> Because in-house counsel may play multiple roles in a corporation, *some* courts applying either federal common law or state law have applied additional scrutiny to assertions of privilege involving communications with in-house counsel, requiring organizations to

<sup>5-5</sup> 1 KENNETH S. BROWN & ROBERT P. MOSTELLER, MCCORMICK ON EVIDENCE § 89 (7th ed. 2016).

<sup>6-6</sup> *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).

<sup>7-7</sup> *In re Pac. Pictures Corp.*, 679 F.3d 1121, 1126 (9th Cir. 2012) (internal citation and quotation marks omitted).

<sup>8-8</sup> *Id.* at 396.

<sup>9-9</sup> 1 THE AMERICAN LAW INSTITUTE, RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 73 (2000). Note: Some states continue to employ the more restrictive “control group” test, which designates only upper-level management as clients of the corporate counsel. *See, e.g.*, *Alaska (see Manumitted Cos. v. Tesoro Alaska Co.*, 2006 WL 8431821, at \*2 (D. Alaska Aug. 16, 2006)); *Illinois (see Consolidation Coal Co. v. Bucyrus-Erie Co.*, 432 N.E.2d 250 (Ill. 1982); *Sterling Fin. Mgmt., L.P. v. UBS PaineWebber, Inc.*, 782 N.E.2d 895, 900 (Ill. 2002)); *Hawaii (HAW. REV. STAT. § 626-503); Maine (ME. R. EVID. 502(a)(2))*. Many other states have yet to specifically decide which test to apply. *See* Brian E. Hamilton, *Conflict, Disparity, and Indecision: The Unsettled Corporate Attorney-Client Privilege*, 1997 ANN. SURV. AM. L. 629, 630 (1997). The control group test has been explicitly rejected for use by federal courts. *See Upjohn Co.*, 449 U.S. at 390–92.

<sup>10-10</sup> In U.S. federal courts, privilege law is governed by FED. R. EVID. 501. If jurisdiction is based on a federal question, FED. R. EVID. 501 provides for the application of the federal common law of privilege. State privilege law applies in most cases brought under the federal court’s diversity jurisdiction, and in other federal proceedings “with respect to an element of a claim or defense as to which state law supplies the rule of decision.” FED. R. EVID. 501. State law regarding privilege issues applies in state court proceedings. Each state has its own articulation of the privilege, and there are considerable differences among jurisdictions regarding its scope and application.

<sup>11-11</sup> *See, e.g., In re Bieter Co.*, 16 F.3d 929 (8th Cir. 1994).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



make a “clear showing” that such communications were made for a legal, rather than a business, purpose.<sup>12</sup>

Communications between “privileged persons” *may* include those between employees, in-house counsel or outside counsel, and any of the company’s subsidiaries or affiliates and any combination of them. These could be communications: (1) from employees to counsel; (2) from counsel to employees; (3) between counsel; (4) between employees or their functional equivalents;<sup>13</sup> or (5) with qualified agents of counsel or the client (e.g., employees or counsel of an agent, confidential litigation consultants, or informal consulting experts).<sup>14</sup> The nature and scope of the privilege varies state-by-state and is not uniform as a matter of federal common law, with certain states and federal courts limiting the extent and/or existence of any claim of privilege, for example, between nonlawyer employees, or with functional equivalents and/or affiliated entities.

Courts have generally held under both federal common law and state law that, for the attorney-client privilege to apply, the dominant or predominant purpose of the communication itself must have been to solicit or render legal advice.<sup>15</sup> At least one state (California) is more protective, providing that communications will be deemed to present a *prima facie* claim of attorney-client privilege so long as obtaining advice was the predominant purpose of the *relationship* between the client and counsel.<sup>16</sup>

<sup>12-12</sup> See, e.g., *In re Vioxx Prod. Liab. Litig.*, 501 F. Supp.2d 789, 799 (E.D. La. 2007) (“While this expanded role of legal counsel within corporations has increased the difficulty for judges in ruling on privilege claims, it has concurrently increased the burden that must be borne by the proponent of corporate privilege claims relative to in-house counsel.”).

<sup>13-13</sup> 2 DAVID M. GREENWALD, ROBERT R. STAUFFER & ERIN R. SCHRANTZ, *TESTIMONIAL PRIVILEGES* § 1:31 (2012).

<sup>14-14</sup> *Id.* at §§ 1:28–1:32 (agents of counsel), and at § 1:36 (representatives and agents of the client).

<sup>15-15</sup> See *In re County of Erie*, 473 F.3d 413, at 420 (2d Cir. 2007) (“We consider whether the predominant purpose of the communication is to render or solicit legal advice.”) (applying federal law); THE AMERICAN LAW INSTITUTE, *supra* note 7, at § 72 cmt. c (2000) (“A client must consult the lawyer for the purpose of obtaining legal assistance and not predominantly for another purpose.”).

<sup>16-16</sup> See, e.g., *Costco Wholesale Corp. v. Super. Ct.*, 219 P.3d 736, 746 (Cal. 2009) (a court must first determine “the dominant purpose of the relationship between the [client] and its in-house attorneys,” and if the dominant purpose is the provision of legal advice, those communications would be subject to the privilege) (emphasis in original); see also *Cason v. Fed. Life Ins. Co.*, No. C-10-0792, 2011 WL 1807427, at \*2 (N.D. Cal. May 11, 2011) (“It is not the dominant purpose of a communication that dictates whether the attorney-client privilege is applicable; rather, the issue is what was the dominant purpose of the relationship.”

(emphasis in original)); *In re Marriott International, Inc. Consumer Data Security Breach Litigation*, 2021 WL 2660180 (D. Md. June 29, 2021) (“[Attorney] had a precise, limited problem and had his client retain IBM experts to solve it. He did this to assist his client in its response to regulatory authorities and in the litigation (such as this case) that was anticipated. [Attorney] also wanted

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font: 10 pt, Italic, Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Normal



~~2. Courts have generally held under both federal common law and state law that the attorney-client privilege can extend to communications involving counsel-retained experts where the expert is necessarily included for the purpose of assisting the attorney in providing legal advice. Specifically, under what is often referred to as the *Kovel* doctrine, the attorney-client privilege will extend to the work and communications of third party experts if the expert was hired “for the purpose of obtaining [confidential] legal advice from the lawyer.”<sup>17</sup> In *Kovel*, the attorney hired an accountant to assist him in understanding his client’s tax position, and the communications at issue were between the client and the accountant. The court analogized the accountant to a translator, whose assistance in overcoming a language barrier would not destroy the privilege. Where the requirements for this exception are met, i.e., where the expert’s presence in the communication is necessary for counsel’s provision of legal advice, courts have held that the privilege may extend not only to communications between counsel and the expert, but also to communications between the expert and the client directly.<sup>18</sup>~~

**Formatted:** Indent: First line: 0", Don't suppress line numbers

~~For communications among company employees (or the functional equivalents of employees) that do not include counsel or counsel-retained experts, the inquiry is highly fact dependent, and generally turns on the intent of the creator of the communications.<sup>19</sup>~~

**Formatted:** Don't suppress line numbers

~~In order to be privileged, a communication must be made in confidence. Communications contained in public documents, such as final press releases and corporate annual reports, are not privileged. The party asserting a privilege or protection has the burden of establishing that withheld information qualifies for protection.~~

the X-Force Red analysis of the post-breach environment of Marriott’s devices because, in his experience, that information might be important to present to regulatory authorities”).

**Formatted:** Font color: Black

~~17.<sup>17</sup> . United States v. Kovel, 296 F.2d 918, 922–23 (2d Cir. 1961); see also CAL. EVID. CODE § 952 (privilege extends to “those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted”); Rodriguez v. Super. Ct., 18 Cal. Rptr. 2d 120, 123–24 (Cal. Ct. App. 1993) (communications between client and a doctor hired by counsel to evaluate client for defense of criminal proceedings were privileged); Nat’l Steel Prods. Co. v. Super. Ct., 210 Cal. Rptr. 535, 538 (Cal. Ct. App. 1985) (privilege could extend to communications involving engineering expert retained by counsel to perform technical analysis of building structure to assist counsel in providing legal advice).~~

~~18.<sup>18</sup> . See Umpqua Bank v. First Am. Title Ins. Co., 2011 WL 997212, at \*7 (E.D. Cal. Mar. 17, 2011) (communications between client and counsel-retained expert protected where for the purpose of furthering legal advice); see also *In re OM Group Sec. Litig.*, 226 F.R.D. 579, 588–89 (N.D. Ohio 2005) (same); *In re Grand Jury Subpoenas Dated March 24, 2003*, 265 F. Supp. 2d 321, 331–32 (S.D.N.Y. 2003) (same).~~

~~19.<sup>19</sup> . E.g., Williams v. Sprint/United Mgmt. Co., 238 F.R.D. 633, 639–40 (D. Kan. 2006) (sustaining privilege as to drafts that ultimately were not shared with counsel, because they nonetheless “constituted communications made for the purpose of obtaining legal advice”); *In re Bieter Co.*, 16 F.3d 929, 938 (8th Cir. 1994) (applying a fact intensive privilege analysis to the functional equivalent of an employee).~~

**Formatted:** Normal



### Work-Product Protection Law

In U.S. federal court, the work-product doctrine is governed by Fed. R. Civ. P. 26(b)(3)(A), which provides that “a party may not discover documents and tangible things that are prepared *in anticipation of litigation* or for trial by or for another party or its representative (including the other party’s attorney, consultant, surety, indemnitor, insurer, or agent).”<sup>20</sup> To satisfy the “anticipation of litigation” test, a document must be prepared after a point at which the company “anticipated” that litigation would be filed against it. Courts applying the rule have differed somewhat in their formulation of the test for determining when an as-yet-uncommenced litigation is sufficiently “anticipated” to make work-product protection potentially applicable. They agree, however, that the prospect of that future litigation must be more than speculative.<sup>21</sup>

Evidence that courts have looked to in determining whether litigation was “anticipated” includes evidence that a prospective plaintiff intended to make a claim;<sup>22</sup> hiring of outside counsel;<sup>23</sup> dissemination of a “litigation hold” or preservation notice;<sup>24</sup> and putting a potential adversary on notice, either directly or through public disclosure, of facts that reasonably could be expected to result in the adversary initiating litigation.<sup>25</sup>

<sup>20-20</sup> FED R. CIV. P. 26(b)(3)(A).

<sup>21-21</sup> See, e.g., *Willis v. Westin Hotel Co.*, No. 85 Civ. 2056 (CBM), 1987 WL 6155, at \*1 (S.D.N.Y. Jan. 30, 1987) (“The mere contingency that litigation may result does not give rise to the privilege.”); *Hertzberg v. Veneman*, 273 F. Supp.2d 67, 75 (D.D.C. 2003) (“While litigation need not be imminent or certain in order to satisfy the anticipation-of-litigation prong of the test, this circuit has held that at the very least some articulable claim, likely to lead to litigation, must have arisen, such that litigation was fairly foreseeable at the time the materials were prepared.”) (quotations and citation omitted); *In re Grand Jury Investigation*, 412 F. Supp. 943, 948 (E.D. Pa. 1976) (“Advising a client about matters which may or even likely will ultimately come to litigation does not satisfy the ‘in anticipation of’ standard. The threat of litigation must be more real and imminent than that.”); *Helt v. Metro. Dist. Comm’n*, 113 F.R.D. 7, 12 (D. Conn. 1986) (“To qualify, the documents must have been prepared any time after initiation of the proceeding or such earlier time as the party who normally would initiate the proceeding had tentatively formulated a claim, demand or charge.”) (internal quotation omitted).

<sup>22-22</sup> See, e.g., *Resolution Trust Corp. v. Mass. Mut. Life Ins. Co.*, 200 F.R.D. 183, 189–90 (W.D.N.Y. 2001); *McNulty v. Bally’s Park Place, Inc.*, 120 F.R.D. 27, 29 (E.D. Pa. 1988).

<sup>23-23</sup> See *Maartin v. Armstrong World Indus., Inc.*, 172 F.R.D. 143 (D.N.J. 1997); but see *Lindley v. Life Investors Inc. Co.*, Nos. 08-CV-0379-CVE-PJC, 09-CV-0429-CVE-PJC, 2010 WL 1741407, at \*4 (N.D. Okla. Apr. 28, 2010) (“[T]he mere fact that the Taskforce consulted in-house or outside counsel about potential litigation scenarios does not mean that defendant was acting in anticipation of litigation.”).

<sup>24-24</sup> See *Major Tours, Inc. v. Colorel*, Civil No. 05-3091 (JBS/JS), 2009 WL 2413631, at \*2 (D.N.J. Aug. 4, 2009) (collecting authorities that deem litigation hold notices subject to work-product protection).

<sup>25-25</sup> See, e.g., *Schwarz & Schwarz of Virginia L.L.C. v. Certain Underwriters at Lloyd’s London*, No. 6:07cv00042, 2009 WL 1043929, at \*3–4 (W.D. Va. Apr. 17, 2009) (finding that the date on which insurer

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Normal



In addition to showing that litigation was anticipated, the proponent of the work-product protection must also show that the document was prepared “in anticipation of” the anticipated litigation, and not for some other purpose. Most circuits decide this aspect of work-product protection by applying the “because of” test, asking if the document was prepared “because of” the prospect of the litigation in question.<sup>26</sup> In regard to “dual purpose” documents that serve both business and litigation purposes, the “because of” test is often characterized as a “but for” test: “[w]here a document was created because of anticipated litigation, and would not have been prepared in substantially similar form *but for* the prospect of that litigation, it falls within Rule 26(b)(3).”<sup>27</sup> The Fifth Circuit applies the more restrictive “primary purpose” test, requiring that “the primary motivating purpose . . . was to aid in possible future litigation.”<sup>28</sup>

Materials otherwise qualifying for work-product protection may be discovered under certain circumstances where a party “shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means.”<sup>29</sup> But, “[i]f the court orders discovery of those materials, it must protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of a party’s attorney or other representative concerning the litigation.”<sup>30</sup>

### 3. Waiver

The attorney-client privilege or the work-product protection may in certain circumstances be waived as to a document or communication that would otherwise be protected from discovery under one or both doctrines. The attorney-client privilege is more easily waived than the work-product protection. For instance, disclosure of an otherwise attorney-client privileged document or communication to any third party generally results in waiver of the privilege (subject to limited exceptions, such as for disclosures to a third-party having a common interest or who is the functional equivalent of an employee), whereas disclosure of a work-product protected document to a third

began to anticipate litigation was the date it denied coverage, and noting the other cases with same holding); *Country Life Ins. Co., v. St. Paul Surplus Lines Ins. Co.*, No. 03-1224, 2005 WL 3690565, at \*7 (C.D. Ill. Jan. 31, 2005) (same); *see also* *United States v. Roxworthy*, 457 F.3d 590, 597 (6th Cir. 2006) (finding that a potential defendant anticipated litigation against the I.R.S. based on the fact that the I.R.S. frequently litigated tax losses of the sort the potential defendant had decided to claim, even though the IRS was not, at the time, aware that the defendant was going to claim such a tax loss).

<sup>26-26</sup> *E.g., In re Grand Jury Proceedings*, 604 F.2d 798, 803 (3d Cir. 1979).

<sup>27-27</sup> *United States v. Adlman*, 134 F.3d 1194, 1195 (2nd Cir. 1998).

<sup>28-28</sup> *In re Kaiser Aluminum & Chem. Co.*, 214 F.3d 586, 593 (5th Cir. 2000).

<sup>29-29</sup> FED. R. CIV. P. 26(b)(3)(A)(ii).

<sup>30-30</sup> FED. R. CIV. P. 26(b)(3)(B).

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



party generally does not waive the protection unless the disclosure is to an adversary or a conduit to an adversary.<sup>31</sup> Courts have also indicated that disclosure of an attorney-client privileged communication within a company may waive that privilege if the disclosure is made to an employee who did not “need to know” of the document or communication.<sup>32</sup> Moreover, language in some decisions could be read to suggest that in jurisdictions that employ a “control group” test for attorney-client privilege, disclosures of attorney-client privileged communications to internal employees outside the “control group” may waive the privilege as well.<sup>33</sup>

Disclosure of attorney-client privileged or work-product protected documents or communications to a third party may result in waiver of the privilege or protection for the documents or communications not only as against that third party, but also as against other third parties. While at least one court has held that a “selective waiver” theory may protect a party who discloses information to a governmental entity from losing either the attorney-client privilege or the work-product protection as to that information as against other entities,<sup>34</sup> many courts have rejected this theory.<sup>35</sup> Some courts have allowed disclosure to law enforcement or regulators under some circumstances without waiving the attorney-client and work-product protections as against other parties, provided that

<sup>31-31</sup> See, e.g., *United States v. Deloitte LLP*, 610 F.3d 129, 140 (D.C. Cir. 2010); *United States v. Graf*, 610 F.3d 1148, 1158 (9th Cir. 2010); *In re Bieter Co.*, 16 F.3d 929 (8th Cir. 1994); *La. Mun. Police Employees Ret. Sys. v. Sealed Air Corp.*, 253 F.R.D. 300, 309 (D.N.J. 2008).

<sup>32-32</sup> See, e.g., *Verschoth v. Time Warner, Inc.*, No. 00CIV1339AGSJCF, 2001 WL 286763 at \*3 (S.D.N.Y. Mar. 22, 2001) (company “lost any privilege with respect to” legal advice when that advice was conveyed to worker who did not need to know that advice).

<sup>33-33</sup> See, e.g., *Barr Marine Prods., Co., Inc. v. Borg-Warner Corp.*, 84 F.R.D. 631, 634 (E.D. Pa. 1979) (“if one member of the control group relays legal advice to another member the privilege is not lost”) (emphasis added).

<sup>34-34</sup> See, e.g., *Diversified Indus., Inc. v. Meredith*, 572 F.2d 596, 611 (8th Cir. 1977) (referring to a selective waiver as a “limited waiver”); *In re McKesson HBOC, Inc. Secs. Litig.*, No. C-99-20743 RMW, No. C-00-20030 RMW, 2005 U.S. Dist. LEXIS 7098, at \*47 (N.D. Cal. Mar. 31, 2005).

<sup>35-35</sup> *In re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289, 306 (6th Cir. 2002) (finding that a party’s voluntary disclosure of protected documents to the SEC, even under a confidentiality agreement, constituted a complete waiver of attorney-client and work-product privilege); see also *Westinghouse Elec. Corp. v. Republic of Phil.*, 951 F.2d 1414, 1429 (3d Cir. 1991) (determining party’s “disclosure of work product to the SEC and to the DOJ waived the work-product doctrine as against all other adversaries,” notwithstanding if there was or was not a finding that there was a confidentiality agreement entered into with government agencies).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



the company entered into a confidentiality or protective order containing appropriate non-waiver and other provisions.<sup>36</sup>

In addition, disclosure of attorney-client privileged and/or work-product protected information may operate not only as a waiver of the disclosed information as to others, but also as a waiver of attorney-client privilege and/or work-product protection as to any related *undisclosed* information, both as to the recipient of the disclosed information and as to others. Such subject-matter waivers historically were not recognized in the work-product protection context (with some exceptions),<sup>37</sup> but were typically recognized in the attorney-client privilege context.<sup>38</sup> Today, Federal Rule of Evidence 502, which became effective in 2008, consolidates treatment of the scope of waiver of the attorney-client privilege and work-product protection into a single regime when the disclosure is made in a federal proceeding or to a federal office or agency.<sup>39</sup> Under Rule 502, when such a disclosure waives the attorney-client privilege or work-product protection, the waiver extends to undisclosed information only if “the waiver is intentional, the disclosed and undisclosed communications or information concern the same subject matter, and they ought in fairness to be considered together.”<sup>40</sup>

#### 4. Privileges for Experts

Courts have generally held under both federal common law and state law that the attorney-client privilege can extend to communications involving counsel-retained experts where the expert is necessarily included for the purpose of assisting the attorney

<sup>36-36</sup> Compare *In re Columbia/HCA*, 293 F.3d at 303 (declining to apply selective waiver even in instances where the parties enter into confidentiality orders), with *In re Steinhardt Partners, L.P.*, 9 F.3d 230, 236 (2d Cir. 1993) (indicating that selective waiver would apply in disclosure to the government as long as a confidentiality agreement existed). See also, e.g., *In re Qwest Commc’ns Int’l Inc.*, 450 F.3d 1179, 1195-99 (10th Cir. 2006). A footnote accompanying documents voluntarily disclosed to a government entity concerning the exemption of such documents from production under the Freedom of Information Act (FOIA) is not a sufficient confidentiality agreement to attain selective waiver. See, e.g., *In re Aqua Dots Prod. Liab. Litig.*, 270 F.R.D. 322, 330 (N.D. Ill. 2010), *aff’d*, 654 F.3d 748 (7th Cir. 2011).

<sup>37-37</sup> See, e.g., *Pittman v. Frazer*, 129 F.3d 983, 988 (8th Cir. 1997); 2 DAVID M. GREENWALD ET AL., *supra* note 13 § 2:32 (3d ed. 2015).

<sup>38-38</sup> See, e.g., *In re Sealed Case*, 676 F.2d 793, 809 (D.C. Cir. 1982); 2 CHRISTOPHER B. MUELLER ET AL., *FEDERAL EVIDENCE* § 5:33 (4th ed. 2017).

<sup>39-39</sup> *Chick-fil-A v. ExxonMobil Corp.*, No. 08-61422-CIV, 2009 WL 3763032 (S.D. Fla. Nov. 10, 2009).

<sup>40-40</sup> FED. R. EVID. 502(a). Even as to disclosures covered by Rule 502(a), however, some courts have been more reluctant to find a subject-matter waiver as to work-product protection than as to attorney-client privilege. See, e.g., *Chick-fil-A*, (subject matter waiver under Rule 502(a) extended only to fact work product, not opinion work product, given the special protection afforded to opinion work product).

Formatted: Superscript

Formatted: Indent: First line: 0", Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



in providing legal advice. Specifically, under what is often referred to as the *Kovel* doctrine, the attorney-client privilege will extend to the work and communications of third-party experts if the expert was hired “for the purpose of obtaining [confidential] legal advice from the lawyer.”<sup>41</sup> In *Kovel*, the attorney hired an accountant to assist him in understanding his client’s tax position, and the communications at issue were between the client and the accountant. The court analogized the accountant to a translator, whose assistance in overcoming a language barrier would not destroy the privilege. Where the requirements for this exception are met, i.e., where the expert’s presence in the communication is necessary for counsel’s provision of legal advice, courts have held that the privilege may extend not only to communications between counsel and the expert, but also to communications between the expert and the client directly.<sup>42</sup>

For communications among company employees (or the functional equivalents of employees) that do not include counsel or counsel-retained experts, the inquiry is highly fact-dependent, and generally turns on the intent of the creator of the communications.<sup>43</sup>

In order to be privileged, a communication must be made in confidence. Communications contained in public documents, such as final press releases and corporate annual reports, are not privileged. One court also refused to expand the attorney-client privilege for communications from one employee of a client to another in the absence of an attorney, even when performing tasks that an attorney directed.<sup>44</sup> The

<sup>41,41</sup> *United States v. Kovel*, 296 F.2d 918, 922–23 (2d Cir. 1961); see also CAL. EVID. CODE § 952 (privilege extends to “those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted”); *Rodriguez v. Super. Ct.*, 18 Cal. Rptr. 2d 120, 123–24 (Cal. Ct. App. 1993) (communications between client and a doctor hired by counsel to evaluate client for defense of criminal proceedings were privileged); *Nat’l Steel Prods. Co. v. Super. Ct.*, 210 Cal. Rptr. 535, 538 (Cal. Ct. App. 1985) (privilege could extend to communications involving engineering expert retained by counsel to perform technical analysis of building structure to assist counsel in providing legal advice).

<sup>42,42</sup> *See Umpqua Bank v. First Am. Title Ins. Co.*, 2011 WL 997212, at \*7 (E.D. Cal. Mar. 17, 2011) (communications between client and counsel-retained expert protected where for the purpose of furthering legal advice); see also *In re OM Group Sec. Litig.*, 226 F.R.D. 579, 588–89 (N.D. Ohio 2005) (same); *In re Grand Jury Subpoenas Dated March 24, 2003*, 265 F. Supp. 2d 321, 331–32 (S.D.N.Y. 2003) (same).

<sup>43,43</sup> *E.g., Williams v. Sprint/United Mgmt. Co.*, 238 F.R.D. 633, 639–40 (D. Kan. 2006) (sustaining privilege as to drafts that ultimately were not shared with counsel, because they nonetheless “constituted communications made for the purpose of obtaining legal advice”); *In re Bieter Co.*, 16 F.3d 929, 938 (8th Cir. 1994) (applying a fact-intensive privilege analysis to the functional equivalent of an employee).

<sup>44</sup> *See In Re Marriott International Inc. Consumer Security Breach Litigation*, Case No. 8:19-md-02879-PWG (D. Md. June 2, 2021) (citing *Upjohn v. United States*, 449 U.S. 383, 390 (1981)) (“Such an experiential expansion of the attorney client privilege has nothing to do with its purpose to encourage clients to speak candidly to their attorneys).

Formatted: Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



party asserting a privilege or protection has the burden of establishing that withheld information qualifies for protection.

Non-testifying experts, or “consulting experts,” may serve as valuable resources for parties engaged in litigation. Non-testifying experts are typically authorities in their field and well-versed on the particular subject matter of their expertise, but who, for whatever reason, do not want to, or lack the ability to, testify at depositions or in court. Under the Federal Rules of Civil Procedure, the work product of, and communications with, non-testifying experts are shielded by the attorney-client privilege and the work-product. Certain courts have recognized that even the identity of the non-testifying expert may be privileged.<sup>45</sup>

Because non-testifying experts are typically consultants of counsel, they are typically included within the broad definition of the attorney’s “agent” for which the attorney-client privilege extends to communications.<sup>46</sup>

Federal Rule of Civil Procedure 26 requires parties to disclose the experts that they intend to call at trial to present evidence. Rule 26(b)(4)(C) permits parties to depose experts so identified. Consistent with *Kovel* and general notions of work product protection, Rule 26 shields from disclosure certain expert materials, such as drafts of any reports.<sup>47</sup> Rule 26(b)(4)(B) provides that “communications between the party’s attorney and any witness required to provide a report” may be protected work product, but exempts from that protection all communications that “(i) relate to compensation for the expert’s study or testimony; (ii) identify facts or data that the party’s attorney provided and that the expert considered in forming the opinions to be expressed, or (iii) identify assumptions that the party’s attorney provided and that the expert relied on in forming opinions relied on in forming the opinions to be expressed.” But, as to non-testifying experts, who are engaged solely “in anticipation of litigation or to prepare for trial,” even communications regarding underlying facts may be privileged.<sup>48</sup>

Accordingly, as in the cases discussed in this Commentary, under the Federal Rules of Civil Procedure, understanding the nature of the expert’s retention and of his or her

<sup>45</sup> . *Williams v. Bridgeport Music, Inc.*, 300 F.R.D. 120, 122 (S.D.N.Y. 2014)(precluding discovery of the identity of an informal consulting expert); *Ager v. Jane C. Stormont Hospital and Training School for Nurses*, 622 F. 2d 496, 500-01 (10th Cir. 1980)(holding that Rule 26’s preclusion of discovery against non-testifying experts encompasses the identity of and other collateral information regarding the retention of experts consulted informally).

<sup>46</sup> . *Andritz, Sport-Bauer, Inc. v. Beazer E., Inc.*, 174 F.R.D. 609, 632 (M.D. Pa. 1997)(“Disclosure to agents retained by counsel to assist him or her in advising the client and handling legal matters does not operate as a waiver. The privilege attaches to agents and representatives of counsel whose services are necessary for effective representation of the client’s interests.”)

<sup>47</sup> . Fed. R. Civ. P. 26(b)(4)(B).

<sup>48</sup> . Fed. R. Civ. P. 26(b)(4)(D).



communications with counsel will be necessary to determine the extent of the privileges afforded to communications between the expert and counsel.

### C. APPLICATION OF ATTORNEY-CLIENT PRIVILEGE AND WORK-PRODUCT PROTECTION PRINCIPLES TO CYBERSECURITY INFORMATION

Taking the general principles of privilege and protection law and applying them to the CI context becomes more complex. The question of whether the attorney-client privilege or work-product protection applies to CI generally arises when a company is faced with litigation or a civil government investigation following a security incident. During this post-incident litigation or investigation, many types of CI may be sought by a regulator or private plaintiff concerning actions taken (or not taken) by the company prior to and after the security incident. These types of CI may be relevant to show the organization's security posture pre-incident, the causes of the incident, and the efficacy of the response.

This Part of the *Commentary* will discuss a variety of CI that organizations may create prior to a security incident when building and implementing a cybersecurity program, and in response to security incidents and breaches. To date, few courts have been faced with questions regarding whether to apply attorney-client privilege and work-product protection principles to the cybersecurity context. While parties often dispute attorney-client privilege and work-product protection issues in cybersecurity litigation or investigations, given the dearth of case law, such disputes appear to be primarily resolved without any judicial intervention. Thus, in addressing how courts may determine whether the attorney-client privilege or work-product protection attaches to certain CI, this Part analyzes not only on-point case law, but also decisions addressing similar types of documents in other contexts. This Part also extrapolates practices that may affect the likelihood that the attorney-client privilege and/or work-product protection will apply.

Because the legal concepts vary in some respects, we have divided this Part into sections separately dealing with the privilege and protection concepts that may apply to CI created (1) before a security incident is discovered ("pre-incident CI"), and (2) after a security incident is discovered (post-incident CI"). The third section of this Part discusses the various types of waiver that may apply if the CI holder discloses privileged or protected information.

This Part analyzes the application to CI of the general governing principles set forth in Part B. It does not consider whether CI should, as a policy matter, receive more or less protection than it does under the general governing principles set forth in Part B. That issue is, however, discussed at length in Part D. Moreover, Part C's analysis of the application of the attorney-client privilege to CI gives no consideration to the importance

Formatted: English (United States)

Formatted: Space After: 12 pt, Don't suppress line numbers

Formatted: Don't suppress line numbers

Formatted: Normal



of the CI in question to plaintiffs and regulators, because there is no basis in attorney-client privilege law for communications otherwise protected by the attorney-client privilege to lose that protection based on the need of the opposing party to obtain such discovery. On the other hand, such a basis does exist in work-product protection law, so Part C's analysis of the application of the work-product protection to CI gives substantial consideration to the importance of the CI in question to the party seeking the CI.<sup>49</sup>

1. *Legal Evaluation and Practice Guidelines as to Application of Attorney-Client Privilege and Work-Product Protection to Pre-Incident CI*

Pre-incident CI concerning an organization's security program, policies, and procedures prior to any security incident being discovered can fall into several distinct categories. Depending on the level of security protocols and programs in place and the size of the organization and its security team, an organization may have little-to-no pre-incident CI, or it may have large amounts. Because cybersecurity issues are multidisciplinary, involving technical tools and processes that interact with legal standards and obligations, this CI may or may not involve lawyers, consultants, technologists, security teams, and others at various stages and for various reasons.

a. *Types of Pre-Incident CI*

The potential pre-incident CI that may be sought in a post-incident situation includes the following, non-exhaustive list.

i. *Technical Inventories, Configuration Reviews, Vulnerability Scans, and Penetration Tests*

One aspect of pre-incident cybersecurity processes can include the identification and inventory of an organization's assets, data, and systems. This identification process allows organizations to prioritize risk and assign security controls in a methodical manner. A technical security expert or vendor may use a variety of tools to take an inventory of the network infrastructure, measure what devices are connected to the network, inventory the software applications installed and where the applications are installed, catalogue external information systems, map communication and data flows, and measure which software applications are up to date.

Configuration reviews may include review of the configuration of servers, firewalls, routers, and user accounts, and a review of certain related policies, such as how user groups are configured for permissions and access to the network.

Technical experts may also be hired, or the internal security team may be used, to conduct vulnerability scans to identify weaknesses in a network or system; for example,

<sup>49</sup> See Part C.2.c.ii, *infra*.

**Formatted:** Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5", Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Outline numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Indent at: 1", Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Normal



open ports, unregistered devices, or firewalls that are not turned on. These scans typically use software tools to investigate the current state of a computer system or network to identify points of weakness. Penetration tests add the aspect of exploiting discovered weaknesses to see if other checks and balances will nonetheless prevent the tester from doing harm to the system. Thus, the testing entity will attempt to access confidential, personal, or sensitive information, alter information, or shut down the system using one of the now-known vulnerabilities.

Data generated and retained with respect to these inventories, reviews, scans, and tests discloses the current state of the system, including possible gaps in security controls or related processes, potential vulnerabilities, and aspects that may be ripe for remediation. In most of these instances, the tools used and expertise required to perform the investigation of a system's "current state" are beyond the understanding of a lawyer or operational personnel within the organization. Thus, whether a lawyer is involved depends on the circumstances. For example, sometimes a basic vulnerability assessment may be conducted through interviews of employees and users to determine the location of weaknesses. This interview could uncover people- or process-oriented vulnerabilities. The interview may (or may not) have been done by a lawyer or someone from audit or compliance working under the direction of a lawyer. The CI in this instance may take the form of attorney notes and, potentially, a written compliance or gap report for management, with potential remediation.

Similarly, while these technical inventories, configuration reviews, vulnerability scans, and penetration tests may be part of an organization's larger risk assessment process done at the behest of counsel, those activities often do not involve counsel.

## ii. Security Risk Assessments, Outside Audits, and Remediation Efforts

Another aspect of pre-incident CI could be in the form of a security risk assessment, which may be completed internally or by hiring third-party security vendors and/or outside counsel. The risk assessment may include the entire organization or some specific systems (systems containing personal information, for example), or some aspect of the organization's security controls (vendor management, for example). The output of these security assessments is often a prioritized list of items the organization may wish to address with more extensive security measures. Sometimes these are technology-based, such as the need to encrypt certain types of data on portable media; sometimes these are process-based, such as the need to create a procedure for dealing with exiting and transferring employees; and sometimes these are people-based, such as the need to increase training or compliance.

If outside counsel is involved, these assessments may be done to help the lawyer explain to the organization what legal obligations it has, whether they are being met, and any opportunities to improve. Such legal assessments may also explain how the

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Normal



organization might remediate its security posture to meet those obligations, including addressing what specific activities are considered reasonable under various laws.

Legal counsel often will work with technical experts within the organization or hire technical experts to assist in creating a legally prioritized remediation report. Assessments prioritized by reference to the legal standards and environment in which the company operates, and conducted under the supervision of counsel, contain legal decisions about what is reasonable under the law for the particular organization.

Other times, only security vendors are involved, and while risks are categorized and prioritized, they typically are not done with reference to the legal environment in which the company sits, but rather prioritized according to technical standards. These security vendors are often, but not always, hired by the IT or security departments, and no counsel is involved.

In addition to security assessments, organizations will sometimes hire outside vendors to perform compliance audits, such as audits to assess for compliance with the Payment Card Industry Data Security Standard (PCI DSS). Again, these are often done without legal counsel's advice, in order to obtain independent certification of PCI compliance.

Following up on these assessments and audits, companies will often engage outside security vendors and/or legal counsel to assist in remediation of any gaps and/or opportunities for improvement identified in the security assessment or audit process.

### iii. Policies and Procedures

Many aspects of a well-run and reasonable cybersecurity system are documented in IT, management, or employee policies or procedures. This could include policies and procedures directed at one specific security control. For example, an access-control policy could dictate how to determine who has access to what, document these permissions, and describe the process for terminating such access, granting additional access, or changing access. Accompanying forms may provide documentation of these decisions, and accompanying procedures would describe how to implement the specific access controls associated with each decision. Another example could be a mobile-device policy regarding how to handle company-owned or "bring your own" mobile devices. The policy could also be one that concerns incident response, privacy and cybersecurity generally, or acceptable use. Some state and federal laws require that organizations maintain a written information security policy, and many other standards indicate that such written policies are a requirement of reasonable cybersecurity.

While the legal team (in-house or outside) will typically be involved in drafting and revising the policies required by state and federal law, that may not be the case with respect to more technology-focused procedures, or technical configuration procedures,

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Normal



such as the type of encryption to use at rest or in transit. During post-incident proceedings, both IT-focused and legal policies and procedures may be relevant and sought. In addition, drafts of those same policies and procedures may be requested. Decisions made during the drafting process may indicate risk-based approaches that can be questioned in hindsight.

#### iv. Tabletop Exercises

Organizations may test their incident detection and response times or the functioning of their incident response programs by conducting tabletop exercises. Tabletop exercises typically involve the presentation of one or more hypothetical scenarios involving a security incident meant to test the incident response capabilities of the organization. These exercises usually include gathering a group of high-level stakeholders within the company, including c-suite executives, the chief information security officer or other individuals responsible for the organization's security, and individuals from the organization's risk, communications, marketing, audit, business units, customer service, and legal teams. These exercises are typically conducted by outside counsel, a technology or security vendor, or a team of both.

In addition to any information documented before and during the tabletop, a lessons-learned report typically documents how the gathered team and the organization responded to the given hypothetical. Potential gaps in process, knowledge, culture, policy, and the like will often be documented with recommendations for improvement.

#### v. Internal Audit Reports

In the course of ensuring a robust security system, organizations often internally test the system controls in place to determine whether they are functioning as planned. The findings from internal audits or ongoing "maintenance" monitoring typically identify gaps in security processes or gaps between policies and practice.

#### vi. Reports of the Security Team

This category of documents includes reports of prior security events or incidents (that may or may not have led to a breach) drafted by the security team. Some of those documents will be forwarded to the legal team or the broader incident response team (if significant enough) to inform their advice and next steps, but many are not.

#### vii. Board-level Documents and Communications

This category includes reports given to the board or board committees responsible for overseeing cybersecurity, as well as meeting minutes or other documentation of the board or board committee itself. As with reports of the security team, some such board-

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Normal



level documents and communications will have been created by or with the involvement of lawyers, but that will not always be the case.

\* \* \*

Each of the above categories of pre-incident CI usually involves some assessment of the organization's information security posture. All will produce evidence of what the organization knew and when, and likely will result in the organization making decisions about what, if any, actions it will or will not take to reduce compliance gaps and identified risks. Below, this Part of the *Commentary* explores how the attorney-client privilege and work-product protection may apply to these general categories of CI, and what factors might be determinative in whether the protection attaches, recognizing that most determinations will be highly fact-specific.

#### b. Application of Attorney-Client Privilege to Pre-Incident CI

Under the basic principles of attorney-client privilege law (Part B, *supra*), the likelihood that pre-incident CI will be protected by the attorney-client privilege will vary, depending on the involvement of counsel in creating the CI in question, the purpose for counsel's involvement, and how the engagement or project is structured and executed. We examine the elements of the attorney-client privilege below and discuss the factors affecting whether the categories of pre-incident CI delineated above would likely be considered privileged under those general principles.

##### i. Involvement of a Lawyer

As discussed above, for documents and communications to be privileged, a lawyer must be involved in the circumstances surrounding the generation of the communication. If an attorney is not involved, under the general legal principles governing attorney-client privilege, the CI will not be considered privileged. Thus, referring back to the categories of CI listed above, any technical inventories, configuration reviews, vulnerability scans, or penetration tests that are done by an internal or outside security vendor or expert and not done to assist an attorney will not be privileged. The same is true for security risk assessments, outside or internal audits, tabletop exercises, reports of the security team, and board-level documents and communications.

##### ii. For the Predominant Purpose of Obtaining Legal Advice from the Lawyer

As discussed above, for documents and communications to be privileged, such documents and communications must have been made predominantly for the purpose of assisting counsel in rendering legal advice to a client.

Courts examining whether the communication is predominantly for the purpose of providing or soliciting legal (as opposed to business) advice will focus on several indicators. Courts will examine the content of the communications to determine whether

**Formatted:** Don't suppress line numbers

**Formatted:** Outline numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Indent at: 1", Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Outline numbered + Level: 1 + Numbering Style: i, ii, iii, ... + Start at: 1 + Alignment: Right + Aligned at: 0.75" + Indent at: 1", Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Normal



they contain or ask for legal analysis or whether they primarily concern the growth and development of profit.<sup>50</sup> In the context of pre-incident CI, the question of whether certain communications were made or documents created for the predominant purpose of obtaining or giving legal advice is difficult. With respect to technical inventories, configuration reviews, vulnerability scans, and penetration tests, these documents often are part of an organization's ongoing IT operations. For example, an inventory of devices, software, or locations of personal information is often part of the IT department's inventory control, which is a business function.<sup>51</sup> An organization may also measure response times for identifying, containing, and remediating security incidents to measure the quality and efficacy of its security team or to maintain its normal operations. This would also not be considered privileged, even if an attorney relied upon such information in conducting a security risk assessment, prioritizing legal risk, or in drafting a report for the board of directors.

However, if this CI was created for the purpose of a legally driven or mandated security assessment, audit, or report, such underlying documents may be privileged. One can readily envision the need for such a legal analysis for any type of organization handling sensitive information; this is especially true given the broad-ranging cybersecurity activities over which the Federal Trade Commission (FTC)<sup>52</sup> has taken enforcement actions, including, for example, protection of passwords or adequacy of operating system security on smartphones. Other laws and regulations governing specific industries or enacted in certain states have express security requirements or require organizations to have "reasonable" or "adequate" security. These requirements include overarching statements regarding the comprehensiveness of the program, the existence of policies and procedures, training requirements, and the effectiveness of the security program. Lawyers may need to give advice regarding whether the company's security requirements comply with these laws and regulations, which often are opaquely drafted. Similarly, many laws and regulations require organizations to oversee the security of their vendors, so legal analysis of such vendor oversight will be necessary. Counsel may also need to be involved regarding compliance with commercial contracts requiring one party to "provide reasonable security measures" for the other party's confidential information or to engage in "adequate security measures."

<sup>50-50</sup> See, e.g., *Fed. Trade Comm'n v. Abbvie, Inc.*, No. CV 14-5151, 2015 WL 8623076, at \*10 (E.D. Pa. Dec. 14, 2015); *Lindley v. Life Inv'rs Ins. Co. of Am.*, 267 F.R.D. 382, 392 (N.D. Okla. 2010), *aff'd in part as modified*, No. 08-CV-0379-CVE-PJC, 2010 WL 1741407 (N.D. Okla. Apr. 28, 2010).

<sup>51-51</sup> "[D]ocuments prepared by non-attorneys and addressed to non-attorneys with copies routed to counsel are generally not privileged since they are not communications made primarily for legal advice." *Neuder v. Battelle Pac. Nw. Nat'l Lab.*, 194 F.R.D. 289, 295 (D.D.C. 2000).

<sup>52-52</sup> The FTC is not the only regulator seeking broad enforcement powers in the data security context, but likely is the most active to date.

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



In other contexts, courts will generally find that documents not primarily concerned with business or marketing decisions, but rather primarily related to legal concerns (including legal risk and potential litigation or regulatory enforcement) are privileged.<sup>53</sup> Given the complex legal landscape and varying cybersecurity standards applicable to organizations, to the extent a lawyer engaged in a security risk assessment or audit focused on prioritizing security controls based on legal risks or compliance with legal requirements, as opposed to business decisions, courts may well find this pre-incident CI primarily related to legal concerns and risk and therefore privileged.<sup>54</sup>

Similarly, internal audit reports drafted to provide insight to counsel, when counsel provides revisions and comments and uses the reports to provide advice to the organization, often are considered privileged in other contexts<sup>55</sup> and thus would normally be expected to be privileged in the CI context. However, courts will carefully scrutinize whether the primary purpose of creating the report was truly to assist counsel's provision of legal advice. The court held in *In re Premera Blue Cross Customer Data Security Breach Litigation (Premera II)* that internal data-security reports prepared before any breach had been discovered (as part of normal business functions), for the purpose of enabling the company to assess the state of its technology and security, were not privileged—even if counsel supervised the audits and later used them for legal advice.<sup>56</sup> But *Premera II* also held that if the draft report or emails about the draft were sent to counsel seeking legal advice, those documents would be protected.<sup>57</sup> In other legal contexts, such as securities litigation, reports from counsel to boards of directors, committees, subcommittees, and senior executives are largely considered the provision of legal advice and subject to

<sup>53-53</sup> See *In re Denture Cream Prods. Liab. Litig.*, No. 09-2051-MD, 2012 WL 5057844, at \*15 (S.D. Fla. 2012) (finding documents regarding legal concerns, including potential litigation, related to product labeling, as opposed to marketing and business decisions related to labeling, privileged); see also *Shire Dev. Inc. v. Cadila Healthcare Ltd.*, C.A. No. 10-581-KAJ, 2012 WL 5247315, at \*7 (D. Del. June 15, 2012) (finding presentation by lawyer reflected legal advice concerning patent design decisions and was therefore privileged).

<sup>54</sup> See Order, *In re Arby's Restaurant Group, Inc. Data Security Litigation*, No. 1:17-cv-00514 (N.D. Ga. Mar. 25, 2019) (communications between a technical consultant and counsel, which had occurred prior to the discovery of the company's security incident, were protected by the attorney-client privilege where the consultant's role had been to assist counsel in connection with a "gap analysis" concerning the company's compliance with the PCI DSS).

<sup>55-55</sup> See *United States v. Lockheed Martin Corp.*, 995 F. Supp. 1460, 1464 (M.D. Fla. 1998) (finding that an internal audit report drafted by a nonlawyer but provided to a lawyer for revisions and used by the lawyer to provide legal advice was privileged).

<sup>56-56</sup> 329 F.R.D. 656, 666 (D. Or. 2019) [hereinafter *Premera II*].

<sup>57-57</sup> *Id.* at 667.

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



privilege protection.<sup>58</sup> Courts would likely treat the cybersecurity context no differently. If a security report to the board of directors is by an attorney and incorporates a security team report, the report may be considered privileged, whereas a security team report without the attorney analysis likely will not be considered privileged. In this pre-incident CI context, this could include not only reports on legal risk, but also reports to the board concerning disclosures to the Securities and Exchange Commission (SEC) in connection with security-related incidents and cybersecurity risk in general. The reports of the board itself are likely not privileged, unless the board hires counsel to represent it in the preparation of the report.<sup>59</sup>

With respect to policies and procedures, generally, attorney-client privilege will apply to protect preliminary drafts of policies and procedures that contain legal advice and attorney opinions;<sup>60</sup> for example, if the policy or procedure contains comments to omit or add certain language for legal reasons. However, privilege will typically not apply to the final versions of policies and procedures merely because they were drafted by in-house or outside counsel; the final versions constitute business communications, not legal advice communications.<sup>61</sup> These general principles appear as applicable to CI policies and procedures as to those that are created in other contexts.

In addition to the involvement of an attorney and whether the pre-incident CI was reviewed and revised or created to assess legal risk or otherwise assist in the provision of legal advice, the creator of the communication may have some impact on whether a court will determine that the communication was made predominantly for the purpose of seeking legal advice. But “the mere fact that a document is created by a non-attorney is not dispositive of the privilege question, so long as the communication of the document to counsel was confidential and for the primary purpose of seeking legal advice.”<sup>62</sup> Thus, whether the communicator is an attorney, or a member of the security team, or otherwise from the business, should not affect the ultimate decision of whether privilege applies, as long as the communication was made predominantly for the purpose of seeking or

<sup>58-58</sup> See, e.g., *In re LTV Sec. Litig.*, 89 F.R.D. 595, 603 (N.D. Tex. 1981).

<sup>59-59</sup> See, e.g., *Picard Chem. Inc. Profit Sharing Plan v. Perrigo Co.*, 951 F. Supp. 679, 689 (W.D. Mich. 1996).

<sup>60-60</sup> See, e.g., *Dewitt v. Walgreen Co.*, No. 4:11-CV-00263-BLW, 2012 WL 3837764, at \*6 (D. Idaho Sept. 4, 2012).

<sup>61-61</sup> See, e.g., *Stevens v. Corelogic, Inc.*, No. 14CV1158 BAS (JLB), 2016 WL 397936, at \*4 (S.D. Cal. Feb. 2, 2016).

<sup>62-62</sup> *United States v. ISS Marine Servs., Inc.*, 905 F. Supp.2d 121, 128–29 (D.D.C. 2012) (citing *In re Grand Jury (Attorney–Client Privilege)*, 527 F.3d 200, 201 (D.C. Cir. 2008) (“Attorney-client privilege applies to a document a client transfers to his attorney ‘for the purpose of obtaining legal advice.’” (quoting *Fisher v. United States*, 425 U.S. 391, 404–5 (1976)))).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



providing legal advice. However, some courts apply additional scrutiny to communications between in-house (as opposed to outside) counsel and corporate employees to determine whether such communications were made predominantly for a legal as opposed to a business purpose.<sup>63</sup> By contrast, under the general tenets of attorney-client privilege law, communications from “outside counsel are presumed to be made for the purpose of providing legal advice.”<sup>64</sup> Thus, communications from in-house counsel may be less likely to be considered privileged, particularly with respect to security assessments, audits, and reports that have a dual purpose.

### iii. Among or Within Privileged Persons

To be privileged, the communication must also be among or within privileged persons. To the extent an employee of the client sent or received the communication, the employee must qualify as part of the client under either the subject-matter or control-group tests described in Part B above. If not—for instance, because the communication was by a front-line IT analyst outside of the “control group” in a control-group jurisdiction—the privilege generally will not apply.<sup>65</sup>

~~Also, courts~~ Courts will also scrutinize communications with outside experts or consultants by an organization or outside counsel to determine whether the use of the third-party expert was necessary for the provision of the legal advice, or whether the consultant was a functional equivalent of a corporate employee. If either is true, courts may extend the attorney-client privilege to cover these experts and consultants.

<sup>63</sup> <sup>63</sup> See *United States v. ChevronTexaco Corp.*, 241 F. Supp.2d 1065, 1076 (N.D. Cal. 2002) (“[U]nlike outside counsel, in-house attorneys can serve multiple functions within the corporation. In-house counsel may be involved intimately in the corporation’s day to day business activities and frequently serve as integral players in business decisions or activities. Accordingly, communications involving in-house counsel might well pertain to business rather than legal matters. The privilege does not protect an attorney’s business advice.”); see also *McGowan v. JP Morgan Bank, N.A.*, 2020 WL 1974109 at \*5-6 (S.D.N.Y. April 24, 2020) (holding that an internal human resources investigation that initially was not privileged became privileged when the company’s in-house counsel stepped in to review allegations of discrimination and unequal treatment. The court noted that an “employer’s investigation may shift from an internal investigation in response to plaintiff’s claims to an investigation for the purpose of mounting a legal defense against such claims,” and found that, once in-house counsel stepped in, the character of the investigation changed to one focused on mounting a legal defense).

<sup>64</sup> <sup>64</sup> *Id.* (emphasis omitted).

<sup>65</sup> <sup>65</sup> See, e.g., *Valenti v. Rigolin*, 1:01-cv-05914, 2002 WL 31415770, at \*3 (N.D. Ill. Oct. 25, 2002) (statement by nurse to employer’s counsel not privileged because nurse was outside the control group).

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



In 1961, in *Kovel*,<sup>66</sup> the U.S. Court of Appeals for the Second Circuit ~~decided *United States v. Kovel*,<sup>67</sup> in which it~~ considered whether communications with an accountant prevented attorney-client privilege protection. *Kovel* held that if the accountant (or other third party) was necessary to “interpret” a client’s “complicated tax story to the lawyer” to enable the lawyer to represent the client, the accountant did not destroy the privilege between the lawyer and his client. ~~Courts~~As noted above, courts following *Kovel* have extended the doctrine to allow the attorney-client privilege to cover communications to and from other, non-accountant third-party experts and consultants in some circumstances as long as the communications were necessary to assist the lawyer in communicating with the client. Typically, communications with experts in the course of an engagement will not be considered privileged if (1) the communications were not necessary to assist the attorney in understanding communications from the client, or (2) the consultant’s expertise was used to make a business decision, rather than to assist the lawyers in communicating legal advice.<sup>68</sup>

The attorney-client privilege may also extend to third parties acting as agents of the client, rather than as an agent of the lawyer as under *Kovel*, although it is more limited. The functional-equivalent doctrine will apply when a third party is retained by a company and is intended to, and does, function as an employee.<sup>69</sup> To determine whether such a third party functions as an employee, courts will look to whether the third party was an integrated member of the company, whether he or she played a significant role in the company, and whether he or she was intimately involved in the creation, development, and implementation of information at issue in the privilege determination and/or the relevant project.<sup>70</sup>

<sup>66</sup> . 296 F.2d 918, 922–23 (2d Cir. 1961).

~~<sup>67</sup> . 296 F.2d 918, 922–23 (2d Cir. 1961).~~

<sup>68</sup><sup>68</sup> See, e.g., *Scott v. Chipotle Mexican Grill*, 94 F. Supp.3d 585, 590-91 (S.D.N.Y. 2015) (finding that a human relations consultant’s report provided to counsel concerning classification of its employees by title was not protected under the *Kovel* doctrine because the consultant engaged in factual research to assist in making a business decision); *Church & Dwight Co. Inc. v. SPD Swiss Precision Diagnostics, GmbH*, No. 14-cv-585, 2014 WL 7238354, at \*2 (S.D.N.Y. Dec. 19, 2014) (holding that a lawyer’s communications with an outside marketing firm were not protected from disclosure under *Kovel* in the context of launching a new product inside a complex regulatory scheme, because the expert was not necessary for lawyers to understand communications from the client, and the lawyers could get the necessary expertise without revealing privileged information).

<sup>69</sup><sup>69</sup> See, e.g., *In re Flonase Antitrust Litig.*, 879 F. Supp.2d 454, 458 (E.D. Pa. 2012); *In re Copper Mkt. Antitrust Litig.*, 200 F.R.D. 213, 220 n.4 (S.D.N.Y. 2001); *In re Myers*, No. 11-61426, 2013 WL 6092447, at \*2 (Bankr. N.D. Ohio Nov. 18, 2013) (information provided to attorney by attorney-hired accountant, as agent for the client, held subject to the attorney-client privilege).

<sup>70</sup><sup>70</sup> See, e.g., *In re Flonase*, 879 F. Supp. 2d at 454.

Formatted: Font: 10 pt, Font color: Black

Formatted: Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



If a third party creates pre-incident CI, then it is possible that technical inventories, configuration reviews, penetration tests, and other pre-incident CI may be considered privileged if they were created for the purpose of aiding counsel in providing an assessment or report to the client. In *In re Arby's Restaurant Group, Inc. Data Security Litigation*, the court held that communications between a technical consultant and counsel, which had occurred prior to the discovery of the company's security incident, were protected by the attorney-client privilege where the consultant's role had been to assist counsel in connection with a "gap analysis" concerning the company's compliance with the PCI DSS.<sup>71</sup> In a decision concerning post-incident CI, *Genesco Inc. v. Visa, Inc.*, the court found that an assessment performed on the client's behalf, which suggested remediation measures, was attorney-client privileged because the expert was "retained . . . to provide consulting and technical services so as to assist counsel in rendering legal advice."<sup>72</sup> While this concerned post-incident CI, the logic appears to apply equally to pre-incident CI.

Therefore, the structure and purpose of outside vendor engagement are factors used by courts to determine whether the attorney-client privilege applies. Pre-incident CI created by third parties may more likely be considered privileged if outside counsel retains the expert and provides clear instructions in the engagement letter that the expert has been retained to assist counsel in providing legal advice. It may also be more likely to be considered privileged if counsel oversees the expert and participates in communications between the client and the expert. Finally, in determining whether a third party's communications were made to assist counsel in providing legal advice, courts have evaluated whether counsel in fact reviewed, and provided legal advice based on, the observations and findings by the expert.<sup>73</sup>

#### iv. Reasonable Expectation the Communication Will Be Kept Confidential

As noted in Part B above, to be privileged, the communication must have been made in confidence, i.e., with the intent that it be kept confidential. If CI is created for the purpose of being shared with a third party outside the circle of privileged persons—for instance, a description of IT inventory prepared for distribution to an assessor not working for the company's counsel—the communication will not have the requisite confidentiality, and the privilege will not attach.<sup>74</sup> Once a communication is privileged,

<sup>71-71</sup> Order, No. 1:17-cv-00514 (N.D. Ga. Mar. 25, 2019).

<sup>72-72</sup> Case No. 3:13-cv-00202, 2015 WL 13376284, at \*1 (M.D. Tenn. Mar. 25, 2015).

<sup>73-73</sup> See, e.g., *United States v. Lockheed Martin Corp.*, 995 F. Supp. 1460, 1464 (M.D. Fla. 1998).

<sup>74-74</sup> See, e.g., *In re Grand Jury Proceedings*, 33 F.3d 342, 353-54 (4th Cir. 1994) (communication intended for public disclosure not privileged).

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



the question of whether further disclosure of the communication would destroy the privilege is an issue of waiver, addressed in subsection 3 below.

### c. Application of Work-Product Protection to Pre-Incident CI

As discussed in Part B, the work-product protection doctrine applies only to documents created “in anticipation of litigation.” Although the application of this doctrine varies somewhat across states and jurisdictions, the requirement for the organization to perceive a real threat of litigation, rather than merely speculate that sometime in the distant future there might be litigation, will typically result in no work-product protection being afforded to any of the above types of pre-incident CI.

## 2. Legal Evaluation and Practice Guidelines as to Application of Attorney-Client Privilege and Work-Product Protection to Post-Incident CI

In addition to CI created prior to the discovery of a security incident, several types of documents may be created following discovery of a security incident that an organization may consider or want to have considered protected by the attorney-client privilege or the work-product protection.

### a. Examples of Post-Incident CI

#### i. Forensic Investigations—Documents and Reports

These documents include forensic investigations into the security incident, the vulnerability exploited, how it was exploited, what evidence of the incident is available, and what information may have been compromised. These forensic investigations are done by a forensic expert and may be conducted through in-house or outside counsel, but may also be commissioned by the organization’s internal security team.

#### ii. Post-Incident Security Assessments

Organizations may also conduct, through a security expert, outside counsel, or both, a post-incident assessment into the organization’s cybersecurity posture. This assessment could span far more of the organization’s data infrastructure and security readiness than what would be necessary to determine the reasons for the security incident at issue. Some assessments, however, are narrowly tailored to a particular aspect of the organization’s security posture associated with an incident.

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Outline numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75", Don't suppress line numbers, Hyphenate

Formatted: Outline numbered + Level: 1 + Numbering Style: i, ii, iii, ... + Start at: 1 + Alignment: Right + Aligned at: 0.75" + Indent at: 1", Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Normal



### iii. Remediation Efforts and Crisis Management<sup>75</sup>

In all post-incident scenarios, organizations will have some documents related to their efforts to remediate the incident that were generated by the security or technology team. There may also be communications about the incident, including internal communications with legal counsel, senior executives, human resources personnel, communications staff, boards of directors, and other portions of the organization, including with respect to: remediation, fact-finding, escalation, whether to notify various entities and individuals, how to notify and what to include in the notifications, and any legal analyses of such incident (including but not limited to litigation and regulatory risk and, for public companies, whether disclosure is required to the SEC). These same types of communications may occur not only internally, but also with outside counsel and public relations consultants, among others. Entities suffering a security incident may also consider whether they should or need to notify an insurance carrier or contractual third party whose systems or data may have been involved in the incident.

\* \* \*

As discussed below, in trying to determine whether documents falling in the above categories should be considered attorney-client privileged and/or work-product protected, and what practices may affect that determination, a few cases involving post-incident CI provide some guidance. In the world of post-incident CI, courts faced with privilege and protection issues have been attempting to apply general legal principles to these unique sets of documents. These fact-intensive decisions (as with most attorney-client privilege and work-product protection cases) will turn on a court's decision as to whether the communication was made to solicit or render legal advice or in anticipation of litigation.

#### b. Application of Attorney-Client Privilege to Post-Incident CI

In the context of post-incident CI, courts have begun to grapple with applying general principles of attorney-client privilege, but the case law is still in its relative infancy. ~~Few~~The few cases that directly address these issues, ~~but the ones that do~~ provide invaluable guidance, even though they do not always clearly distinguish between the type of protection being applied or the exact purpose for which it is or is not being applied in any given circumstance. For example, when attempting to determine whether the report of a forensic expert is protected (by either the attorney-client privilege or the work-product protection), courts may not distinguish between whether the report was

---

<sup>75</sup> Whether legally required notifications or communications with law enforcement, state attorneys' general, and other governmental entities will waive the privilege is discussed below, even though interaction with law enforcement is often done during and as part of the remediation efforts and crisis management.

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Don't suppress line numbers

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



commissioned by an attorney “for the purpose of providing legal advice” (attorney-client privilege) or whether the report was drafted in a certain way “because of anticipated litigation” (work-product protection). For purposes of this Part of the *Commentary*, we have attempted to distinguish between the attorney-client privilege and the work-product protection where possible, noting along the way the ambiguities in the existing case law.

i. For the Predominant Purpose of Obtaining Legal Advice from a Lawyer

As with pre-incident CI, whether the predominant purpose of the CI in question was to provide legal advice, as opposed to serving a business purpose, is likely to become a prevalent inquiry in deciding whether certain post-incident CI is privileged. This especially may be the case when in-house counsel is communicating internally with the organization directly following the incident. For example, questions may arise regarding whether the in-house counsel is merely trying to remedy the breach or is providing legal advice concerning how to manage breach notifications or legal risk. The communications may have a dual purpose to both assist in breach remediation *and* breach notification management or legal risk analysis, in which case the courts will determine the predominant purpose of the communications.

In *In re Target Corp. Customer Data Security Breach Litigation*, the court examined whether various types of post-incident CI were protected by the attorney-client privilege.<sup>76</sup> The court analyzed whether the privilege applied to CI relating to a data-breach task force that Target established by Target in response to respond to the data breach.<sup>77</sup> Plaintiffs’ counsel argued that the communications and documents were not protected by the attorney-client privilege because “‘Target would have had to investigate and fix the data breach regardless of any litigation, to appease its customers and ensure continued sales, discover its vulnerabilities, and protect itself against future breaches.’”<sup>78</sup> Target argued that those communications and documents were protected because the task force was established at the request of its lawyers (both in-house and retained) to educate counsel about the breach and allow counsel to provide Target legal advice.<sup>79</sup> While the court did not specifically weigh the business and legal purpose of various CI, it did determine that some internal communications were privileged, while others were not, by discussing the purpose of the communications. Specifically, the court found that

<sup>76-76</sup> 2015 WL 6777384 (D. Minn. Oct. 23, 2015).

<sup>77-77</sup> *Id.* at \*1.

<sup>78-78</sup> *Id.* (quoting Pls.’ Letter Br. 3-4).

<sup>79-79</sup> *Id.*<sup>79</sup> *Id.*; see also *In re Marriott International, Inc. Customer Data Security Breach Litig., Case No. 8:19-md-02879-PWG* (D. Md. June 2, 2021)(*ruling that emails within the company to employees that were never transmitted to counsel are not privileged, even though made as part of counsel-directed breach investigation...*).

**Formatted:** Outline numbered + Level: 1 + Numbering Style: i, ii, iii, ... + Start at: 1 + Alignment: Right + Aligned at: 0.75" + Indent at: 1", Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font color: Black

**Formatted:** Normal



internal communications from Target’s CEO to the Board of Directors were not privileged because they did not “involve any confidential communications between attorney and client, contain requests for or discussion necessary to obtain legal advice, nor include the provision of legal advice.”<sup>80</sup> Conversely, the court did find that other communications with and documents created by the task force were privileged, as Target had demonstrated that the task force “was focused not on remediation of the breach, . . . 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.”<sup>81</sup> The court also found other email communications between in-house counsel and other Target employees privileged because they were made for the purpose of obtaining legal advice.<sup>82</sup> Evident in the court’s determination is a consideration specifically regarding whether the communications and documents were created for the predominant purpose of providing or obtaining legal advice.

The District of Oregon, in *In re Premera Blue Cross Customer Data Security Breach Litigation (Premera I)*,<sup>83</sup> had opportunity to do the same. Similar to the court in *Target*, the *Premera* court engaged in a detailed analysis of whether CI was created for the primary purpose of informing counsel so that counsel could provide legal advice. The court evaluated the purpose behind CI created by non-attorneys that “incorporated” advice of counsel but were not sent to counsel, and CI created by employees “supervised” by counsel.<sup>84</sup> The court examined whether the CI was prepared primarily to assist counsel in providing legal advice, or whether the CI was prepared by the business to fulfill a business function, or required to be prepared by the business in response to the data breach, such as press releases, media interactions, and notices to consumers.<sup>85</sup> Generally, the court found that this CI was created for business purposes, not legal ones.<sup>86</sup> However, attorney redlines or edits communicating legal advice would be covered by the attorney-client privilege.<sup>87</sup>

Subsequently, in *Premera II*, the District of Oregon assessed the application of the attorney-client privilege to CI that was sent to and from counsel, as well as CI prepared at the request of counsel. The court stated that in order to qualify for the attorney-client

<sup>80</sup> *Id.* at \*2.

<sup>81</sup> *Id.* at \*3.

<sup>82</sup> *Id.*

<sup>83</sup> 296 F. Supp.3d 1230 (D. Or. 2017) [hereinafter *Premera I*].

<sup>84</sup> *Id.* at 1240–47.

<sup>85</sup> *Id.*

<sup>86</sup> *Id.*

<sup>87</sup> *Id.* at 1242, 1250.

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



privilege, emails sent to and from counsel about matters such as press coverage, notices to consumers, and remediation must request or provide legal advice (as opposed to containing merely a factual discussion), or they must contain facts transmitted to counsel so that counsel can provide adequate legal representation.<sup>88</sup> The court further stated that draft documents (e.g., draft notices) prepared by attorneys, at the request of attorneys, or by company employees or vendors and sent to or from attorneys for legal advice relating to the drafts are likely subject to the attorney-client privilege.<sup>89</sup> However, in the court's view, a draft document that is prepared for a business purpose and merely sent to an attorney for the attorney's file or information, or is distributed among company employees or to third-party vendors for general discussion with an attorney merely copied, is not privileged merely because an attorney received it.<sup>90</sup> The court further held that Premera's "investigation into the breach was conducted primarily for a business purpose."<sup>91</sup> But if an attorney took the information from these documents and drafted a different document in preparation for litigation, and/or received emails or draft reports seeking the attorney's advice, those documents would be protected.<sup>92</sup> And the court allowed that CI relating to Premera's later actions in response to the breach may also be privileged: "Other than the initial business steps of remediation, notifying customers, and making public statements, which Premera would have had to do regardless, the later actions by Premera were likely guided by advice of counsel and concerns about potential liability."<sup>93</sup>

More recently, in *Attorney General v. Facebook, Inc.*,<sup>94</sup> the Supreme Judicial Court of Massachusetts considered whether the Massachusetts Attorney General's requests for information related to Facebook's investigation into Cambridge Analytica's use of Facebook user information, sought privileged communications between Facebook and its counsel. Facebook launched an internal "App Developer Investigation" ("ADI") in March 2018 in response to the revelation that Cambridge Analytica had used data it obtained through a Facebook app developer to influence the 2016 United States Presidential election. After public reporting revealed Cambridge Analytica's misuse of the data, Facebook hired counsel to "conduct a far-reaching investigation to identify the extent to which apps had misused user data, and advise Facebook on potential resulting

<sup>88</sup> 329 F.R.D. 656, 662–66 (D. Or. 2019).

<sup>89</sup> *Id.*

<sup>90</sup> *Id.*

<sup>91</sup> *Id.* at 666.

<sup>92</sup> *Id.* at 666–67.

<sup>93</sup> *Id.*

<sup>94</sup> 164 N.E. 3d 873, 877 (March 24, 2021).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



legal liabilities.”<sup>95</sup> The Massachusetts Attorney General issued Civil Investigative Demands to Facebook, serving six requests for documents. Facebook resisted each request citing attorney-client privilege and work product.

Resolving Facebook’s attorney-client privilege arguments, the court found that the Attorney General had narrowly targeted its first five requests to avoid disclosing attorney-client privileged communications.<sup>96</sup> For example, the Attorney General asked that Facebook identify the apps that Facebook suspended, and provide its internal policies and procedures governing the use of third-party apps.<sup>97</sup> The information that the Attorney General requested included, inter alia, the identification of the app developer or publisher, the date on which Facebook first reviewed the app’s privacy policy, and the number of users who installed or downloaded the app.<sup>98</sup> For the first five requests, the Attorney General specified that Facebook could produce a spreadsheet containing the information, rather than responsive documents. Accordingly, the court observed, Facebook was not required to produce documents sent to or created by counsel.<sup>99</sup>

Facebook had argued that the Attorney General’s requests sought information that did not exist independently of its communications with its counsel. The court observed that Facebook’s position “failed to take into account the fact that the underlying data about apps’ breaches of privacy policies is all independently discoverable and cannot be protected by Facebook’s initiation of its own factual investigation.”<sup>100</sup> The production of those facts, which had “almost certainly been contained in attorney-client communications,” did not, however, “require the production of the attorney-client communications themselves.”<sup>101</sup>

In its sixth request, however, the Attorney General asked Facebook to produce internal communications about the third-party apps.<sup>102</sup> These, the court held, were privileged. The court focused on the distinction between attorney-client communications and underlying facts, noting that the attorney-client privilege does not “immunize underlying facts available from another source from discovery just because a client disclosed the facts to an attorney.”<sup>103</sup> The court held that the attorney-client privilege did protect those communications between counsel and Facebook made as part of the internal

<sup>95</sup> . *Id.* at 880-881.

<sup>96</sup> . *Id.* at 880.

<sup>97</sup> . *Id.* at 881.

<sup>98</sup> . *Id.*

<sup>99</sup> . *Id.* at 882.

<sup>100</sup> . *Id.* at 887.

<sup>101</sup> . *Id.*

<sup>102</sup> . *Id.*

<sup>103</sup> . *Id.* at 886, quoting *Upjohn Co. v. United States*, 449 U.S. 383, 395-396, 101 S. Ct. 677, 66 L. Ed. 2d 584 (1981) (“A fact is one thing and a communication concerning that fact is an entirely different thing.”)



investigation, undertaken to gather facts to provide legal advice.<sup>104</sup> The court observed that, given the breadth of the sixth request, it was possible that the request sought information outside of the investigation that might not otherwise involve the attorney-client privilege.<sup>105</sup> Therefore, agreeing with the trial court, the Supreme Judicial Court remanded the matter so that Facebook could prepare a detailed privilege log, which would allow the Attorney General to challenge each withheld document individually.

By contrast, in a Report & Recommendation In re Marriott International, Inc. Customer Data Security Breach Litig., Case No. 8:19-md-02879-PWG (D. Md. June 2, 2021), the court protected as privileged e-mails and documents that Marriott's employees transmitted to Marriott's outside counsel, sent for the purposes of offer and receipt of legal advice. This included email attachments that concerned underlying facts of the investigation. The plaintiff had argued that the attachments were not, and should not be, protected by the attorney-client privilege. The court disagreed. While documents do not "become privileged merely because they are communicated to an attorney,"<sup>106</sup> the court noted, the court rejected the plaintiff's argument that "whatever the client gave the lawyer that is not a direct communication to her from the client lost its protection because the client did not utter the words in the document to the lawyer."<sup>107</sup> The court focused on the client's intent in transmitting the document to the lawyer. "A document that a client transmits to a lawyer maintains its protection if the client transmits the document intending that the lawyer consider it in providing legal services or legal advice to the client."<sup>108</sup> The fact that a client includes a document in a request for legal advice is in and of itself privileged, because it "partially reveals the substance of the client's privileged communication to an attorney." The e-mail, with its attachment, is privileged.

In Marriott, the court also sustained Marriott's privilege claim over post-breach work that IBM had performed to (i) assist Marriott's counsel in understanding how Marriott's security alerting tool functioned, and (ii) conduct a post-incident security assessment. The plaintiff urged the court to find that, because of a pre-existing business relationship between Marriott and IBM, Marriott's reason for retaining IBM was business-driven. The court disagreed, finding instead that the declarations that Marriott submitted demonstrated that the purpose for IBM's inquiry into the alert system was to help Marriott's counsel understand a distinct issue relating to the alerting system, to assist Marriott to understand its legal obligations. The court further found that IBM performed

---

<sup>104</sup> . *Id.* at 888.

<sup>105</sup> . *Id.* at 888-89.

<sup>106</sup> . Marriott Int'l, Case No. 8:19-md-02879-PWG (D. Md. June 2, 2021), citing Greenwald, et al., Testimonial Privileges, section 1:19 at 76 (2019-2020).

<sup>107</sup> . *Id.*

<sup>108</sup> . *Id.*



the post-breach security assessment to assist Marriott's counsel to develop Marriott's legal strategy for responding to regulatory investigations and lawsuits.

ii. Among or Within Privileged Persons

Courts conduct a similar analysis with respect to CI created by third parties. In *Genesco*,<sup>109</sup> Genesco brought suit against Visa in response to Visa's attempt to assess more than \$13 million in fines and assessments for Genesco's alleged failure to comply with Visa's cybersecurity standards. Visa had assessed the fines and assessments in response to a breach of Genesco's network that exposed credit card data.<sup>110</sup> Genesco retained a forensic investigator, Stroz Friedberg, to provide consulting and technical services to Genesco's in-house and outside counsel regarding the breach and its own cybersecurity posture, as well as with respect to a report issued by a forensic investigator authorized by the Payment Card Industry Security Standards Council, Trustwave International Security and Compliance (Trustwave).<sup>111</sup> Genesco provided evidence that it retained Stroz Friedberg, through outside counsel, specifically to conduct an investigation, under privilege, following the earlier investigation by Trustwave, to assist Genesco's attorneys in providing it legal advice.<sup>112</sup>

In these circumstances, the court, relying on *Kovel*, found that the documents and communications generated by the forensic expert were protected by the attorney-client privilege because the expert was "retained by counsel for the purpose of providing legal advice."<sup>113</sup> The court noted that the privilege extended to Stroz Friedberg because the firm "assisted counsel in his investigation."<sup>114</sup> The court also found, separately, but relying on its earlier ruling, that the privilege applied to documents and communications with IBM, which was retained to provide advice concerning remediation, because it was also hired to assist counsel in rendering legal advice to Genesco.<sup>115</sup>

<sup>109</sup> *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 170 (M.D. Tenn. 2014).<sup>109</sup>  
*Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 170 (M.D. Tenn. 2014).

<sup>110</sup> *Id.*

<sup>111</sup> *Id.* at 169.

<sup>112</sup> *Id.* at 180–81.

<sup>113</sup> *Id.* at 190 (citing *United States v. Kovel*, 296 F.2d 918, 922 (2d Cir. 1961)). As noted above, it is unclear from the decision how important the retention of the third party was to the determination that the privilege applied.

<sup>114</sup> *Id.*

<sup>115</sup> *Genesco, Inc. v. Visa USA, Inc.*, Case No. 3:13-cv-00202, 2015 WL 13376284, at \*1 (M.D. Tenn. Mar. 25, 2015).

**Formatted:** Indent: Left: 0.25", First line: 0", Space Before: 0 pt, After: 0 pt, Don't suppress line numbers, Hyphenate

**Formatted:** Space Before: 12 pt, Don't suppress line numbers

**Formatted:** Don't suppress line numbers

**Formatted:** Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between: (No border), Tab stops: 0.25", Right + 0.38", Left

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Normal



The court also addressed the privilege issues associated with third-party consultants in the *Target* case.<sup>116</sup> In that case, Target had hired a consultant firm to conduct two investigations following its breach. One investigation was conducted by Target's outside counsel, which hired the expert to provide the attorneys information about the breach and how to defend Target; the other investigation was conducted by the consultant firm "on behalf of several credit card brands" to assist in determining how the breach happened and how to remediate.<sup>117</sup> While the two investigations were being conducted by the same outside technical firm, the consultant set up two separate teams that did not communicate with one another.<sup>118</sup> At issue in the action was whether the documents created by and communications with the consultant team hired by outside counsel were privileged and protected from disclosure.<sup>119</sup>

The court found that the documents associated with the team of experts retained by outside counsel were protected by the attorney-client privilege because the investigation "was focused not on remediation of the breach, . . . 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."<sup>120</sup>

Similarly, the *Premera* decisions evaluated whether CI created by a third-party public relations firm<sup>121</sup> to inform counsel and by a third-party forensic investigator prior to and after the discovery of the breach was protected by the attorney-client privilege.<sup>122</sup> Relying on the primary purpose of the third party, the *Premera I* court generally found that CI created by an attorney-hired public relations firm following the breach (and communications between the firm and *Premera*) was not privileged. The court relied on the business nature and function of the public relations firm and denied the ability of companies to cloak CI in privilege merely by claiming such CI was created on behalf of an attorney or under the supervision of an attorney. Likewise, the court in *Premera II* held that merely sending such CI to counsel did not make it privileged.<sup>123</sup> The court held in *Premera I* and *II*, however, that if communications were sent to or from counsel seeking or

<sup>116</sup> *In re Target Corp. Customer Data Security Breach Litigation*, MDL No. 14-2522 (PAM/JJK), 2015 WL 6777384, at \*1 (D. Minn. Oct. 23, 2015).

<sup>117</sup> *Id.*

<sup>118</sup> *Id.*

<sup>119</sup> *Id.*

<sup>120</sup> *Id.* at \*3.

<sup>121</sup> The court conducted a similar analysis with respect to eDiscovery and other vendors hired by *Premera*. *Premera I*, 296 F. Supp.3d 1230, 1240-47 (D. Or. 2017).

<sup>122</sup> *Id.*

<sup>123</sup> *Premera II*, 329 F.R.D. 656, 663 (D. Or. 2019).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



providing actual legal advice, such as about possible legal consequences of proposed text or an action being contemplated by Premera, then such communications would be privileged.<sup>124</sup>

In connection with the third-party forensic investigator, two sets of CI were at issue: (1) CI created by the investigator prior to discovery of the breach, when the investigator had been hired by the company; and (2) CI, including at least one forensic report, created by the investigator after the discovery of the breach, after being hired by counsel, and after entering into a new and separate statement of work.<sup>125</sup> The court summarily rejected the notion that simply because the forensic investigator was hired by counsel after discovery of the breach, documents and communications relating to that investigator would necessarily be covered by the attorney-client privilege.<sup>126</sup> Largely relying on the fact that the company had initially hired the forensic investigator for business purposes prior to discovery of the breach, the court found that Premera would have “the burden of showing that [the forensic investigator] changed the nature of its investigation at the instruction of outside counsel and that [the forensic investigator’s] scope of work and purpose became different in anticipation of litigation versus the business purpose [the forensic investigator] was performing when it was engaged by Premera before the involvement of outside counsel.”<sup>127</sup> The court held, however, that if there were specific documents or portions of documents relating to the investigator that were prepared for the purpose of communicating with an attorney for the provision of legal advice, those particular documents could be withheld as attorney-client privileged.<sup>128</sup>

~~Other courts have followed suit. For example, in Arby’s, the court held that the attorney-client privilege protected the final and interim analyses of a cybersecurity~~

<sup>124</sup> *Premera I*, 296 F. Supp.3d at 1240–47; *Premera II*, 329 F.R.D. at 662.<sup>124</sup> *Premera I*, 296 F. Supp.3d at 1240–47; *Premera II*, 329 F.R.D. at 662. At least one other court in an analogous situation has applied this logic. In *United States ex. rel. Wollman v. Massachusetts Gen. Hosp., Inc.*, 475 F. Supp. 3d 45, 51 (D. Mass. 2020), the plaintiff alleged that defendants fraudulently billed Medicare and Medicaid for overlapping and concurrent surgeries that required patients to be under anesthesia at the same time. Before the lawsuit, after a surgeon employee challenged the practice, the defendant hired outside counsel to conduct an investigation. The plaintiff moved to compel the report, arguing that defendant hired counsel to conduct a factual investigation. While the court found that the investigation was subject to the attorney-client privilege, the hospital had waived the privilege because it shared the report with a public relations firm to assist the hospital to respond to the Boston Globe’s inquiries into the defendant’s practices. Because the defendant sought advice from the public relations firm, and not outside counsel, the court found that the hospital had waived any attorney-client privilege. ▲

<sup>125</sup> *Premera I*, 296 F. Supp.3d at 1240–47. ▲

<sup>126</sup> *Id.* ▲

<sup>127</sup> *Id.* ▲

<sup>128</sup> *Id.* ▲

Formatted: Font color: Black
Formatted: Font: 10 pt, Font color: Black
Formatted: Font color: Black
Formatted: Font: 10 pt, Font color: Black
Formatted: Font color: Black
Formatted: Font: 10 pt, Font color: Black
Formatted: Font color: Black
Formatted: Font: 10 pt, Font color: Black
Formatted: Font color: Black
Formatted: Normal



~~consultant retained in the wake of the company's consultant's interim and final and interim analyses regarding a cybersecurity incident.~~<sup>129</sup>~~The court reasoned, reasoning that the company had hired the consultant "to produce a report in anticipation of litigation and for other legal purposes," and, therefore, the consultant's analyses were "privileged attorney-client communications between [the consultant] and counsel."~~<sup>130</sup>

~~And in *New Albertson's, Inc. v. MasterCard International*, the court likewise held that certain work that two companies commissioned from a forensic investigator following a cybersecurity breach the companies had suffered was protected by the attorney-client privilege, because the work was done principally for a legal purpose.~~<sup>131</sup>~~The court observed that while one of the companies had initially engaged the investigator directly (not through counsel), that changed when the company learned a new and material fact about the cybersecurity breach.~~<sup>132</sup>~~At that point, the company engaged outside counsel experienced in data breach cases for the purpose of assisting it in conducting an investigation, and the outside counsel then entered into a new engagement with, and began directing the work of, the investigator with knowledge of the likelihood that litigation would result from the security breach.~~<sup>133</sup>~~Both companies then entered into a common interest agreement documenting their common legal interest in connection with the security breach, permitting them to share information with each other without waiving the privilege.~~<sup>134</sup>~~This joint work with the forensic investigator under the direction of outside counsel, the court held, was protected by the attorney-client privilege.~~<sup>135</sup>

~~But, recently, in *Wengui v. Clark Hill, PLC*,~~<sup>136</sup>~~the court granted the plaintiff's motion to compel the defendant, his former law firm, to produce all reports of its forensic investigation into a cyberattack that led to the public dissemination of the plaintiff's~~

<sup>129</sup>. *In re Arby's Restaurant Group, Inc. Data Sec. Litig.*, No. 1:17-cv-00514, at 1-3 (N.D. Ga. Mar. 25, 2019).

<sup>130</sup>. *Id.*<sup>130</sup>. *In re Arby's Restaurant Group, Inc. Data Sec. Litig.*, No. 1:17-cv-00514, at 1-3 (N.D. Ga. Mar. 25, 2019); see also *New Albertson's, Inc. v. MasterCard International* (holding that a forensic investigator's post-breach work was protected by the attorney-client privilege, because the work was done principally for a legal purpose, an observing that, although one company had engaged the investigator directly, not through counsel, the nature of the relationship changed when the company learned a new and material fact about the breach. The company then engaged outside counsel experienced in data breach cases for the purpose of assisting it in conducting an investigation, and the outside counsel then entered into a new engagement with, and began directing the work of, the investigator with knowledge of the likelihood that litigation would result from the security breach.)

<sup>131</sup>. No. 01-17-04410, slip op. at 6 (Idaho 4th Dist. Ct., Ada Cty., May 31, 2019).

<sup>132</sup>. *Id.* at 6-7.

<sup>133</sup>. *Id.*

<sup>134</sup>. *Id.*

<sup>135</sup>. *Id.*

<sup>136</sup>. 338 F.R.D. 7, 10-11 (D. D.C. 2021).

**Formatted:** Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

**Formatted:** Font color: Black

**Formatted:** Normal



confidential information. At the time of the breach, the defendant employed an IT vendor. The defendant retained counsel to represent it in matters related to the breach, and counsel retained a forensic consultant to investigate the breach and defendant's response to it. The forensic consultant undertook a full investigation to determine not only how the attack happened but also how the defendant could strengthen its cybersecurity, and shared information with the company's IT staff and the FBI. Thus, the court rejected the defendant's argument that its counsel retained the forensic consultant primarily for the purpose of obtaining legal advice from its lawyer.

Based upon ~~the Target, Genesco, Premera, Arby's, and New Albertson's~~ these decisions\* discussed above, it appears courts that face attorney-client privilege claims as to post-incident CI will employ the generally applicable principle of focusing on the predominant purpose of the CI in question to make such privilege determinations—that is, whether the documents and communications were created or solicited predominantly for the purpose of aiding to aid the lawyer in providing legal advice, ~~including not and whether such reports are shared only those created by forensic experts, but also by non forensic investigator experts like public relations consultants with counsel, or instead distributed more widely to others both internally and outside the client organization.~~<sup>137</sup>

~~In this regard, courts~~ Courts will also likely look to who retained the service provider as evidence of the purpose of, and hence whether to apply the privilege to, the CI at issue. Courts may be more likely to find a service provider was primarily retained to assist a lawyer in providing legal advice if such provider was retained by counsel, as the Target, New Albertson's, ~~and Genesco~~ and Marriott courts noted that the expert was retained by counsel in making the determination that the CI at issue was privileged. ~~While not noted by~~ In Marriott, for example, the court noted that the specific purpose of IBM's work for which Marriott's counsel retained it was to help Marriott's counsel understand a distinct issue related to the breach, for purposes of advising Marriott as to its legal obligations. As in Arby's, Target, and Genesco, Clark Hill,<sup>138</sup> courts may also look to consider the extent to which the agreement with the expert provided that documents/communications generated as part of the engagement will be kept confidential, provides for confidentiality of materials, and the extent to which the lawyer actually relied upon the report and documents of the provider, and. Moreover, as

<sup>137-137</sup> See, e.g., H.W. Carter & Sons, Inc. v. William Carter Co., No. 95 CIV. 1274, 1995 WL 301351, at \*3 (S.D.N.Y. May 16, 1995) (finding the public relations consultants assisted the lawyers in rendering legal advice, which included how to respond to a lawsuit, and thus information was protected under the Kovel doctrine).

<sup>138</sup> 338 F.R.D. at 10-11 (D. D.C. 2021)

Formatted: Font: Not Italic

Formatted: Don't suppress line numbers

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



specifically highlighted ~~by the court~~ in *New Albertson's*, the courts may also consider the extent to which the lawyer supervised the outside consultant.<sup>139</sup>

#### b. Application of Work-Product Protection to Post-Incident CI

Similarly, courts have already given some indication of whether and when post-incident CI will be protected under the work-product doctrine. As noted above, the discussion of whether the predominant purpose of a document or communication was to provide or obtain legal advice often melds into the discussion of whether a document or communication was created because of anticipated litigation, as these analyses are similar. The court often will rely on both the privilege and work-product protection, or find that neither applies, as discussed below.

##### i. Because of Anticipated Litigation

Courts dealing with work-product protection claims that are made as to post-incident CI have examined carefully whether the post-incident CI in question was created “because of” anticipated litigation, as is required for work-product protection. When a document may be used for both litigation and business purposes, courts must determine “the driving force behind the preparation of” the requested document.<sup>140</sup> For example, the *Target* court found that communications from Target’s CEO to the Board of Directors did not qualify for work-product protection because nothing showed that the update to the Board was made *because of* any anticipated litigation.<sup>141</sup> However, as described in detail in Section 4 below, with respect to the application of the attorney-client privilege in that case, the court found that the documents created by and communications with the data-breach task force were protected by the work-product doctrine.<sup>142</sup> The court found those documents were created to “prepare to defend the company in litigation that was already pending and was reasonably expected to follow.”<sup>143</sup>

<sup>139-139</sup> Contrarily, however, the court in *Premiera I* used the fact that the attorney hired the public relations firm as evidence that the firm was not acting as the company’s in-house public relations firm (entitling it to step into the shoes of the corporation vis-à-vis counsel), but rather was outside of that relationship and was advising both the company and counsel separately. *Premiera I*, 296 F. Supp.3d 1230 (D. Or. 2017).

<sup>140</sup> *In re Capital One Consumer Data Sec. Breach Litig.*, 2020 WL 3470261 (E.D. Va. June 25, 2020), citing *Nat’l Union Fire Ins. Co. of Pittsburgh, Pa. v. Murray Sheet Metal Co.*, 967 F. 2d 980, 984 (4th Cir. 1992).

<sup>141-141</sup> *In re Target Corp. Customer Data Security Breach Litig.*, MDL No. 14-2522 (PAM/JJK), 2015 WL 6777384, at \*3 (D. Minn. Oct. 23, 2015)-23, 2015); see also *In re Dominion Dental Servs. USA, Inc. Data Breach Litig.*, 429 F. Supp. 3d 190, (E.D. Va. 2015), citing *Nat’l Union Fire Ins. Co.*, 967 F. 2d at 984.

<sup>142-142</sup> *Id.*

<sup>143-143</sup> *Id.*

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Outline numbered + Level: 1 + Numbering Style: i, ii, iii, ... + Start at: 1 + Alignment: Right + Aligned at: 0.75" + Indent at: 1", Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



~~A California federal court has similarly~~ Several courts have examined whether post-incident CI ~~was~~ reports were prepared “because of” anticipated litigation. For example, in *In re Experian Data Breach Litigation*,<sup>144</sup> the court found that the question is whether the totality of the circumstances suggests that the document “was created because of anticipated litigation, and would not have been created in substantially similar form but for the prospect of that litigation.”<sup>145</sup> The court examined whether a report drafted by an outside forensic investigator was drafted “because of” anticipated litigation, focusing on whether the report was more relevant to the internal investigation and remediation of the incident, or to the defense of the litigation.<sup>146</sup> In making its determination, the court relied in part on the fact that the full report was shared only with the legal team (as opposed to the entire incident response team).<sup>147</sup> The court reasoned that the report would have been given in full to the incident response team if it “was more relevant to Experian’s internal investigation or remediation efforts, as opposed to being relevant to defense of this litigation.”<sup>148</sup>

The court in *In re Rutter’s Data Sec. Breach Litig.* distinguished the ruling in *Experian*, finding that the work-product doctrine did not preclude production of a forensic report because 1) the forensic report was first provided to the defendant when it was completed, and there was no evidence it was first provided to counsel, 2) the forensic company was to work alongside the defendant’s IT personnel to identify and remediate any potential vulnerabilities, whereas in *Experian*, the report’s legal nature was supported by declarations, and 3) unlike the declarations in *Experian*, the defendant’s corporate designee testified that he was unaware of anyone at the defendant who contemplated a lawsuit when the forensic report was compiled.<sup>149</sup>

In *Genesco*, the court also examined whether documents created by and communications with third-party experts were protected by the work-product doctrine.<sup>150</sup> Citing *United States v. Nobles*, the court found this post-incident CI squarely

<sup>144</sup> See Order Denying Motion to Compel Production of Documents, *In re Experian Data Breach Litigation*, No. SACV 15-01592 AG (DFMx) (C.D. Cal. May 18, 2017).

<sup>145</sup> *Id.* at 2 (quoting *In re Grand Jury Subpoena* (Mark Torf/Torf Envtl. Mgmt.), 357 F.3d 900, 907 (9th Cir. 2004)).

<sup>146</sup> *Id.* at 3–4.

<sup>147</sup> *Id.*

<sup>148</sup> *Id.*

<sup>149</sup> No. 1:20-CV-382, 2021 WL 3733137, at \*3 (M.D. Pa. July 22, 2021).

<sup>150</sup> *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 190–91 (M.D. Tenn. 2014); *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 190–91 (M.D. Tenn. 2014).

Formatted: Indent: First line: 0", Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

Formatted: Font color: Black

Formatted: Normal



within the doctrine because the investigator was counsel's agent and was working under counsel's direction to prepare for litigation.<sup>151 152</sup>

~~Likewise~~ Similarly, in *Arby's*, the court found that a third-party consultant's post-incident final and interim analyses of a data breach were subject to the work-product protection because the consultant was hired "in anticipation of litigation."<sup>153</sup>

~~And in~~ *New Albertson's*, the court held that certain applied the work product doctrine to work that two companies commissioned from a forensic investigator following a cybersecurity breach ~~the companies had suffered was subject to the work-product protection~~.<sup>154</sup> The court observed that while one of the companies had initially engaged the investigator directly ~~(not through counsel), that changed,~~ when the company learned a new and material fact about the cybersecurity breach.<sup>155</sup> ~~At that point, the company, it~~ engaged outside counsel experienced in data breach cases for the purpose of assisting it in conducting an investigation, and the outside counsel counsel. Counsel then entered into a new engagement with, and began directing directed the work of, the investigator with knowledge of the likelihood, knowing that it was likely that litigation would result from the security breach.<sup>156</sup> Both companies then entered into a common interest agreement documenting their common legal interest in connection with the security breach, permitting that permitted them to share information with each other without waiving the privilege.<sup>157</sup> This joint work with the forensic investigator under the direction of outside counsel, the court held, was subject to the work-product protection.<sup>158</sup>

In *Premiera I*, the court stated that if the CI at issue (drafts and CI created by employees and third parties following the breach, including press releases, notices, etc.) had a dual purpose, that CI would be protected by the work-product doctrine if the CI was created "because of" the prospect of litigation.<sup>159</sup> The court rejected the notion that the CI at issue

<sup>151-151</sup> *Id.* at 191.

<sup>152</sup> See also Order, *In re Arby's Restaurant Group, Inc. Data Sec. Litig.*, No. 1:17-cv-00514, at 2-3 (N.D. Ga. Mar. 25, 2019) (court likewise found that a third-party consultant's post-incident final and interim and final analyses of a data breach were subject to the work-product protection because the consultant was hired "in anticipation of litigation.").

<sup>153</sup> Order, *In re Arby's Restaurant Group, Inc. Data Sec. Litig.*, No. 1:17 cv 00514, at 2-3 (N.D. Ga. Mar. 25, 2019).

<sup>154-154</sup> *New Albertson's, Inc. v. MasterCard Int'l*, No. 01-17-04410, slip op. at 6 (Idaho 4th Dist. Ct., Ada Cty., May 31, 2019).

<sup>155</sup> *Id.* at 6-7.

<sup>156-156</sup> *Id.*

<sup>157-157</sup> *Id.*

<sup>158-158</sup> *Id.*

<sup>159-159</sup> *Premiera I*, 296 F. Supp.3d 1230, 1240-47 (D. Or. 2017).

Formatted: Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



was necessarily created because of litigation, rather than for business reasons, simply because the business functions at issue were directed by attorneys.<sup>160</sup> Rather, the court held that in order to establish that a particular document is subject to work-product protection, Premera must show that the document was prepared specifically because of anticipated litigation.<sup>161</sup> Likewise, with respect to the third-party investigator, the court relied on the fact that the investigator had not changed its scope or purpose at the direction of outside counsel in finding that Premera had not yet established that the CI relating to the investigator was created because of the anticipated litigation.<sup>162</sup> However, the court noted that if there were specific documents relating to the investigator that were created because of anticipated litigation, Premera could properly withhold them as subject to the work-product protection.

In *Premera II*, the court held that narratives drafted to help prepare responses to regulatory inquiries were entitled to work-product protection insofar as they were prepared for the regulatory inquiry and not a general business purpose.<sup>163</sup> It also held that draft notices and scripts prepared by counsel because of anticipated litigation were protected.<sup>164</sup> However, it stated that a timeline prepared by in-house counsel relating to remediation would not be protected if Premera did not demonstrate that the timeline would have been prepared in substantially different format absent anticipated litigation or regulatory investigations.<sup>165</sup>

In *In re Dominion Dental Servs. USA, Inc. Data Breach Litigation*, 429 F. Supp. 3d 190 (E.D. Va. 2019), the court granted plaintiff's motion to compel a post-breach report that Mandiant, the defendant's third-party cybersecurity vendor, prepared. The court rejected the defendant's argument that Mandiant prepared the report in anticipation of litigation, citing Mandiant's pre-breach relationship with the defendant. The court observed that Mandiant's 2019 post-breach statement of work, which included computer incident response support, digital forensics support, advanced threat actor support, and advanced threat/incident assistance was "almost identical to the services promised in the June 2018 statement of work," into which Mandiant and the defendant had entered months before any threat of litigation."<sup>166</sup> Mandiant had merely added the words "under the direction of Counsel" to the 2019 statement of work, which, as the court observed,

<sup>160</sup> *Id.*

<sup>161</sup> *Id.*

<sup>162</sup> *Id.*

<sup>163</sup> *Premera II*, 329 F.R.D. 656, 666 (D. Or. 2019).

<sup>164</sup> *Id.* at 664.

<sup>165</sup> *Id.* at 665.

<sup>166</sup> 429 F. Supp. 3d at 194.

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



appeared “to be designed to help shield material from disclosure rather than to fundamentally alter the business purposes of the work.”<sup>167</sup> Moreover, the defendant had touted its retention of Mandiant for “non-litigation purposes” such as reassuring customers that it had engaged Mandiant as a “world leading cyber security firm.”<sup>168</sup>

In *In re Capital One Consumer Data Sec. Breach Litig.*,<sup>169</sup> the court found that, although at the time Capital One retained its forensic consultant for incident response services, there was a “very real potential” that Capital One would face substantial claims related to a data breach that affected millions of consumers, Capital One failed to establish that its consultant would not have prepared the report in substantially similar form “but for the prospect of litigation.”<sup>170</sup> As in *Dominion Dental*, Capital One’s relationship with the consultant predated the breach. The Capital One court reviewed the consultant’s scope of services covered set forth in its engagement agreement with Capital One’s counsel, and the scope of work in an earlier agreement between Capital One and the consultant, noting that the primary difference between the two was a specific reference in the later agreement to counsel’s role. Accordingly, the court noted that, absent outside counsel’s involvement, there was “no difference” between what the consultant produced and what it would have produced in the ordinary course of business.<sup>171</sup>

The pre-breach existence of a relationship between the party exposed to the data breach and the forensic investigator appears to be the lynchpin of the courts’ reasoning. In *Capital One*, months after the court compelled Capital One to produce its consultants’ report, the court denied three other motions from plaintiffs to compel production of a root cause analysis report that PricewaterhouseCoopers (“PWC”) prepared for Capital One. A major difference between PWC’s role in the investigation and that of Capital One’s forensic consultant appears to be timing. Capital One had retained PWC post-breach as a consulting expert to conduct the root cause analysis of the breach. PWC’s statement of work provided that its analysis was intended “to assist Capital One’s Legal Department ... with its provision of legal advice to the Board and the Risk Committee and in anticipation of litigation.”

Similarly, in *Maldonado v. Solara Medical Supplies, LLC*, No. 1:20-CV-12198, after a data breach involving a medical device supplier, the supplier immediately engaged counsel to begin preparing for lawsuits. The supplier’s counsel hired Charles River Associates, Ltd. to perform a privileged forensic investigation into the event to assist the attorneys in providing legal advice to the supplier. CRA did not provide a report, but

---

<sup>167</sup> . *Id.*

<sup>168</sup> . *Id.*

<sup>169</sup> . 2020 WL 2731238 (E.D. Va. May 26, 2020).

<sup>170</sup> . *Id.*

<sup>171</sup> . *Id.*



communicated findings periodically through the investigation to the supplier and its counsel. The plaintiff served a subpoena duces tecum on CRA for documents related to its investigation. The court quashed the subpoena on work product grounds, distinguished Dominion Dental, noting the absence of a “previous relationship” between CRA and Solara. The court also observed that, given the complex litigation and regulatory issues resulting from a data breach, “particularly where individuals’ personal medical data is involved,” one “cannot imagine an attorney providing advice to a company ... without having a technical expert assist the attorney in investigating the facts.” Accordingly, given that counsel retained CRA, post-breach, to “assist counsel in advising Solara,” the court held the materials generated by the investigation to be privileged under both work product and attorney-client privilege.

Whether post-incident CI is protected by the work-product doctrine may also include an examination of when the documents or information were generated. Often, internal IT or security teams may create documents and engage in communications while trying to determine whether a breach occurred. If no lawyer is engaged in these communications or consulted and no regulatory investigation or litigation has been contemplated up to that point, courts may be less likely to find that these early documents were created in anticipation of litigation. If a company is contemplating that a security incident may result in an investigation or litigation, and has open lines of communication between first-line responders on the IT or security team and the relevant in-house or external counsel in connection with that contemplated investigation or litigation, the work-product protection is more likely to apply.

In *In re Rutter’s Data Sec. Breach Litig.*,<sup>172</sup> when it found that the work-product doctrine did not shield a forensic consultant’s report because it was not prepared for litigation purposes, the court focused primarily on the timing of the consultant’s retention and its scope of work. The consultant’s scope of work described its services as relating to determining whether unauthorized activity within the Rutter’s systems environment resulted in the compromise of sensitive data, and if so, the extent of the compromise.<sup>173</sup> The court determined that the language demonstrated that the defendant “did not have a unilateral belief that litigation would result at the time it requested” the consultant prepare a report.<sup>174</sup> Put another way, “without knowing whether or not a data breach occurred, Defendant [could not] be said to have unilaterally believed that litigation would result.”<sup>175</sup> Moreover, the defendant’s corporate representative testified that he was

<sup>172</sup> . 2021 WL 3733137 (M.D. Pa. July 22, 2021)

<sup>173</sup> . *Id.* at \*2.

<sup>174</sup> . *Id.*

<sup>175</sup> . *Id.*

Formatted: Don't suppress line numbers

Formatted: Normal



unaware of anyone contemplating a lawsuit at the time the consultant prepared its report.<sup>176</sup>

A court's determination regarding whether litigation was reasonably anticipated may rely either on language directly in a retainer agreement (as in *Genesco*)<sup>177</sup> or on the fact that litigation, though not yet commenced, has at least been threatened. Courts will also consider whether, regardless of the language stated in the retainer agreement (as in *Clark Hill*)<sup>178</sup> the forensic consultant's services exceeded the scope of preparing a report in anticipation of litigation. Courts may also rely on the issuance of a litigation hold, the retention of outside counsel, or documentation that litigation or an investigation may be forthcoming.<sup>179</sup>

Analogous case law—such as the line of decisions concerning how the work-product protection's "anticipation of litigation" requirement applies to a situation in which a company suspects a defect in its product and investigates the defect, its scope, and remedial action—further underscores that courts likely will carefully distinguish between documents prepared because of anticipated litigation and documents prepared for business purposes. For example, in *Adams v. Gateway, Inc.*, concerns about problems with its computers led Gateway to launch an internal investigation headed by an attorney and labeled a "legal investigation."<sup>180</sup> The attorney interfaced with engineers and other technical personnel as part of the investigation, and Gateway attempted to claim that several of the documents related to the investigation were work-product protected on that basis.<sup>181</sup> The court disagreed, finding that while Gateway may have become aware of product performance issues as a result of a litigation, "the investigation had at its core the diagnosis and resolution of potential problems" and was motivated by "Gateway's

<sup>176</sup> . *Id.*

<sup>177</sup> . *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 181 (M.D. Tenn. 2014). The retention agreement with the forensic investigator specifically stated that the investigator was being retained "in anticipation of potential litigation and/or legal or regulatory proceedings" and to assist its attorneys in preparing for such litigation and providing legal advice. *Id.*

<sup>178</sup> . *Clark Hill*, 338 F.R.D. at 13 (noting that, although the engagement letters "state that Clark Hill hired MPG in anticipation of litigation and that, on the same day, MPG in turn retained Duff & Phelps, Duff & Phelps's role seems to have been far broader than merely assisting outside counsel in preparation for litigation.") (emphasis in original); see also *Capital One, CITE* (finding that PWC performed its root cause analysis in anticipation of litigation).

<sup>179</sup> . Companies should carefully consider when to issue a litigation hold and ensure that the litigation hold, once issued, is being complied with. The issuance of a litigation hold may have the unintended consequence of triggering notification requirements in some jurisdictions.

<sup>180</sup> . See Order Granting Motion to Compel, *Adams et al. v. Gateway*, 2:02-cv-00106, 2003 WL 23787856, at \*3 (D. Utah Dec. 30, 2003), ECF No. 136 [hereinafter *Adams Order*].

<sup>181</sup> . *Id.* at \*5-6.

Formatted: Don't suppress line numbers

Formatted: Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

Formatted: Font: 10 pt, Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



self-interest as a retailer of computer products.”<sup>182</sup> In determining whether specific documents were work-product protected, the court found some of the documents showed “concrete litigation-related preparation” and attorney instructions, whereas others showed “technical efforts and results,” not revealing or responsive to litigation concerns.<sup>183</sup> Thus, the court ordered the production of the latter documents.<sup>184</sup>

Other case law evaluating whether an internal investigation or an internal audit qualifies for work-product protection indicates that courts are not likely to find post-incident CI work-product protected merely because counsel involved in a litigation generated or received the CI in question.<sup>185</sup> This may be more true to the extent it involves

<sup>182</sup>,<sup>182</sup> *Id.* at \*4.

<sup>183</sup>,<sup>183</sup> *Id.* at \*17.

<sup>184</sup>,<sup>184</sup> *Id.* at \*34, \*38. Similarly, in *Janicker by Janicker v. George Washington Univ.*, the District Court of Washington, D.C., found that “[i]f in connection with an accident or an event, a business entity in the ordinary course of business conducts an investigation for its own purposes, the resulting investigative report is producible in civil pretrial discovery.” 94 F.R.D. 648, 650 (D.D.C. 1982). The court found that the report was “prepared in the ordinary course of business with the primary motivation being to determine what steps could be taken to prevent any repetition of such a tragedy to protect other resident college students and the University’s standing in the college community and in recruiting students to attend the institution in the future.” *Id.* For additional examples in the defective products’ context, see, e.g., *Soeder v. Gen. Dynamic Corp.*, 90 F.R.D. 253, 255 (D. Nev. 1980) (granting plaintiffs’ motion to compel in-house report regarding aircraft accident on grounds that “given the equally reasonable desire of Defendant to improve its aircraft products, to protect future pilots and passengers of its aircraft, to guard against adverse publicity in connection with such aircraft crashes, and to promote its own economic interests by improving its prospect for future contracts for the production of said aircraft, it can hardly be said that Defendant’s ‘in-house’ report is not prepared in the ordinary course of business”); *Bradley v. Melroe Co.*, 141 F.R.D. 1 (D.D.C. 1992) (ordering production of files related to incidents involving product); *Scott Paper Co. v. Ceilcote Co., Inc.*, 103 F.R.D. 591, 595–96 (D. Me. 1984) (recognizing the “important but subtle distinction between reports prepared in response to an unfortunate event, that might well lead to litigation, and materials prepared as an aid to litigation” and finding that documents had business purpose of maintaining relationship with plaintiff and avoiding litigation).

<sup>185</sup>,<sup>185</sup> *In re Air Crash Disaster at Sioux City*, 133 F.R.D. 515, 520 (N.D. Ill. 1990) (documents not work-product protected just “because the ultimate findings of the employees will be conveyed to the attorneys who are in charge of the litigation”); *In re Kidder Peabody Sec. Litig.*, 168 F.R.D. 459, 465–66 (S.D.N.Y. 1996) (investigation conducted by outside counsel not protected work product because the investigation would have been undertaken even if litigation had not been filed against the company, noting the situation was “not only with a serious legal problem, but with a major business crisis” and “litigation was not the ‘principal,’ or dominant, motivator, but rather was, at most, an inducement equivalent in importance to the business necessities that we have already cited”); see also *In re OM Sec. Litig.*, 226 F.R.D. 579, 586–87 (N.D. Ohio 2005) (holding that although company correctly anticipated litigation, documents prepared by audit committee and its consultant were not protected work product because investigation would have been conducted regardless of litigation).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



in-house counsel, as opposed to outside counsel.<sup>186</sup> Courts may be more likely to afford work-product protection to an internal investigation with a dual purpose if the litigation purpose is clear from the particular documents at issue, such as the legal ramifications of the investigation's findings.<sup>187</sup>

Given the case law in both the CI and non-CI scenarios, courts seem likely to scrutinize closely whether CI claimed to be work-product protected was in fact prepared in anticipation of litigation. Such scrutiny may include an examination as to whether counsel had a significant enough role in the preparation of a document as to suggest that it was created "because of" and/or for the "primary purpose of" aiding litigation, and/or whether it would not have been prepared in substantially the same form but for the litigation. If portions of such CI were created in anticipation of litigation and others were not, segregation of these portions may also affect a court's decision.<sup>188</sup>

## ii. Substantial Need

As discussed in Part B, work-product protection is not absolute, and courts may order documents and information covered by the work-product protection produced if the requesting party can show a substantial need for the information. The court in the *Target* case specifically addressed whether the work-product protection could be overcome by the "substantial need" exception, but found that plaintiffs did not have a substantial need to discover the work product being withheld because Target had "produced documents and other tangible things, including forensic images, from which Plaintiffs can learn how the data breach occurred and about Target's response to the breach."<sup>189</sup>

The court also addressed the substantial-need issue in *Experian*. In that case, plaintiffs argued that Experian's third-party expert had access to live servers that plaintiffs did not

<sup>186-186</sup> See *United States v. ChevronTexaco Corp.*, 241 F. Supp. 2d 1065, 1076 (N.D. Cal. 2002) ("[U]nlike outside counsel, in-house attorneys can serve multiple functions within the corporation. In-house counsel may be involved intimately in the corporation's day to day business activities and frequently serve as integral players in business decisions or activities.")

<sup>187-187</sup> See, e.g., *Adams Order*, 2003 WL 23787856, at \*21 (D. Utah Dec. 30, 2003) (concluding that email from in-house counsel "noting legal implications" of investigation of product deficiencies qualified as work-product protected); *Hallmark Cards, Inc. v. Murley*, No. 09-377-CV-W-GAF, 2010 WL 4608678, at \*4 (W. Dist. Mo. Nov. 9, 2010) (work-product protection extended to documents created by outside counsel and forensic expert it retained to assess concern that third party had provided client with information misappropriated from former employer).

<sup>188-188</sup> This may also have unintended consequences of making some portions of the document less likely to be protected by the work-product doctrine but should not impact the attachment of the attorney-client privilege.

<sup>189-189</sup> *In re Target Corporation Customer Data Security Breach Litigation*, 2015 WL 6777384 at \*3 (D. Minn. Oct. 23, 2015).

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



have access to, and therefore plaintiffs had a substantial need to access the work-product protected information.<sup>190</sup> Because Experian refuted that claim and plaintiffs could “get those exact server images and hire their own expert to perform the work,” plaintiffs did not meet the substantial-need exception to the work-product protection.<sup>191</sup>

Similarly, the court in *Arby's* rejected plaintiffs’ attempt to obtain post-incident CI of a forensic consultant that the court deemed subject to the work-product protection.<sup>192</sup> Although it did not explicitly address the “substantial need” exception by name, the court appears to have implicitly ruled that plaintiffs did not meet the exception, because the court reasoned that the “[p]laintiffs have not shown that [the consultant’s] analyses cannot be duplicated should [the plaintiffs] be provided the underlying information used by” the consultant.<sup>193</sup> The court therefore ordered the defendant to provide plaintiffs “with the underlying information used by” the consultant in its investigation.<sup>194</sup>

In *New Albertson's*, the court held that the opposing party failed to demonstrate a substantial need for the ~~work product of the breached companies’ investigator~~investigator’s work because the opposing party’s own investigator had ~~already~~been provided with ~~all of~~ the same data and system access that the breached companies’ investigator had.<sup>195</sup> ~~Not~~There was ~~there any~~also no indication that the breached companies were using the work-product protection to shield facts about the breach from being discovered.<sup>196</sup>

However, in *In re Ambry Genetics Data Breach Litigation*, the court denied without prejudice the defendants’ attempt to strike allegations in a complaint that the defendants asserted were attorney work product because the allegations contained analyses from two post-breach forensic reports that defendants voluntarily produced to plaintiffs while negotiating search terms.<sup>197</sup> Despite the defendants’ claim that they preserved their work product objection when producing the reports, the court noted that it “does not have enough information to determine if the reports at issue, or the specific portions [the

<sup>190-190</sup> Order Denying Motion to Compel Production of Documents at 5, *In re Experian Data Breach Litigation*, No. SACV 15-01592 AG (DFMx), (C.D. Cal. May 18, 2017).

<sup>191-191</sup> *Id.*

<sup>192-192</sup> Order, *In re Arby's Restaurant Group, Inc. Data Sec. Litig.*, No. 1:17-cv-00514, at 2–3 (N.D. Ga. Mar. 25, 2019).

<sup>193-193</sup> *Id.*

<sup>194-194</sup> *Id.*

<sup>195-195</sup> *New Albertson's, Inc. v. MasterCard Int'l*, No. 17-04410, slip op. at 8–9 (Idaho 4th Dist. Ct., Ada Cty., May 31, 2019).

<sup>196-196</sup> *Id.* at 10–11.

<sup>197</sup> No. SACV 20-00791 CJC (KESx), 2021 WL 4860514, at \*2-3 (C.D. Cal. July 30, 2021).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



plaintiffs] cite and quote in their [complaint], are subject to work product protection," because it did not have the forensic reports themselves. The court went on to state that "it appears likely that the [forensic reports] do not contain opinion work product. Even if the documents were prepared in anticipation of litigation, without opinion work product, they would be subject to discovery if Plaintiffs show that they have a substantial need for the materials to prepare their case and cannot, without undue hardship, obtain their substantial equivalent by other means. Fed. R. Civ. P. 26(b)(3)(A). This seems to be a standard Plaintiffs could meet. It is also possible that [the defendant] would have obtained reports showing the cause and severity of the data breach even without the anticipation of litigation."<sup>198</sup> When defendants then failed to provide the court with either the forensic reports or evidence showing the material should be kept under seal, the Court ordered Plaintiffs to publicly file an unredacted version of their complaint revealing the challenged information.<sup>199</sup>

In Facebook, while the appellate court found that Facebook's ADI was created in anticipation of litigation and therefore work product, the appellate court held that the Attorney General had demonstrated a "substantial need" for the information, and that there was no other source from which the Attorney General could obtain the information without "undue hardship." The appellate court also noted that it could not conclude that none of Facebook's information fell into the category of "opinion" work product. It remanded the matter to the trial court to determine what, if any, information constituted fact work product as opposed to opinion work product.

Finally, in Solara Medical Supplies,<sup>200</sup> the court found that the work product shielded the information yielded from the forensic investigation, and that plaintiffs had failed to meet their burden of demonstrating a substantial need for the materials, or that they could not obtain a substantial equivalent without undue hardship. In its analysis, the court focused on Solara's retention as an expert of a former CRA employee who conducted a separate investigation. Solara had not objected to that expert's materials or the underlying facts being disclosed to the plaintiffs: "Hart's reports and the data he reviewed or on which he relied have been produced to plaintiffs, and those materials 'demonstrate that the underlying facts are available to plaintiffs without any need to 'invade' privileged materials.'"

These cases indicate that courts likely will not find the substantial-need exception to work-product protection applicable to post-incident CI unless the party seeking to apply the exception can prove that it lacks sufficient information regarding the breach, the

<sup>198</sup> . *Id.*

<sup>200</sup> . No. 1:20-CV-12198 (D. Mass. June 2, 2021).

Formatted: Don't suppress line numbers

Formatted: Normal



investigation, and/or the response to the breach to recreate on its own the work product reflected in the CI in question.

### c. Application of Non-Testifying Expert Privilege to Post-Incident CI

In Marriott, the plaintiff moved to compel documents that CrowdStrike generated when Marriott's counsel hired it to help it respond to a data breach. The special magistrate appointed for discovery deferred discovery from CrowdStrike until Marriott indicated whether it intended to designate CrowdStrike as an expert witness, subject to the Federal Rules of Civil Procedure.<sup>201</sup> When Marriott determined that it would not designate CrowdStrike as an expert, the special magistrate ruled that Marriott had hired CrowdStrike in anticipation of litigation, and that the plaintiffs were not entitled to ascertain the facts known to, or opinions held by, Crowdstrike, unless the plaintiffs demonstrated exceptional circumstances that made it impracticable for them to obtain the facts by any other means. The magistrate's willingness to wait to determine privilege until Marriott determined whether CrowdStrike would serve as an expert illustrates that reliance on the non-testifying expert privilege may avoid the need for a court to conduct a document-by-document analysis of the reasons for generating particular material.<sup>202</sup>

### 3. Waiver of Attorney-Client Privilege and Work-Product Protection as to CI

Even if a court finds that the attorney-client privilege and/or work-product protection applies to certain CI, it may determine that the company has waived the privilege or protection as to that CI. This could be because the company disclosed the CI to a third party—which could include disclosure to: (1) a regulator (the FTC, the SEC, state attorneys' general, the Office for Civil Rights of the Department of Health and Human Services, etc.) pursuant to statute, an investigative demand, or voluntarily; (2) contract parties whose data or systems may have been impacted during an incident; (3) law enforcement to assist in the investigation seeking to apprehend the criminal attacker; (4) an information-sharing organization; (5) an insurance carrier; (6) an affiliated entity; or

<sup>201</sup> In re Marriott International, Inc. Customer Data Security Breach Litigation, MDL No. 19-MD-2879 (July 12, 2021).

<sup>202</sup> . See also Maldonado v. Solara Medical Supplies, LLC, et al., No. 1:20-CV-12198-LTS (D. Mass. June 2, 2021) (“Solara does not dispute that plaintiffs should receive the reports produced by Hart, and all the data he relied on in writing those reports. Further, Solara has named Hart as a retained expert in this case and plaintiffs have access to his expert report and discovery concerning it.”)

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Normal



(7) other parties involved in the same or similar litigation. A court could even potentially find waiver because company personnel disclosed the CI to others within the company.<sup>203</sup>

a. Disclosures to Direct or Indirect Contract Parties

In *Genesco*, the court relied on *In re TJX Cos. Retail Sec. Breach Litig.*<sup>204</sup> in determining that the company's disclosure of brief portions of the counsel-retained forensic expert's report to Visa and the assistance of the forensic expert in creating an annotated response to Visa's forensic report did not constitute a waiver of the attorney-client privilege and work-product protection because the sections of the report containing the privileged information were not disclosed to Visa or any other third parties.<sup>205</sup> And in *Premiera II*, the court suggested that whether disclosure of a document to a third-party vendor created a waiver would depend on whether the vendor is providing a "legal" as opposed to "business" service.<sup>206</sup> While neither *Genesco*, *TJX*, nor *Premiera II* clearly distinguished between the test for waiver of the attorney-client privilege and the test for waiver of the work-product doctrine, these tests are in fact very different, with the attorney-client privilege generally being much more readily subject to waiver.<sup>207</sup> That being the case, there may be circumstances in which disclosure of CI to one person will waive the attorney-client privilege, but not the work-product protection, as to that CI in regard to other persons.

b. Disclosures to Internal Company Employees

One example of a situation where such differing results could arise is the disclosure of an attorney-client privileged and work-product protected forensic report, cybersecurity assessment, or other CI to internal company employees. While such a disclosure would *not* result in a waiver of the work-product protection unless a court were to somehow conclude that the employee recipient was likely to turn the report over to an adversary, the disclosure might result in waiver of the attorney-client privilege if

<sup>203-203</sup> The Federal Rules of Evidence provide that a federal court may order that disclosure of privileged or protected information in connection with federal court litigation does not constitute a waiver. FED. R. EVID. 502(d). In that event, the privilege or protection is also preserved in other federal or state proceedings. *Id.* However, this provision would not protect CI disclosed outside of or before a federal proceeding has been instituted. *Id.* Accordingly, it would not apply to disclosures outside of litigation to regulators, contract parties, law enforcement, information sharing organizations, insurance carriers, or other third parties.

<sup>204-204</sup> 246 F.R.D. 389 (D. Mass. 2007).

<sup>205-205</sup> *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168 (M.D. Tenn. 2014).<sup>205</sup> *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168 (M.D. Tenn. 2014).

<sup>206-206</sup> *Premiera II*, 329 F.R.D. 656, 668 (D. Or. 2019).

<sup>207-207</sup> See Part B.3 *supra*.

**Formatted:** Outline numbered + Level: 1 + Numbering  
Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned  
at: 0.5" + Indent at: 0.75", Don't suppress line  
numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Normal, Justified, Space Before: 3 pt,  
Border: Top: (No border), Bottom: (No border), Left: (No  
border), Right: (No border), Between : (No border), Tab  
stops: 0.25", Right + 0.38", Left

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Normal



the employee recipients did not “need to know” the information in the CI (e.g., where there was no need for the employee to provide feedback to the attorney on the report to facilitate the attorney’s legal advice)<sup>208</sup> and/or the recipient employees were outside of the company’s “control group.”<sup>209</sup> Under either test, courts will likely scrutinize the employee recipients to determine whether their receipt of, for instance, an attorney-client privileged data-breach forensic report results in waiver of the privilege. For example, though an IT analyst may rank far lower on the company hierarchy than a vice president of sales, the IT analyst’s role and knowledge may be critical for enabling the company’s attorneys to provide legal advice. If so, sharing the forensic report with the IT analyst is unlikely to waive the attorney-client privilege under the widely used subject-matter test. However, insofar as the IT analyst is not considered part of the company’s control group, sharing the report may waive the privilege in a control-group jurisdiction like Illinois.

### c. Disclosures to Law Enforcement

Courts may also eventually need to determine whether, when, and to what extent, protected CI loses its protection by reason of being disclosed to law enforcement in connection with its investigation seeking to apprehend the perpetrator of the incident or to a regulator during its investigation of the breached entity’s possible role in the incident. As noted in Part B above, at least one court has held that a “selective waiver” theory may protect a party who discloses information to a governmental entity from losing the attorney-client privilege or work-product protection as to that information as against other entities.<sup>210</sup> However, many courts have rejected this theory, despite the public policy benefits of such a position.<sup>211</sup> Some courts have found that disclosure of information to law enforcement or regulators does not waive otherwise applicable attorney-client and

<sup>208-208</sup> As the court noted in *Verschoth v. Time Warner, Inc.*, 2001 WL 286763 at \*2 (S.D.N.Y. Mar. 22, 2001), the need to know “must be analyzed from two perspectives: (1) the role in the corporation of the employee or agent who receives the communication; and (2) the nature of the communication, that is, whether it necessarily incorporates legal advice. To the extent that the recipient of the information is a policymaker generally or is responsible for the specific subject matter at issue in a way that depends upon legal advice, then the communication is more likely privileged.”

<sup>209-209</sup> See Part B.3 *supra*.

<sup>210-210</sup> See, e.g., *Diversified Indus. v. Meredith*, 572 F.2d 596, 611 (8th Cir. 1977); *In re McKesson HBOC, Inc. Secs. Litig.*, 2005 U.S. Dist. LEXIS 7098, \*47 (N.D. Cal. Mar. 31, 2005).

<sup>211-211</sup> *In re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289, 307 (6th Cir. 2002) (finding that a party’s voluntary disclosure of protected documents to the SEC, even under a confidentiality agreement, constituted a complete waiver of attorney-client and work-product privilege); see also *Westinghouse Elec. Corp. v. Republic of Phil.*, 951 F.2d 1414, 1429 (3d Cir. 1991) (determining party’s “disclosure of work product to the SEC and to the DOJ waived the work-product doctrine as against all other adversaries” notwithstanding if there was or was not a finding that there was a confidentiality agreement party entered into with government agencies).

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



work-product protections, provided that the company entered into a confidentiality or protective order containing appropriate non-waiver and other provisions.<sup>212</sup> Thus, while doing so may not necessarily prevent waiver, depending on the court at issue and the circumstances of the disclosure, requiring non-waiver and confidentiality provisions or agreements as a condition to any disclosure of CI to the government may at least increase the likelihood that a court will not find that such disclosure waived, as against other persons, any attorney-client privilege and/or work-product protection to which the disclosed CI might otherwise have been entitled.

#### d. Disclosures to Information Sharing Organizations

Information sharing of certain aspects of an incident or other vulnerabilities may also be protected via the Cybersecurity Information Sharing Act (CISA) of 2015. CISA provides protections to encourage sharing cyber threat indicators and defensive measures with the federal government, state and local governments, and other companies and private entities. Relevant here, CISA provides that the sharing of information pursuant to CISA does not waive as to other persons any attorney-client privilege or work-product protection to which the information may have been entitled and also protects information shared from Freedom of Information Act (FOIA) disclosure.<sup>213</sup>

#### e. Common Interest, Joint Defense, and Joint Representation Arguments Against Waiver

Whether the sharing of CI with insurance providers, third parties whose systems or data may be involved in the incident, and/or affiliated entities waives any attorney-client privilege or work-product protection that may otherwise have applied to such CI as against other persons may revolve around a court's determination as to whether the parties have a common interest. If the CI in question otherwise qualifies for protection under the attorney-client privilege or work-product doctrine, courts will typically find that a party sharing information with a person or entity in pursuit of a common legal goal

<sup>212</sup> Compare *In re Columbia/HCA*, 293 F.3d at 303 (declining to apply selective waiver even in instances where the parties enter into confidentiality orders), with *In re Steinhardt P'ners, L.P.*, 9 F.3d 230, 236 (2d Cir. 1993) (indicating that selective waiver would apply in disclosure to the government as long as a confidentiality agreement existed). See also, e.g., *In re Qwest Commc'ns Int'l Inc.*, 450 F.3d 1179, 1195 (10th Cir. 2006). A footnote accompanying documents voluntarily disclosed to a government entity concerning the exemption of such documents from production under the FOIA is not a sufficient confidentiality agreement to attain selective waiver. See, e.g., *In re Aqua Dots Prod. Liab. Litig.*, 270 F.R.D. 322, 330 (N.D. Ill. 2010), *aff'd*, 654 F.3d 748 (7th Cir. 2011).

<sup>213</sup> CISA requires all personal information to be removed from the disclosure, however, and only protects the disclosure of some information that may not be considered privileged in any case.

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Font: 10 pt, Font color: Black

Formatted: Font: 10 pt, Italic, Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font: 10 pt, Italic, Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



or concerning a matter of mutual legal concern did not waive the privilege/protection by sharing the information.<sup>214</sup> Sharing of CI with third parties may qualify for the joint defense privilege if the contracting parties have a common legal goal, such as to prepare for defense of claims anticipated to be asserted against both entities by consumers or regulators. However, if one of the two parties believes the other is responsible for the incident and the disclosure occurs within the context of a discussion of who is at fault, a common legal goal will not be present. The common interest doctrine may also shield communications between affiliated companies, although a prominent appellate decision held that the so-called “joint representation doctrine”—which prevents waiver of communications between clients who share a common attorney—is a better fit for situations where a single attorney or group of attorneys represents multiple corporate affiliates.<sup>215</sup>

A fact-intensive determination will dictate whether a common interest exists between an insured and its insurer, as courts do not recognize a blanket privilege between insureds and insurers.<sup>216</sup> This determination will likely depend in part on whether the insurer has accepted or denied coverage. When the insurer has accepted coverage (or accepted subject to a reservation of rights), there is more likely a common interest, specifically, the interest in defeating a data breach plaintiff’s claims.<sup>217</sup> By contrast, when the insurer has rejected coverage or the insured is making the disclosure in order to obtain coverage, there is a higher risk that a common interest will not be recognized.<sup>218</sup> Notably, materials generated for insurers in anticipation of litigation are protected by the work product protection, and questions of waiver do not come into play in this inquiry, given that Fed. R. Civ. P. 26(b)(3)(A) specifically includes insurers as among the party representatives covered by the work product doctrine. Case analysis prepared for mediation, status updates, risk assessments, and similar documents prepared during litigation would likely qualify for this protection.<sup>219</sup> Other documents, such as investigation reports, will likely involve a more fact-intensive inquiry.

<sup>214-214</sup> See, e.g., *United States v. Evans*, 113 F.3d 1457, 1467 (7th Cir. 1997).

<sup>215-215</sup> *In re Teleglobe Commc’ns Corp.*, 493 F.3d 345, 370 (3d Cir. 2007) (“Courts typically offer versions of three arguments for not construing the sharing of communications with the corporate family as a waiver: (1) the members of the corporate family comprise one client; (2) the members of the corporate family are joint clients; and (3) the members of the corporate family are in a community of interest with one another. Of these three rationales, we believe only the second withstands scrutiny.”) (internal citations omitted).

<sup>216-216</sup> See, e.g., *Linde Thoms Langworthy Kohn & Van Dyke, P.C. v. Resolution Trust Corp.*, 5 F.3d 1508, 1514–15 (D.C. Cir. 1993); *Imperial Corp. of Am. v. Shields*, 167 F.R.D. 447, 451 (S.D. Cal. 1995) (a limited common interest exists between an insured and an insurer paying for counsel).

<sup>217</sup> See *Lectrolam Custom Sys., Inc. v. Pelco Sales, Inc.*, 212 F.R.D. 567, 571 (E.D. Cal. 2002).

<sup>218</sup> See, e.g., *Conf’l Cas. Co. v. St. Paul Surplus Lines Ins. Co.*, 265 F.R.D. 510, 527 (E.D. Cal. 2010).

<sup>219</sup> See *Chaiken v. VV Publishing Corp.*, 1994 WL 652492, at \*2 (S.D.N.Y. Nov. 18, 1994).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font: 10 pt, Italic, Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font: 10 pt, Italic, Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



Similarly, where the two parties are in other sorts of privity, their contractual relationship may assist or work against a common-interest claim, depending on the nature of the contract and the relationship between the parties.

The court in *Premiera I* had the occasion to review whether the disclosure of CI to third parties who were not defendants in the same litigation, but in similar litigations, was shielded by the common-interest doctrine.<sup>220</sup> Noting that generally joint-defense or common-interest parties are subject to the same litigation, the court found that entities in similar litigation to which *Premiera* had disclosed documents would share a sufficient common interest if they were subject to the same data breach, but otherwise would not.<sup>221</sup>

Although the court in *Rutter* did not reach the issue of waiver because it found that the forensic report and communications were “either factual in nature or, where advice and tactics were involved, did not include legal input,” the court cited favorably in a CI context that “[a]s a general matter, the privilege is not destroyed when a person other than the lawyer is present at a conversation between an attorney and his or her client if that person is needed to make the conference possible or to assist the attorney in providing legal services.”<sup>222</sup>

Similarly, although the court in *Guo Wengui v. Clark Hill, PLC* did not reach the question of waiver, the court found that a forensic report that was shared not only with the defendant’s outside and in-house counsel, but also with the defendant’s “IT staff and the FBI, presumably with an eye toward facilitating both entities’ further efforts at investigation and remediation,” was used for a range of non-litigation purposes, which “reinforces the notion that it cannot be fairly described as prepared in anticipation of litigation.”<sup>223</sup>

#### f. Subject-Matter Waiver

Finally, in a situation where disclosure of attorney-client privileged and/or work-product protected CI operates as a waiver of the privilege and/or protection afforded to the *disclosed* CI, the question may then arise whether such disclosure also operates as a waiver of the privilege and/or protection as to related *undisclosed* CI, both as to others and as to the recipient of the disclosed CI. Under the general principles discussed in Part B.3 above, whether there is such a “subject-matter waiver” may turn on both the identity of the recipient (e.g., federal government versus private party) and the circumstances surrounding the disclosure.

<sup>220-220</sup> *Premiera I*, 296 F. Supp.3d 1230, 1247–50 (D. Or. 2017).

<sup>221-221</sup> *Id.*

<sup>222</sup> *In re Rutter’s Data Sec. Breach Litig.*, No. 1:20-CV-382, 2021 WL 3733137, at \*3 (M.D. Pa. July 22, 2021) (quoting *Miller v. Haulmark Transp. Sys.*, 104 F.R.D. 442, 445 (E.D. Pa. 1984)).

<sup>223</sup> *Guo Wengui v. Clark Hill, PLC*, 338 F.R.D. 7, 12-14 (D.D.C. 2021).

Formatted: Don't suppress line numbers

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



The court in *Premiera I* had occasion to briefly consider whether a disclosure to third parties involved in similar litigation constituted a subject-matter waiver of all related documents. The court declined to find a subject-matter waiver as to all communications relating to the subject matter of the disclosed CI, on the ground that:

because Premiera believed in good faith that it and these entities were subject to the common interest exception to waiver, under the unique circumstances of this case, fairness requires that the waiver of privilege extend only to the communications actually shared among the entities and not to all documents relating to the same subject matter that was addressed in the communications that were shared.<sup>224</sup>

However, the court suggested that, but for this “good faith” exception, a broad subject-matter waiver would have applied.<sup>225</sup>

On the other hand, where attorney-client privileged information is used affirmatively or as a defense, courts have been inclined to hold that such use can operate as a waiver of the privilege in regard to related privileged CI. In *In re United Shore Financial Services, LLC*, the court found a waiver of the privilege in regard to CI created by an investigator because, according to the court, the defendant had used the conclusion of the investigator as a defense in the litigation.<sup>226</sup>

\* \* \*

#### 4. Dual Track Investigations

In light of the decisions noted above addressing defendants’ arguments for privilege or protection based in part on their “dual tracking” of post-breach work, a closer examination of the concept of dual tracking is warranted. “Dual tracking”<sup>227</sup> is a strategy for post-incident CI that attempts to separate investigative efforts into two workstreams: one focused on remediating the data breach and restoring business operations, the other focused on educating legal counsel about the breach so that they may assess legal exposure and potential defenses. In subsequent litigation, entities may produce post-incident CI from the former track but seek to protect post-incident CI from the latter track by asserting attorney-client privilege, work-product, or both.

<sup>224</sup> *Id.* at 1247–49.

<sup>225</sup> *Id.*

<sup>226</sup> No. 17-2290, 2018 WL 2283893 (6th Cir. Jan. 3, 2018).

<sup>227</sup> Courts may refer to a dual track investigation as a “two-track investigation.” See, e.g., *In re Target Corp. Customer Data Security Breach Litig.*, 14-MD-2522, 2015 WL 6777384, at \*2 (D. Minn. Oct. 23, 2015); *In re Dominion Dental Servs. USA, Inc. Data Breach Litig.*, 429 F. Supp. 3d 190, 195 (E.D. Va. 2019) (citing *In re Target Corp.*); *Guo Wengui v. Clark Hill PLC*, 338 F.R.D. 7, 14 (D.D.C. 2021) (citing *In re Target Corp.*).

**Formatted:** Space Before: 0 pt, After: 0 pt, Add space between paragraphs of the same style, Don't suppress line numbers

**Formatted:** Indent: First line: 0", Space Before: 0 pt, Don't suppress line numbers

**Formatted:** Space After: 12 pt, Don't suppress line numbers

**Formatted:** Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Normal



#### a. Benefits and Drawbacks of Dual Track Investigations

One goal<sup>228</sup> of dual tracking is to provide a clear structure for what post-incident CI exists and over which a party is not claiming privilege, with benefits inuring to both plaintiffs and defendants. Defendants can move quickly to contain (and eliminate) the threat and restore their systems to normal business function. Simultaneously, defendants can prepare for potential litigation in a way that minimizes the risk that sensitive elements of their defensive strategy are revealed. Plaintiffs may benefit from a more expedited discovery process as defendants may be more inclined to disclose the factual findings of the remediation track if certain elements of the legal track remain privileged. Furthermore, the bounds of some discovery disputes, at least in theory, are confined ahead of time, thereby potentially reducing the range of disagreement.

Conversely, there are logistical drawbacks and gamesmanship incentives to dual tracking. First, setting up—and maintaining—two separate investigations is twice as expensive and cumbersome as both teams will need to access much of the same information. Communication between the dual tracks, while worth considering in some contexts as explored in Part [cross talk section], risks undermining the structure’s overall clarity, and thus its intended purpose, jeopardizing the privileged aspects. Second, entities may prioritize the remediation track at the expense of preserving privilege in an effort to restore business, or entities may seek to limit the remediation track to present a more favorable picture, or both. Correspondingly, plaintiffs will likely seek production of the privileged legal track regardless of what is produced in the remediation track.

#### b. Case Law Endorsing the use of Dual Track Investigations

Although dual tracking is a more recent innovation, as noted above, some courts have already considered the investigative strategy, usually within the context of the work-product doctrine. For example, the court in *In re Target Corporation Customer Data Security Breach Litigation* recognized that dual tracking could support defendant Target’s assertions of attorney-client privilege and work-product protection.<sup>229</sup> In *In re Target*, as noted above, Target engaged Verizon Business Network Services in early 2014 for a “two-track investigation” following a large-scale data breach that affected Target’s

<sup>228</sup> There may be other reasons that an organization may decide to have two tracks, such as providing non-privileged reports to regulators or stakeholders.

<sup>229</sup> . *In re Target Corp.* 2015 WL 6777384, at \*2.



customer credit card data.<sup>230</sup> The first non-privileged track consisted of Target's own ordinary-course investigation and a Verizon team tasked with producing a PCI Forensic Investigator report on behalf of Target for various credit card companies.<sup>231</sup> The second track consisted of Target's own "Data Breach Task Force" and a separate Verizon team.<sup>232</sup> Target sought to defend the second track as privileged because it was formed with the purpose of educating Target's lawyers about the breach "so that they could provide Target with legal advice and protect the company's interests in litigation that commenced almost immediately after the breach became publicly known."<sup>233</sup>

After reviewing the privilege log documents in camera, the *In re Target* court credited the declaration of Target's chief legal officer as to the purpose of the second track and denied all but two of the plaintiffs' privilege log challenges.<sup>234</sup> The court found that the second track was focused 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."<sup>235</sup> Furthermore, the court found that the plaintiffs failed to meet the substantial need and undue hardship exception to work product protection. In doing so, the court cited Target's first-track productions of "documents and other tangible things, including forensic images" that included the 131-page PCI Forensic Investigator report from Target's first, non-privileged track.<sup>236</sup>

As demonstrated in *In re Target*, the intent and purpose of the separate investigations feature prominently in a court's dual tracking analysis, as they would in any work-

<sup>230</sup> . *Id.*, at \*1-2.

<sup>231</sup> . *Id.*, at \*2; Letter to Magistrate Judge at 1-2, *In re Target Corp. Customer Data Security Breach Litig.*, 14-MD-2522, (D. Minn. Oct. 23, 2015), 2015 WL 6777384, ECF No. 599. The Payment Card Industry Security Standards Council ("PCI SSC") directs certain entities to engage forensic investigators following some security incidents that impact credit card information. The resulting PCI Forensic Investigator ("PFI") report is shared with the relevant payment card brands. See PCI Sec. Standards Council, PCI Forensic Investigator (PFI) Program Guide (2016), [https://www.pcisecuritystandards.org/documents/PFI\\_Program\\_Guide\\_v3.0.pdf](https://www.pcisecuritystandards.org/documents/PFI_Program_Guide_v3.0.pdf). For these reasons, a PFI report would not be privileged. Here, Target did not assert the PFI report was privileged and produced the 131-page report in discovery. See Letter to Magistrate Judge, *supra*, at 5-6; Declaration of Michelle Wugmeister at 4, *In re Target Corp.*, 14-MD-2522, 2015 WL 6777384, ECF No. 603.

<sup>232</sup> *In re Target Corp.*, 2015 WL 6777384, at \*2.

<sup>233</sup> *Id.*

<sup>234</sup> *Id.*, at \*2-4.

<sup>235</sup> *Id.*, at \*3.

<sup>236</sup> *Id.*, at \*3; Letter to Magistrate Judge, *supra* note 5, at 5-6.



product evaluation that examines whether the document at issue was “prepared in anticipation of litigation or for trial.”<sup>237</sup>

Where multiple motivations may obfuscate the intent of an investigation, *In re Experian Data Breach Litigation* shows that dual tracking can strengthen a work-product claim.<sup>238</sup> In *re Experian*, defendant Experian retained outside counsel upon learning that one of its systems was breached by an unauthorized third party.<sup>239</sup> Outside counsel then hired a cybersecurity firm, which had worked with Experian in the past, to “conduct an expert report analysis of the attack . . . to help [outside counsel] provide legal advice to Experian regarding the attack.”<sup>240</sup> At the same time, Experian conducted its own internal investigation of the data breach.<sup>241</sup>

The court found that the cybersecurity firm’s report was protected under the work-product doctrine because the cybersecurity firm “was hired by [outside counsel] to assist [outside counsel] in providing legal advice in anticipation of litigation.”<sup>242</sup> Critically, the court relied on declarations regarding the purpose of the investigation, but also the fact that the cybersecurity report was not shared with Experian’s internal investigation team. “If the report was more relevant to Experian’s internal investigation or remediation efforts, as opposed to being relevant to defense of this litigation,” the court noted, “then the full report would have been given to that team.”<sup>243</sup>

*In re Experian* suggests that the existence of two separate tracks headed by two separate parties can enhance a claim that one is privileged. While not explicitly stated, the *In re Experian* court relied on the fact that the privileged, legally oriented track did not share its report with the remediation track, a fact that may be more difficult to prove if a single entity is responsible for both tracks.

#### c. Case Law That Rejects Arguments Regarding Dual-Track Investigations

<sup>237</sup> Fed. R. Evid. 502.

<sup>238</sup> *In re Experian Data Breach Litig.*, 15-CV-1592, 2017 WL 4325583 (C.D. Cal. May 18, 2017).

<sup>239</sup> *Id.*, at \*2.

<sup>240</sup> *Id.*

<sup>241</sup> *Id.*

<sup>242</sup> *Id.*

<sup>243</sup> *Id.*



However, other courts have rejected attempts to characterize certain post-breach investigations as “dual track” to avoid full disclosure. In *Clark Hill*,<sup>244</sup> for example, the defendant had presented a nuanced argument that the post-incident CI report qualified as being prepared in anticipation of litigation because it was the result of only one half of a “two-tracked investigation of the incident.”<sup>245</sup> One one track, Clark Hill’s pre-existing cybersecurity vendor worked to investigate and remediate the attack to preserve business continuity, and, on a “separate track,” the defendant’s counsel hired the forensic consultant for the sole purpose of gathering information to render legal advice.<sup>246</sup> The court flatly rejected the defendant’s argument, finding no support in the evidentiary record and quoting *Dominion Dental* and *Premiera I*. The court noted that defendant’s internal emails referred to the forensic consultant as the “incident response team,” and that defendant had not involved its existing cybersecurity vendor once counsel retained the forensic consultant.<sup>247</sup>

\*\*\*

The use of dual tracking ultimately does not alter the court’s privilege analysis, as courts will still assess whether dual track investigations meet work-product protection or attorney-client privilege thresholds. The rigor with which courts review dual track investigations may discourage defendants from nominally employing the investigative strategy in the hopes of shielding post-incident CI from discovery. By the same token, a dual tracking strategy that is properly initiated and executed can strengthen an entity’s claim that some post-incident CI is protected.

5. *Practical Guidance: The Relationship Between the Burden of Proof and Limits on the Ability to Obtain Information, and an Exploration of the Concept of “Substantial Need”*

Attorney-client privilege and the work product doctrine play a particularly important role when litigating cases arising from security incidents because a plaintiff will likely seek to obtain certain pre-incident and post-incident CI from the defendant to prove his

<sup>244</sup> . 338 F.R.D. 7, 10-11 (D. D.C. 2021)

<sup>245</sup> . *Id.*

<sup>246</sup> . *Id.*, citing *Target*, 2015 WL 6777384 at \*2-3.

<sup>247</sup> . *Id.*



or her case and the Defendant will likely assert such CI is protected by attorney-client privilege and/or the work product doctrine.<sup>248</sup>

The CI likely to be sought by Plaintiffs will be contained in sources ranging from those that are purely factual and unlikely to be considered privileged, to some tending to have privileged aspects, to those that are likely to be completely privileged. The more intertwined CI becomes with legal advice or an attorney's mental impressions, thoughts, or legal strategy, the more likely the CI contained therein is privileged, and will thus be shielded from discovery. The purpose of this section is to explore the relationship between attorney client privilege, work product, and a plaintiff's ability to obtain relevant CI when facts and privilege are intertwined.

#### a. CI a Plaintiff May Seek in Discovery

The types of CI a plaintiff may seek in discovery can be grouped into the following five categories: data security practices; timeline of the security incident, source of the security incident, scope of the security incident, and remediation of the security incident.

##### i. Data Security Practices

Data security practices involve a defendant's written (internal and external) privacy and security policies that were in place prior to the security incident; defendant's security practices implemented prior to the security incident, i.e. what was the state of the defendant's pre-incident security controls and what/when were critical vulnerabilities known and how, if at all, addressed; and was the defendant aware of the specific vulnerability(ies) that led to the security incident, and if so, what did the defendant do to mitigate the vulnerability(ies)? This information is likely to be relevant because they bear on the defendant's duty of care regarding data security.

##### ii. Timeline of the Security Incident

---

<sup>248</sup> . See e.g., *Guo Wengui v. Clark Hill, PLC*, 338 F.R.D. 7, 9 (D.D.C. 2021) (discovery dispute arose between the parties over documents generated by defendant in the wake of the security incident – i.e., forensic reports, analyses, and internal communications – that defendant claimed were protected by attorney client privilege and work product.)



The timeline of the security incident generally involves answers to the following questions: when did the incident occur; when did the defendant become aware of the incident; when did the defendant determine or have enough evidence to determine that the incident was a security incident; when did the defendant determine the scope of the data impacted; what notifications and public statements did the defendant make to regulators, customers, contract partners, and the general public; and when did the defendant notify regulators, customers, and contract partners? This information is likely to be relevant because of the notification requirements in many states that must be made within a certain time after discovery of the incident.

### iii. Source of the Security Incident

The source of the security incident focuses on the who, what, and how of the security incident. That is how did it occur; what caused it; and who, i.e., cybercriminals or hackers, were involved? This information is likely to be relevant because it may bear on whether the defendant owed a duty and/or breached a duty to the plaintiff.

### iv. Scope of the Security Incident

The scope of the security incident relates to the severity of the security incident, including what systems were impacted; what data and information were impacted; was data accessed, acquired, exfiltrated, ect.; and was the data at issue encrypted? This information is likely to be relevant because it bears on whether CI was exposed or potentially exposed, the number of persons impacted by the security incident, and potential damages suffered by the persons affected.

### v. Remediation of the Security Incident

Remediation of the security incident involves actions a defendant took in light of the security incident. These include actions defendant took once it became aware of the security incident, i.e., what remedy the defendant provided to consumers (such as credit monitoring) and how defendant resolved the security incident, i.e., did the defendant address or cure the security vulnerability or other similar issue?

### b. Sources of CI


There are many sources of the CI discussed above. The chart below lists the sources and the likelihood that a court will find them to be privileged:

Formatted: Normal



## SOURCES OF PRE-INCIDENT CI


### LEAST LIKELY TO BE PRIVILEGED

- 
- Technical Inventories, Configuration Reviews, Vulnerability Scans, and Penetration Tests, Security, and IT-Oriented Alerts and Logs.
  - Company Policies, Practices, Procedures, IR Plans, IR Playbooks, and Risk Registers
  - Security Risk Assessments, Outside Audits, Internal Audits, and Remediation Efforts
  - Reports of Security Team and Tabletop Exercises
  - Board-Level Documents and Communications

### MOST LIKELY TO BE PRIVILEGED

## SOURCES OF POST-INCIDENT CI

### LEAST LIKELY TO BE PRIVILEGED

- 
- Security and IT-Oriented Alerts and Logs
  - Ticketing Systems, Messaging Systems, GRC Systems, Collaboration Tools, and Helpdesk Phone Logs
  - Post-Incident Security Assessments
  - Regulatory and Industry Standard Reports
  - Law Enforcement and Investigation Disclosures
  - Sworn Testimony and Interviews
  - Breach Log (document or spreadsheet)
  - Emails about the Security Incident
  - Forensic Consultant Reports
  - Attorney-driven incident management, workflow, and legal operations platforms

### MOST LIKELY TO BE PRIVILEGED

c. Whether CI is Privileged Depends on Factual Information Contained within the CI.

Formatted: Normal



CI in a defendant's possession can be subject to both attorney-client privilege and work product protection. Defendant need only show CI is protected by either attorney-client privilege or work product to shield it from discovery.<sup>249</sup>

i. Separating the Facts from Attorney-Client Communications

Whether CI is privileged under the attorney-client privilege will often hinge on whether the attorney-client communication contains a request for or provision of legal advice or simply contains underlying facts.<sup>250</sup>

To avoid issues of privilege, this means that a plaintiff should target CI that was created independent of attorney involvement or advice. For example, in *In re Rutter's Data Security Breach Litigation*, the plaintiffs moved to compel the production of "an investigative report created in response to the data breach by a third-party cybersecurity consultant."<sup>251</sup> Because the consultant's report was inherently factual, and without any mention of attorney involvement, the court found that the report was not protected by attorney-client privilege.<sup>252</sup>

However, it is more likely that the underlying facts are intertwined with attorney-client communications. If facts are contained in attorney-client communications a plaintiff's discovery requests should differentiate the underlying facts from attorney-client communications. For instance, in *Attorney General of the Commonwealth of Massachusetts v. Facebook, Inc.*, the Massachusetts Attorney General requested documents and communications sufficient to identify applications and developers that Facebook reviewed during an internal investigation conducted by its legal counsel.<sup>253</sup> The Massachusetts Supreme Court ordered the production of these documents because the requests asked for underlying factual data about the apps' breaches and of privacy policies.<sup>254</sup> The requests did not impinge on privilege because even if the facts "ha[d]

<sup>249</sup> . *Att'y Gen. v. Facebook, Inc.*, 164 N.E.3d 873, 888 (Mass. 2021) (explaining that where discovery requests were not covered by attorney-client privilege, they did implicate the work product doctrine).

<sup>250</sup> . *Id.*

<sup>251</sup> . *In re Rutter's Data Sec. Breach Litig.*, No. 1:20-CV-382, 2021 WL 3733137, at \*1 (M.D. Pa. July 22, 2021).

<sup>252</sup> . *Id.*, at \*4.

<sup>253</sup> . *Id.*

<sup>254</sup> . *Id.*



almost certainly been contained in attorney-client communications” Facebook was not required to produce “the attorney-client communications themselves.”<sup>255</sup>

In contrast however, courts have recognized that where the underlying facts are available in discoverable, non-privileged sources, a plaintiff’s attempt to discover those facts through attorney-client communications will fail. Relevant to this concept is *Maldonado v. Solara Medical Supplies, LLC*, where the defendant engaged in a two-track investigation after a security incident – one privileged and one not.<sup>256</sup> When the plaintiffs moved to compel Solara to produce the results of its legally oriented investigation, the court denied the plaintiffs’ motion because the underlying facts were all available in the other track’s investigation.<sup>257</sup>

Based on the forgoing analyses, these cases indicate that when drafting discovery requests or objecting to discovery requests involving CI, it is important for the parties to distinguish independently discoverable CI from CI that does not exist independently from attorney-client communications.

A related concept to the discovery of the underlying facts, is the discovery of documents attached to attorney-client communications. As already discussed, a document does not become privileged because it is attached to an attorney-client communication.<sup>258</sup> But the attachment will become privileged when sent to the lawyer because the fact that the attachment is sent partially reveals the substance of the privileged communication.<sup>259</sup> As such, it is also important to differentiate requests for pre-existing CI from requests for CI attached to privileged communications. Instructive is *In re Marriott International, Inc. Customer Data Security Breach Litigation*, where the court found that attachments emailed to counsel were privileged because they brought the information to counsel’s attention or helped answer one of his questions.<sup>260</sup> Accordingly, a plaintiff should request the original document, not the copy attached to an attorney-client communication.

---

<sup>255</sup> . *Id.*

<sup>256</sup> . *Order on Plaintiffs’ Motion to Compel Compliance With Subpoena Duces Tecum Directed to Non-Party Charles River Associates (#1)*, *Maldonado v. Solara Medical Supplies, LLC*, Civil Action No. 20:12198-LTS, at 1–2 (D. Mass. June 2, 2021).

<sup>257</sup> . *Id.* at 9.

<sup>258</sup> . *In re Marriott Int’l, Inc.*, No. 19-MD-2879, 2021 WL 2222715, at \*3 (D. Md. June 2, 2021).

<sup>259</sup> . *Id.*

<sup>260</sup> . *Id.*, at \*3.



The last distinction regarding CI and attorney-client privilege is to identify whether the CI exists independent of attorney involvement, or whether the facts are collected at counsel's requests for later use in providing legal advice. Marriott is again instructive. There the court explained that communications "gathering information at the direction of counsel for the purposes of rendering legal advice and in anticipation of litigation about security questions related" to Marriott's security incident were privileged.<sup>261</sup> As such, it is not enough to separate facts from privileged communications. When the facts are gathered during a legal investigation directed by counsel for the purpose of securing legal advice, those facts become so intertwined with the attorney-client communications, that they become privileged themselves.

In the end, these cases demonstrate the difficulties in discovering CI in the defendant's possession as a plaintiff's discovery requests must be narrowly tailored to requesting underlying factual information regarding the security incident that is independent of attorney involvement.

ii. "Substantial Need" and "Undue Hardship" to Overcome the Work Product Doctrine Will turn on whether the CI Constitutes Factual or Opinion Work Product.

As already discussed, the work product protection is not absolute. But even though work product may be discoverable, the extent to which work product is discoverable will turn on whether it constitutes "opinion work product," or "fact work product." The distinction is important because a party may only discover opinion work product, if at all, "in rare or 'extremely unusual' circumstances."<sup>262</sup> As such, opinion work product is "virtually undiscoverable."<sup>263</sup> On the other hand, fact work product is discoverable upon a showing that (1) the party seeking the discovery has a "substantial need of the materials" and (2) the party is "unable without undue hardship to obtain the substantial equivalent by other means."<sup>264</sup>

Before parties litigate over the discovery of work product containing CI, however, it is necessary to determine whether the documents at issue are opinion work product or

---

<sup>261</sup> . Id., at \*4.

<sup>262</sup> . Facebook, Inc., 164 N.E.3d at 890 (quoting Comm'r of Revenue v. Comcast Corp., 901 N.E.2d 1185, 1202 (Mass. 2009)).

<sup>263</sup> . Dir., Off. of Thrift Supervision v. Vinson & Elkins, LLP, 124 F.3d 1304, 1307 (D.C. Cir. 1997).

<sup>264</sup> . Facebook, Inc., 164 N.E.3d at 890.



fact work product. Opinion work product is that which contains “the mental impressions conclusions, opinions, or legal theories of a party’s attorney or other representative concerning litigation.”<sup>265</sup> Fact work product is essentially all other work product, including the results of factual investigations.<sup>266</sup> Determining which type of work product is at issue is important because it determines how discoverable the work product might be. While the line between opinion and fact work product is unfortunately not always clear, a helpful distinction may be to consider whether “the focus selection, or arrangement of the facts . . . reflect the attorney’s thought process in some ‘meaningful way.’”<sup>267</sup> Still, even where a document contains both fact and opinion work product, a court may order the disclosure of the factual matters, if they can be “disclosed without revealing the attorney’s opinions.”<sup>268</sup>

Again, Facebook is instructive regarding the importance of distinguishing opinion from fact work product. There, the court concluded that if the Attorney General’s requests were for fact work product, they should be produced as the Attorney General established a showing of substantial need and undue hardship for that information.<sup>269</sup> Unfortunately, the court was unable to conclude whether the app information was opinion or fact work product because while Facebook publicly disclosed some statements regarding the investigation process, the investigation was staffed by outside counsel and consultants, focused on past violations to defend Facebook in litigation rather than improving its ongoing business operations, and thus it was unclear on the record before the court on whether the work product included “strategic decision-making by counsel, including the assessment of legal risk or liability.”<sup>270</sup> As such, the court remanded to determine whether the work product was fact or opinion.<sup>271</sup> Accordingly, Facebook demonstrates that before challenging the discovery of work product on the basis of substantial need and undue hardship, it is important for a plaintiff to have enough facts to argue why the work product is fact and not opinion work product.

---

<sup>265</sup> . Burrow v. Forjas Taurus S.A., 334 F. Supp. 3d 1222, 1229 (S.D. Fla. 2018) (quoting Fed. R. Civ. P. 23(b)(3)(B)).

<sup>266</sup> . Id.

<sup>267</sup> . Facebook, Inc., 164 N.E.3d at 890 (quoting F.T.C. v. Boehringer Ingelheim Pharms., Inc., 778 F.3d 142, 152 (D.C. Cir. 2015)).

<sup>268</sup> . Boehringer Ingelheim Pharms., Inc., 778 F.3d at 152.

<sup>269</sup> . Facebook, Inc., 164 N.E.3d at 893.

<sup>270</sup> . Id. at 894–95.

<sup>271</sup> . Id. at 895.



Once a plaintiff has established which CI is fact work product, they may have a case for a establishing a substantial need and undue hardship for CI if it is only available through the defendant's work product.<sup>272</sup> In demonstrating substantial need and undue hardship, a plaintiff must generally show "that the materials are relevant to the case, the materials have a unique value apart from those already in the movant's possession, and "special circumstances" excuse the movant's failure to obtain the requested materials itself."<sup>273</sup> Ultimately "[t]he 'substantial need' inquiry requires a careful examination of whether non-disclosure will impair the truth-seeking function of discovery."<sup>274</sup> For instance in Facebook, the court found that, if the requested work product was fact work product, the Attorney General established a substantial need and undue hardship to discover documents and communications sufficient to identify applications and developers that Facebook reviewed during an internal investigation conducted by its legal counsel.<sup>275</sup> In reaching this determination, the court noted that the information was central to the Attorney General's investigation, "uncovering this otherwise discoverable factual information would be a monumental, if not herculean, task absent Facebook disclosing the app information," and it was "unlikely that the Attorney General would be able to obtain the substantial equivalent of this app information, even with extraordinary efforts."<sup>276</sup>

However, courts will refuse to find a showing of substantial need and undue hardship where the CI exists in another non-privileged, discoverable form. This is true even when it is "expens[ive] or inconvenien[t] to Plaintiffs in hiring an expert to perform the same analysis."<sup>277</sup> For instance, in In Re Experian Data Breach Litigation, the court found that the plaintiffs failed to establish a substantial need to discover a forensic report prepared by Mandiant after Experian suffered a security incident.<sup>278</sup> The court refused to compel the production of the report because Mandiant only observed the server images when creating the report, and thus the plaintiffs could conduct their own investigation by

---

<sup>272</sup> . Burrow, 334 F. Supp. 3d at 1230 ("a common justification for discovery is the claim which relates to the opposite party's knowledge that can only be shown by the documents themselves.") (internal quotations omitted).

<sup>273</sup> . Boehringer Ingelheim Pharms., Inc., 778 F.3d at 155.

<sup>274</sup> . Id. at 156.

<sup>275</sup> . Facebook, Inc., 164 N.E.3d at 891.

<sup>276</sup> . Id. at 896–97.

<sup>277</sup> . In re Experian Data Breach Litig., No. SACV1501592AGDFMX, 2017 WL 4325583, at \*3 (C.D. Cal. May 18, 2017).

<sup>278</sup> . Id.



discovering and analyzing those same server images.<sup>279</sup> On the other hand, in *Wengui v. Clark Hill, PLC*, the court denied Clark Hill's privilege claim with respect to a Duff & Phelps forensic report, in part because nearly all of the investigation's factual findings could be found only in that report; the competing report from eSentire that was produced to the plaintiff was effectively worthless.<sup>280</sup>

As such, these cases demonstrate that when challenging purported work product that may contain CI on the basis of substantial need and undue hardship, a plaintiff must target factual work product, not opinion work product. In turn, this limits a plaintiff's ability to obtain CI the more it becomes intertwined with an attorney's thoughts, impressions, and legal strategy. Further these cases indicate that, unless it would be an enormous effort to replicate the defendant's investigation, if a plaintiff has access to the underlying factual information contained in fact work product, a plaintiff is unlikely to establish a substantial need and undue hardship to overcome work product protection.

6. Legal Evaluation and Practice Guidelines as to Application of Attorney-Client Privilege and Work Product Protection for Specific Entities: Vendors and Service Providers

A range of external vendors and service providers may be engaged to assist an organization and its legal counsel to prepare for and respond to cybersecurity incidents. These may include, among others:

- Digital Forensics/Incident Response firms
- Managed Security Service Providers
- E-Discovery/data hosting and analytics firms
- Penetration testing firms
- Source code review consultants
- Cyber risk assessment consultants
- Crisis communications and public information consultants

Cases involving attorney-client privilege and work product protection in the cybersecurity context suggest that the practices of these third parties are material considerations and may even be pivotal in a court's determination. As such, firms offering pre- and post-incident services may wish to observe the following guidance.

a. Pre-Engagement Practices

---

<sup>279</sup> . *Id.*

<sup>280</sup> . *Guo Wengui*, 338 F.R.D. at 11 ("Clark Hill turned to Duff & Phelps instead of, rather than separate from or in addition to, eSentire, to do the necessary investigative work.") (emphasis in original).



#### i. Training

Vendors should train their engagement managers and service delivery teams to sensitize them to the nuances of privilege in the cybersecurity context. Doing so will prepare them to address the potential privileged nature of the vendor's work in the pre-engagement scoping and contracting phase and help them avoid actions during the engagement that might waive privilege.

#### ii. Engagement Agreements

Courts have scrutinized engagement agreements to discern the purpose of the vendor's retention. Accordingly, in engagements that support counsel's provision of legal advice, the agreements should include language making clear the purpose of the retention. When a client-vendor relationship is created pre-incident and for an apparent business purpose, if there is the potential that the vendor will be called upon to support counsel's provision of legal advice, the parties are best served to use a specific statement of work or separate agreement to address those circumstances.<sup>281</sup> Even in those circumstances, a court may conclude that the business purpose for the vendor's original retention is imputed to a successive assignment, especially if the scope of services has not materially changed.<sup>282</sup> Therefore, in an abundance of caution, the vendor may wish to assign separate personnel to the latter work to counter the view that it was only an extension of prior services rendered to the client for business purposes.

#### iii. Billing and Payment Arrangements

In setting up an engagement, vendors should consider what entity, unit, or individual should be chosen for billing and payment. If the engagement's purpose is to support outside counsel's provision of legal advice and/or in anticipation of trial, it may be better for the vendor to bill outside counsel for the services, rather than the ultimate client. Where that arrangement is not feasible, submitting invoices to internal legal counsel may strengthen a client's claim of privilege of CSI involving or generated in the engagement. The same can be said of having the engagement funded through the client's legal

<sup>281</sup> . New Albertson's Inc. v. Mastercard Int'l, Inc., Case No. CV01-17-04410 (Idaho Dist. Ct. 4th Dist. May 31, 2019), at 5 (noting that prior direct retention of cybersecurity firm (Dell) by client was terminated once outside counsel was engaged and outside counsel retained same firm for privileged investigation).

<sup>282</sup> . In re: Capital One Consumer Data Security Breach Litigation, MDL No. 1:19md2915 (AJT/JFA) (Document 490) (E.D. Va. May 26, 2020), at 11 (distinguishing prior case in which outside counsel retained cybersecurity vendor from instant case in which a client-vendor relationship existed when incident was discovered in determining that report was not prepared because of potential litigation).



department's budget, as opposed to another business unit.<sup>283</sup> While vendors cannot control this, they can facilitate a discussion with the client about this option and the potential bearing it may have on later determinations about privilege.

#### b. Practices During an Engagement

##### i. Meetings and Interim Written Communications

Vendors should confer with legal counsel at the outset of and regularly during the engagement to provide verbal updates and receive guidance related to progress of the work.<sup>284</sup> In addition, the vendor's staff should refrain from meeting with, reporting to, or receiving taskings from others in the client's business, unless supervising counsel specifically approves. While the participation of others in the business may be required at various times to support the vendor's work (e.g., to inform the vendor about the client's IT environment and data holdings, to furnish access to data or systems) care should be given not to widen the circle of participants beyond those necessary to support legal counsel's provision of advice.

Relatedly, written communications between a vendor's staff and the client's team should be limited to what is necessary to advance the objectives defined by legal counsel. Counsel should be copied on any such communications and the messages themselves should bear an appropriate marking that they are privileged CSI. Diary entries for timekeeping purposes should, at a minimum, note the participation of legal counsel in meetings and note any taskings received from the attorneys.

##### ii. Internal Procedures

Vendors will undoubtedly have executed a written agreement with confidentiality provisions at the start of the engagement. The vendor's internal files should be maintained and marked in such a way that the privileged status of their work is apparent (if indeed they are supporting the provision of legal advice and not serving only a

---

<sup>283</sup> . In re: Capital One Consumer Data Security Breach Litigation, MDL No. 1:19md2915 (AJT/JFA) (Document 490) (E.D. Va. May 26, 2020), at 8 (determining that investigation was not entitled to privileged status in part because the client paid a cybersecurity investigator out of a retainer that was classified as "business-critical and not a legal expense at the time it was paid"); id. at 13 (noting that scope of work had not materially changed from prior direct engagement by client of cybersecurity investigator and later engagement of same by outside counsel).

<sup>284</sup> . New Albertson's Inc. v. Mastercard Int'l, Inc., Case No. CV01-17-04410 (Idaho Dist. Ct. 4th Dist. May 31, 2019), at 6 (finding privilege extended to investigation supervised by external counsel who "did take an active role in directing the ongoing investigation").



business purpose of the client) and access limited to personnel assigned to the matter or with a bona fide need-to-know.

A vendor should preserve data that it receives for analysis from a client in a privileged engagement so that it is available for production to a third party in litigation. The availability of such data offers a potential litigant the ability to analyze it and may help the client maintain privileged status over the vendor's analysis of the same data.

### iii. Deliverables (Reports, Presentation Slides, and Memoranda)

Before documenting findings in a written report, presentation slides, or memorandum in a privileged engagement, the vendor should confer with counsel as to whether such a deliverable is desired and what its scope should be. Recommendations for remediation or future improvements should not be incorporated into a forensic report detailing matters that occurred in the past without specific instructions from counsel to include them. Deliverables should be maintained in draft and circulated to counsel for review and comment prior to sending to the ultimate client. Vendors should avoid sending written deliverables to individuals or groups within the client's organization who are not involved in supporting counsel's provision of legal advice without first discussing with counsel.<sup>285</sup> Even when a wider distribution is authorized by counsel, caveats limiting the deliverable's use, as well as restrictions on further dissemination, should be placed in the document.<sup>286</sup>

## 7. Legal Evaluation and Practice Guidelines as to Application of Attorney-Client Privilege and Work-Product Protection in Evaluating Business versus Legal Advice

<sup>285</sup> . Compare Guo Wengui v. Clark Hill, PLC, 338 F.R.D. 7, 12 (D.D.C. 2021) (distribution of forensic report beyond outside and in-house counsel, specifically to "select members of [client's] leadership and IT Team," supported finding that report was not protected work product) with In re: Capital One Consumer Data Security Breach Litigation, MDL No. 1:19md2915 (AJT/JFA) (Document 490) (E.D. Va. May 26, 2020), at 10 (cybersecurity firm's report was disseminated widely, including to the client's "cyber technical, enterprise services, information security and cyber teams and that it was used by the client "for various business and regulatory purposes") and In re Dominion Dental Servs. USA, Inc. Data Breach Litig., 429 F. Supp. 3d 190, 194 (E.D. Va. 2019) (client could not represent that purportedly privileged forensic report was not shared with its incident response team) and In re Experian Data Breach Litig., 2017 WL 4325583 (C.D. Cal May 18, 2017), at \*3 (stating that if the report "was more relevant to the [client's] internal investigation or remediation effort, as opposed to being relevant to defense of the litigation, then the full report would have been given to [client's incident response team].").

<sup>286</sup> . In re: Capital One Consumer Data Security Breach Litigation, MDL No. 1:19md2915 (AJT/JFA) (Document 490) (E.D. Va. May 26, 2020), at 5 (noting that client seeking to avoid producing forensic report failed to identify any handling restrictions placed on dissemination of report within client's organization, to its board, to an external accounting firm, and to four regulators).



#### a. In-House Concerns

Walking the line between business advice and legal advice remains a balancing act, particularly for in-house counsel in the data privacy and/or cybersecurity arena. As discussed above, for documents and communications to be privileged, such documents and communications must have been made predominantly for the purpose of assisting counsel in rendering legal advice to a client.<sup>287</sup> In cases involving claims of privilege based on communications with in-house counsel, the law requires that the protections afforded by the attorney-client privilege be “applied more narrowly and cautiously.”<sup>288</sup> In-house counsel, more so than their outside counsel counterparts, are likely to be involved in a company’s day-to-day business operations and may also play a role in business decisions.<sup>289</sup> As a result, not every communication with an in-house lawyer is subject to the attorney-client privilege.<sup>290</sup>

The inquiry into whether a communication involving in-house counsel reflects business advice or legal advice is itself a fact-specific, context-driven one that emphasizes the primary purpose of the communication. Courts continue to diverge on the components of this analysis with certain courts applying a test that inquires whether soliciting or rendering legal advice is merely a primary purpose of the communication<sup>291</sup> and other courts favoring assessing whether the requesting or conveying legal advice is

---

<sup>287</sup> Upjohn Co. v. United States, 449 U.S. 383, 394-395 (1981) (analyzing communications involving company’s general counsel’s communications with company employees during interviews related to internal investigation with legal implications); THE AMERICAN LAW INSTITUTE, *supra* note 7, at § 72 cmt. c (2000) (“A client must consult the lawyer for the purpose of obtaining legal assistance and not predominantly for another purpose.”).

<sup>288</sup> . In Re Ford Motor Co. Crown Victoria Police Interceptor Products, 2003 WL 22217673, \*1 (N.D. Ohio July 1, 2003).

<sup>289</sup> . See United States v. ChevronTexaco Corp., 241 F. Supp.2d 1065, 1076 (N.D. Cal. 2002) (“[U]nlike outside counsel, in-house attorneys can serve multiple functions within the corporation. In-house counsel may be involved intimately in the corporation’s day to day business activities and frequently serve as integral players in business decisions or activities. Accordingly, communications involving in-house counsel might well pertain to business rather than legal matters. The privilege does not protect an attorney’s business advice.”); Burgos-Stefanelli v. Napolitano, 09-60118-CIV, 2009 WL 10667764, at \*2 (S.D. Fla. 2009) (recognizing unique issues regarding the attorney-client privilege arise when in-house counsel is involved).

<sup>290</sup> . “[D]ocuments prepared by non-attorneys and addressed to non-attorneys with copies routed to counsel are generally not privileged since they are not communications made primarily for legal advice.” Neuder v. Battelle Pac. Nw. Nat’l Lab., 194 F.R.D. 289, 295 (D.D.C. 2000).

<sup>291</sup> . New York v. Mayorkas, No. 20-CV-1127 (JMF), 2021 WL 2850631 (S.D.N.Y. July 8, 2021) (continuing to apply the “a” predominant purpose test); In re Smith & Nephew Birmingham Hip Resurfacing Hip Implant Prod. Liab. Litig., No. 1:17-MD-2775, 2019 WL 2330863, at \*2 (D. Md. May 31, 2019) (same); Louise Trauma Ctr., LLC v. Dep’t of Just., No. CV 20-3517 (RC), 2022 WL 278771 (D.D.C. Jan. 30, 2022) (same).



the primary purpose of the communication.<sup>292</sup> In either instance, courts will examine the content of the communications to determine whether they contain or ask for legal analysis or whether they primarily concern the growth and development of profit.<sup>293</sup>

Regardless of the specific test applied, courts look at the communication itself and context to determine whether in-house counsel is acting as a legal advisor or business associate.<sup>294</sup> Some relevant factors courts consider to determine the primary purpose of a mixed communication include: (1) the context of the communication and the content of the document; (2) whether the legal purpose permeates the document and can be separated from the rest of the document; and (3) whether legal advice is specifically requested and the extent of the recipient list.<sup>295</sup>

Communications with in-house lawyers in the data privacy or cybersecurity context involve unique nuance when it comes to application of the attorney client privilege. Many communications with in-house counsel, particularly in the data privacy and cybersecurity area, serve a dual purpose both to ensure the compliant operation of the company and to address legal mandates which include security assessments, audits, reports and even litigation. The duality of the in-house counsel role in the data privacy and cybersecurity context and the privilege protections flowing from it are frequently categorized temporally.

For example, and as emphasized above, courts are increasingly likely to find communications with in-house counsel related to compliance efforts as falling outside the purview of the attorney client-privilege unless they are specifically responding to legal inquiries, audits, or reports.<sup>296</sup> As evidenced by the *Premiera II* decision, the

---

<sup>292</sup> . *In re OneJet, Inc.*, 613 B.R. 841 (Bankr. W.D. Pa. 2020) (applying “the” predominant purpose test); *In re Polaris, Inc.*, No. A20-0427, 2021 WL 5913633 (Minn. Dec. 15, 2021) (same); *Walker v. Shangri-La Corp.*, No. 6:20-CV-01577-MK, 2022 WL 263493 (D. Or. Jan. 28, 2022).

<sup>293</sup> . See, e.g., *Fed. Trade Comm’n v. Abbvie, Inc.*, No. CV 14-5151, 2015 WL 8623076, at \*10 (E.D. Pa. Dec. 14, 2015); *Lindley v. Life Inv’rs Ins. Co. of Am.*, 267 F.R.D. 382, 392 (N.D. Okla. 2010), *aff’d in part as modified*, No. 08-CV-0379-CVE-PJC, 2010 WL 1741407 (N.D. Okla. Apr. 28, 2010).

<sup>294</sup> . *In re Grand Jury Proceedings*, 2001 WL 1167497, \*27-28 (S.D.N.Y. Oct. 3, 2001) (privilege applied where in-house counsel was “functioning as an attorney”).

<sup>295</sup> . *Phillips v. C. R. Bard, Inc.*, 290 F.R.D. 615, 629 (D. Nev. 2013).

<sup>296</sup> . *In re Seroquel Prods. Liab. Litig.*, No. 06-md-1769, 2008 WL 1995058, at \*7 (M.D. Fla. May 7, 2008) (discussing “mixed purpose” documents involving in-house counsel including those involving regulatory compliance and ordering production of same; the court stated the fact of “extensive or pervasive regulation does not make the everyday business activities legally privileged from discovery.” *Id.* at 7.); *Hennigan v. General Electric Company*, No. 09-11912, 2011 WL 13214444 (E.D. Mich. Jun. 1, 2011) (ordering production of documents reflecting communications with in-house lawyer as to certain safety concerns related to microwaves manufactured by the defendant over privilege objections because the “Safety Council” where those safety concerns were discussed occurred in the ordinary course of the company’s operations and the related documents “consist[ed] of reports of a technical nature relating to consumer complaints or reported incidents of microwave fires or self-starts” rather than clear legal advice).



distinction between communications with in-house counsel which are protected by the attorney-client privilege and those that are not is one of degrees. In *Premera II*, the court determined an internal investigation to determine the cause of the subject breach, despite involvement of in-house counsel, was not subject to attorney-client privilege because “Premera needed to conduct an investigation as a business in order to figure out the problem that allowed the breach to occur so that Premera could solve that problem and ensure such a breach could not happen again.”<sup>297</sup> In the same order, however, the *Premera II* Court also expressed a limitation to its opinion reflecting the nuance of this issue stating “just because an underlying audit or investigatory report is not privileged, an email to an attorney seeking legal advice regarding the report would be privileged and could be redacted. A draft report sent to counsel seeking legal advice and input on the draft also would be privileged.”<sup>298</sup> In *Capital One*, following *Premera II*, the court rejected the defendant’s claim of privilege over the at-issue Mandiant report despite it being prepared for regulators, at the direction of counsel, and initially delivered to outside counsel.<sup>299</sup>

Similarly, courts have addressed skepticism over the application of the attorney-client privilege to communications substantively addressing public relations issues or concerns remains a tall order. In *Premera I*, provided insight into this issue by finding that press releases prepared by a vendor engaged by counsel was not privileged, noting “drafting press releases relating to a security breach is a business function that Premera would have engaged in, regardless of actual or potential litigation. Having outside counsel hire a public relations firm is insufficient to cloak that business function with the attorney-client privilege.”<sup>300</sup> While an attorney’s retention or other delegation of duties to a public relations firm limits the application of the privilege, the *Premera I* Court was careful to state that certain communications between in-house counsel and public relations covered certain topics “such as about possible legal consequences of proposed text or an action being contemplated by Premera, then such communications would be privileged.”<sup>301</sup> *Premera* is largely in accord with other decisions around the country.<sup>302</sup>

<sup>297</sup> . *Premera II*, 329 F.R.D. at 666.

<sup>298</sup> . *Id.* at 667.

<sup>299</sup> . *In re Cap. One Consumer Data Sec. Breach Litig.*, No. 1:19MD2915 (AJT/IFA), 2020 WL 2731238, at \*4 (E.D. Va. May 26, 2020), *aff’d*, No. 1:19MD2915 (AJT/IFA), 2020 WL 3470261 (E.D. Va. June 25, 2020).

<sup>300</sup> . *Premera I*, 296 F. Supp. 3d at 1242-43.

<sup>301</sup> . *Id.* at 1244.

<sup>302</sup> . *In re Riddel Concussion Reduction Litig.*, No. 13-7586, 2016 WL 7108455, at \*7 - \*8 (Dec. 5, 2016) (finding communications between in-house lawyers and other non-legal employees were not privileged because they involved “messaging” concerns and not legal issues.); *Amway Corp. v. Procter & Gamble Co.*, No. 1:98-CV-726, 2001 WL 1818698, at \*5 (W.D. Mich. 2001) (overruling privilege objections as to certain documents and communications exchanged between in-house counsel and other senior members of non-legal departments because, for example, certain documents related only to the defendant company’s “public relations strategy, which included the possibility of filing lawsuits.”).



## b. Pre-Incident Considerations

The line between business and legal advice is often particularly hard to judge before any incident or litigation has occurred. During these “business as usual” periods, outside counsel is less likely to be involved in communications and courts may struggle to determine whether an in-house lawyer is communicating in a legal or business capacity. Undoubtedly, in-house lawyers field questions and communications from various sectors of their organizations on a day-to-day basis which may or may not relate entirely to legal advice. In the context of data privacy and cybersecurity, organizations frequently engage in preventative conduct that involves legal and non-legal departments intersecting, communicating, and addressing and resolving issues and concerns. Whether communications around these activities are deemed privileged will largely depend on the face of each communication, the specific context, and the applicable jurisdiction. Nonetheless, there are several practical steps that in-house counsel can take to preserve or bolster the application of the attorney-client privilege in the pre-incident context:

- Educating business colleagues that the attorney-client privilege does not shield a particular communication from disclosure simply because a lawyer is copied on the communication;
- Making the legal purpose—and the provision of legal advice—the centerpiece of the communication, rather than implicit in the text or an afterthought;
- Ensuring that any security vendors that are assisting in the provision of legal advice are engaged by the legal department, rather than the business unit, and working only under the direction of counsel;
- Carefully limiting the recipients of the communication, excluding those who are not employed by the company or working under the instruction of counsel; and
- Cautioning employees to avoid forwarding any privileged communications, including by providing them to regulators, insurers, vendors, customers, or other third-parties.

## c. Post-Incident, Pre-Litigation Considerations

After a data security incident occurs, in-house counsel will want to be particularly careful with their communications to maintain the attorney-client privilege.

Beginning with the most immediate steps following a data incident, in-house counsel should be cognizant of the details surrounding their organization’s relationship with any consultants hired to respond to the incident. Which department of the business hires the outside consultant can influence whether communications with that consultant are privileged. For example, if the IT department hired a forensic consultant to investigate the breach, courts are less inclined to apply the attorney-client privilege to communications between the legal department and that consultant. Conversely, if the

Formatted: Normal



legal department hires the consultant, courts are more likely to find the privilege exists. Critically, in some jurisdictions, a privilege assertion may nevertheless be rejected if the legal department is not the department paying the consultant. Thus, in-house counsel should ensure the legal department both retains and compensates the consultant from the legal budget, rather than the business unit.

In addition, in-house counsel should carefully monitor the scope of work for the consultant. To the extent the scope of work focuses on remediating the data breach, communications with that consultant are less likely to be privileged. Conversely, if the scope of work clearly outlines the purpose of the engagement is for the consultant to provide technical advice to the legal department to expressly assist with the provision of legal advice by the legal department, courts are more inclined to find application of the attorney-client privilege. See *supra*.

Likewise, in-house counsel should exercise care with respect to their communications with other third-parties who may be involved in the response to a security incident. For example, in-house counsel's communications directly with any insurance companies may not be considered privileged, depending on the applicable jurisdiction. And, to the extent in-house counsel is asked to work with external public-relations firms, those communications are unlikely to be privileged as courts typically view public-relations work as an inherently business activity. Likewise, if the security incident involves a third-party vendor, in-house counsel will need to exercise significant care in communicating with the vendor, given the absence of any attorney-client relationship. By taking an active role in the investigation or communicating extensively with the breached entity, in-house counsel runs the risk of moving into a business-oriented role that could compromise subsequent claims of attorney-client privilege.

Beyond strategically engaging consultants, in-house counsel should also consider the creation of a "facts-only" summary or timeline related to the data incident. Since the attorney-client privilege only protects legal advice—not facts—from disclosure, outlining the key information related to the breach and disclosing it in some form may be the simplest way to avoid costly or protracted disputes should litigation ensue. This consideration is particularly important where regulatory agencies are increasingly requiring organizations in varying industries to promptly disclose data incidents and supplement those disclosures as post-incident investigations progress.<sup>303</sup> In-house counsel should be aware of the company's various reporting requirements and the fact

<sup>303</sup> . See Security and Exchange Commission's Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure Proposed Rule, 2022-39 (Mar. 9, 2022), <https://www.sec.gov/news/press-release/2022-39>.



that the corporation's disclosures to regulatory authorities will likely be the subject of a discovery request in litigation.

#### d. Considerations After Litigation

As noted above, several privilege issues will inevitably come to the forefront, and present complicated issues for the parties and the Court – including communications with in-house counsel, outside counsel, third-party investigators, public relations personnel (within and outside the company), and regulators. From a practical standpoint, the parties should consider some steps to prevent a devolution into costly tangential motion practice regarding communications and items that will likely be subject to discovery requests.

For example, in federal cases, the parties may wish to acknowledge these incipient privilege issues at the initial Rule 26 conference with the court and ask for a precise *format* and *timing* of a *privilege log*. Without guidance, a log may come late in discovery, after depositions or damage models are already under consideration. Motions to compel further productions, or re-depose witnesses, and extend deadlines, may follow to the chagrin of the parties and the court. Further, an agreed-upon format for the log may preempt tedious and repetitive communications about the supposed sufficiency of the log. In addition, the decision on log formatting and timing would join ESI protocols, protective orders, and clawbacks under Fed. R. Evid. 502(d) as the customary items the litigants and the court would resolve at or near the initial conference.

Regarding *log format*, it is important to consider the log's purpose. Judge Paul Grimm of the District of Maryland has explained that "in order for the court to determine whether the attorney-client privilege was properly asserted regarding a particular document, the court must make the following fact determinations:

(1) the asserted holder of the privilege is or sought to become a client; (2) the person to whom the communication was made (a) is a member of the bar of a court, or his subordinate and (b) in connection with this communication is acting as a lawyer; (3) the communication relates to a fact of which the attorney was informed (a) by his client (b) without the presence of strangers (c) for the purpose of securing primarily either (i) an opinion on law or (ii) legal services or (iii) assistance in some legal proceeding, and not (d) for the purpose of committing a crime or tort; and (4) the privilege has been (a) claimed and (b) not waived by the client."<sup>304</sup>

That means any log that is used should provide sufficient information to address those factors before the letter (or email) writing reaches a fever pitch. Not surprisingly,

<sup>304</sup> *Victor Stanley, Inc., v. Creative Pipe, Inc.*, 250 F.R.D. 251, 265 (D. Md. 2008).



the District of Maryland has guidelines for logs served in response to requests for production or interrogatories that addresses these factors.<sup>305</sup> Judge David Waxse set out similar elements that must be present in a privilege log back in the early 2000s. These include: 1) a description of the document; 2) the general subject matter of the document; 3) the date of the document; 4) the author of the document, whom s/he works for, their title and whether they are counsel; 5) each recipient of the document, their employer, titles, and whether they are counsel; 6) the purpose of preparing the document; 7) the number of pages of the document; 8) the specific basis for withholding the document; and 9) any other pertinent information necessary to establish the elements of the asserted privilege.<sup>306</sup>

There are practical benefits to just creating such a log. A party that may otherwise be inclined to rashly log an item, must slow down and spend more time with the document. This may reveal a weak legal argument, or that another document outside of the scope of the privilege has already revealed the information, or simply that the document is so innocuous to the case that it is not worth the trouble. Meanwhile, the log recipient may abandon any thoughts of moving to compel.

The other component for early resolution is the *timing and frequency* of log production. While Federal Rule of Civil Procedure 26 describes the basis for withholding discovery responses, it does not state when a privilege log must be produced. Logs that arrive late are often the source of contentious motions and accusations of “sandbagging,” when it may simply be non-production items were forgotten about and left to accumulate. An earlier review by more senior reviewers of documents set aside for withholding as privilege or work product may inspire different choices and permit better, more informed advocacy. A stipulation between the parties as to when the initial log must be produced, and the time after a production when the corresponding log (if any) must follow, can prevent privilege log trifles from pestering a magistrate judge or special master. The timing should be flexible and correspond to the anticipated production in a matter, and the parties can agree to revisit, much as done with search terms or additional document custodians.

\* \* \*

Having considered how courts have employed and presumably will continue to employ traditional principles of attorney-client privilege and work-product protection to analyze privilege/protection claims in the CI context, the Commentary next seeks to

**Formatted:** Indent: First line: 0", Don't suppress line numbers

**Formatted:** Font: Not Italic

<sup>305</sup> . See <https://www.mdd.uscourts.gov/sites/mdd/files/LocalRules.pdf> at App. A, p. 120.

<sup>306</sup> . Hill v. McHenry, No. CIV.A. 99-2026-CM, 2002 WL 598331, at \*3 (D. Kan. Apr. 10, 2002); Simmons Foods, Inc. v. Willis, No. 97-4192-RDR, 2000 WL 204270, at \*5 (D. Kan. Feb. 8, 2000); see also *In re Denture Cream Prods. Liab. Litig.*, No. 09-2051-MD, 2012 WL 5057844, at \*9 (S.D.Fla. Oct.18, 2012).

**Formatted:** Normal



address whether such application of traditional principles adequately promotes the policy rationales favoring and disfavoring the discoverability of CI.

## D. THE PATH FORWARD

Because discovery of CI is such a novel issue, it is not surprising that existing law fits imperfectly among many of the issues discussed in the previous Part regarding application of the attorney-client privilege and work-product protection to CI. Accordingly, Section 1 of this Part critically assesses the protections the current regime apparently provides and fails to provide to CI. Section 2 then considers various proposals for adapting existing attorney-client privilege and work-product protection law, or developing entirely new protections, in the CI context, and the tradeoffs those proposals present. We believe the existing regime has significant problems in the CI context that evolution of existing doctrines and/or development of new doctrines could address. First, as discussed in Sections 2.a and 2.b below, we believe the current regime's undesirable chilling effect on conducting frank and pointed analyses of (or even undertaking) various cybersecurity measures, coupled with its undesirable incentive for a data holder to put cybersecurity decision-making largely in the hands of the data holder's lawyers, calls for enacting a qualified—but not an absolute—stand-alone cybersecurity privilege under which CI would enjoy some measure of protection against discoverability, whether or not lawyers were sufficiently involved in its creation to qualify the CI in question for the attorney-client privilege and/or work-product protection. Second, as discussed in Section 2.c below, because of the significant hazards—including the risk of waiver—for data holders in sharing CI with law enforcement, and the public interest in prompt and complete knowledge about cybersecurity incidents, we propose that state and federal law recognize a “selective waiver” doctrine providing that, under certain specified circumstances, a data holder's disclosure of CI to law enforcement would not waive any privilege that might otherwise be claimed as to that CI in future civil litigation.

### 1. A Critical Assessment of the Existing Regime

An all-things-considered judgment about the merits of existing attorney-client privilege and work-product protection law in the CI context requires a consideration of many factors. These include (in no particular order): (1) the data holder's interests, as a crime victim and potential defendant in future civil litigation and/or regulatory enforcement actions; (2) law enforcement's (and the public's) interest in apprehending the criminal actors and preventing future crimes by the same actors and/or using the same techniques; (3) the privacy interests of individuals whose information has been or might be compromised by the incident; (4) the public's interest in and regulators' responsibility for enforcing the law and ensuring that entities that collect protected

**Formatted:** English (United States), Highlight

**Formatted:** No page break before, Don't suppress line numbers, Hyphenate

**Formatted:** English (United States)

**Formatted:** Don't suppress line numbers

**Formatted:** Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5", Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Normal



information have appropriate incentives to adopt legally required security and privacy protections; and (5) everyone's interest in seeing that justice is done.

These varying interests cut in different and sometimes conflicting ways.

*Data holders:* Typically, data holders will want a legal regime that prevents forced disclosure of CI to its actual or potential adversaries in a litigation or regulatory enforcement context. Even where it makes sense from a data holder's perspective to share CI with one or more of those adversaries, the data holder will want to make that decision on its own terms, rather than have the law require disclosure.

*Law enforcement:* The interests of criminal law enforcement tend to favor disclosure of CI, at least to law enforcement. Criminal law enforcement will need some access to CI to find clues about potential wrongdoers, even if criminal law enforcement is much more interested in misconduct by hackers than misconduct by data holders.

*The public:* The interests of the public are as varied as the public itself. To some extent, the public whose information is in the hands of data holders may want access to the data holders' CI, to make better decisions about sharing information with the data holder in the future. On the other hand, to the extent data holders will be better able to protect sensitive information if CI is not exposed, the public itself may be protected by having that CI under wraps.

*Regulators:* A regulator's interest in enforcing the law will almost always argue in favor of more rather than less access to CI. CI contains critical clues about a data holder's legal compliance, and a regulator is practically working blind if it is unable to view that information.

*Affected individuals:* Similarly, the interests of individuals whose personal information may have been, or may be vulnerable to being, compromised in a cyberattack will almost always argue in favor of more rather than less access to CI. As CI contains critical clues about a data holder's compliance with any potentially applicable legal regime that imposes a cybersecurity duty in regard to personal information, such individuals will want access to CI to evaluate and pursue claims that the data holder violated that duty.

*Justice:* The legal system is meant to produce just results, which the system tries to accomplish by generally permitting broad discovery of legally relevant facts (suggesting greater access to CI), but then creating an exception that protects attorney-client privileged and work-product protected communications and documents from disclosure (suggesting less access to CI).

**Formatted:** Space Before: 0 pt, After: 0 pt, Add space between paragraphs of the same style, Don't suppress line numbers

**Formatted:** Normal



Part C shows that whether CI is protected from disclosure under the current regime hinges largely on two broad factors: (1) the type and extent of involvement by attorneys; and (2) the extent to which information was created or procured predominantly for purposes of obtaining legal advice or in anticipation of litigation. This tight focus on the role of attorneys and the connection to legal obligations, and especially litigation, is predictable given that we are discussing a set of protections designed to facilitate candid discussions between attorneys and their clients and to facilitate effective legal representation in an adversary system.

**Formatted:** Space Before: 0 pt, Don't suppress line numbers

The rigid structure of the rules governing the attorney-client privilege, and even the somewhat more flexible approach that recognizes exceptions to work-product protection, however, largely preclude any balancing of the interest in effective legal representation against the other, similarly significant, interests that cybersecurity litigation implicates. That same rigid structure also ties any expansion or reduction of these protections in the cybersecurity context to a set of concerns that, at best, occasionally and largely incidentally overlap with the important objectives of incentivizing the adoption of robust and resilient cybersecurity measures and protecting all concerned against criminal cyberattacks.

**Formatted:** Don't suppress line numbers

a. Perverse Incentives Created by the Existing Regime

Ideally the rules for disclosure of CI would promote robust cybersecurity practices and policies. Companies should do what they reasonably can to protect information and computer networks, and the law should help them do that.

**Formatted:** Outline numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75", Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

Given the limited protections against disclosure the existing regime affords to CI, companies may think twice before conducting the type of risk assessments that are essential to proper security, but that they otherwise are not required to do. And even where, after thinking twice, companies decide to do such a risk assessment, the existing regime could have a chilling effect on how frank and pointed the assessment, and the company's response to the assessment, turns out to be. A risk assessment may well reveal shortcomings in the company's security posture. With the law as it stands, an organization could not be reasonably confident that the results of a risk assessment will be protected from disclosure in litigation. These concerns may lead companies to entirely forgo non-legally-required risk assessments, or be less than thorough in creating or responding to risk assessments, both those that are legally required and those that are not. While such behaviors may be desirable and understandable from the perspective of protecting the company against legal exposure created by the risk assessment, they are assuredly undesirable from the perspective of making the company's cybersecurity efforts as efficacious as possible.

The counterargument that the existing CI disclosure regime operates to promote better cybersecurity practices assumes the precise opposite: organizations are more likely

**Formatted:** Normal



to expend sufficient resources and take proactive measures to prevent data breaches because their security planning and implementation processes will be closely scrutinized in litigation if they suffer a breach. Which assumption is correct ultimately is an empirical question, the answer to which almost certainly will shift over time and likely depends on the relative maturity of an organization's cybersecurity posture.

Risk assessment activities have substantial operational components, because they are intended to create, test, and improve security policies and practices. Distinguishing between the core operational activities and activities arguably conducted for the purpose of seeking legal guidance is the central factor in determining whether and to what extent attorney-client privilege or work-product protection will apply to any given CI.<sup>307</sup> Moreover, pre-incident risk assessment activities typically are not initiated in response to a specific or reasonably foreseeable threat of litigation, which makes extending work-product protection to them next to impossible.

At the same time, these reports, or the information they contain, often are essential to determining whether an organization has taken reasonable measures to protect confidential and personal information. They are highly relevant to the core issues in data-breach litigation and investigations and frequently contain information that would be difficult or impossible for regulatory authorities or litigants to obtain in other ways.

While the example of risk assessments well illustrates the perverse incentives the existing regime creates regarding the creation of CI, those perverse incentives extend to *any* CI that discloses a company's mental impressions, conclusions, opinions, assessments, evaluations, or theories concerning its cybersecurity posture, a cyberattack on the company, or its actual or potential actions in anticipation of, or in response to, a cyberattack. The more frank and pointed companies are when they generate such CI, the more efficacious their cybersecurity efforts would be expected to be. But the current regime potentially chills companies from generating such frank and pointed CI because, except to the extent attorney-client privilege or work-product protection can validly be claimed as to the CI in question, the current regime allows such CI to be discovered and used against the company in question by regulators and private litigants intent on building a case that the company's cybersecurity efforts were legally insufficient.

Pre-breach activities most clearly illustrate the view that existing privilege and work-product law creates perverse incentives in the CI context. The law punishes companies that fail to engage in everyday risk assessments—a future adversary will surely argue that risk assessments are a bare minimum of adequate security. But then again, the law

---

<sup>307</sup> See *In re Target Corporation Customer Data Security Breach Litigation*, 2015 WL 6777384 at \*2 (D. Minn. Oct. 23, 2015) (rejecting claims of attorney client or work-product protection for emails from Target's CEO that "merely update[d] the Board of Directors on what Target's business-related interests were in response to the breach").

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Normal, Justified, Space Before: 3 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: 0.25", Right + 0.38", Left

**Formatted:** Font color: Black

**Formatted:** Normal



creates legal risk for companies that engage in routine risk assessments—the results may see the light of day, to the company’s detriment. These conflicting incentives emerge directly from the fact that CI protection law and cybersecurity law are motivated by divergent goals.

To be sure, these perverse incentives are not as relevant after a breach. For one thing, responding to a known data breach is always a business imperative and often a legal one, so the perverse incentives are far less likely to result in a “do nothing” approach in the post-breach context than they are in the pre-breach context. Moreover, post-breach CI is frequently generated specifically with the guidance of outside counsel and in anticipation of litigation. Thus, treating the discoverability of post-breach CI under the guise of the influence of lawyers and litigation is at least less unrealistic for post-breach situations. A majority of the few cases in this area confirm this assessment: in the *Arby’s*, *Target*, *New Albertson’s*, and *Genesco* cases, courts protected almost all the CI in dispute from disclosure based on counsel’s involvement in the creation of that CI.<sup>308</sup> *Premera*, however, is a recent important exception that underscores the substantial uncertainty regarding the scope of disclosure protection even in the post-breach context and even where counsel is involved in the creation of the CI in question.<sup>309</sup> Even in the post-breach context, then, the current regime gives companies reason for concern that anything and everything they do or say in their breach response efforts can potentially be used against them in a court of law, whether or not a lawyer has guided those efforts. That risk may make companies

<sup>308-308</sup> *Id.* (denying plaintiffs’ motion to compel with respect to all documents except a few post-breach emails updating the Board of Directors on Target’s “business related interests . . . in response to the breach”); *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 194 (2014) (barring discovery of all contested documents except those connected to “remedial measures that Genesco took in response to” the breach); see also *New Albertson’s, Inc. v. MasterCard Int’l*, No. 17-04410, slip op. at 11–12 (Idaho 4th Dist. Ct., Ada Cty., May 31, 2019) (denying motion to compel as to all contested information, noting that certain underlying data had already been produced); *In re Arby’s Restaurant Group, Inc. Data Sec. Litig.*, No. 1:17-cv-00514, at 2–3 (N.D. Ga. Mar. 25, 2019) (denying discovery except as to certain underlying information used by cybersecurity consultants). Moreover, to the extent post-incident CI is not protected by the attorney-client privilege or work-product protection, it may nevertheless in many cases be inadmissible as a “subsequent remediation measure” under Federal Rule of Evidence 407 and its state analogs insofar as it relates to the company’s efforts to remediate the breach. See FED. R. EVID. 407 (“When measures are taken that would have made an earlier injury or harm less likely to occur, evidence of the subsequent measures is not admissible to prove negligence, culpable conduct, a defect in a product or its design, or a need for a warning or instruction.”). This aspect of the existing regime arguably reduces or eliminates whatever disincentive companies otherwise might have to take remediation measures in the wake of a data security incident.

<sup>309-309</sup> *Premera I*, 296 F. Supp.3d 1230 (D. Or. 2017) (rejecting defendant’s assertion that several categories of documents, including a forensic investigator’s report, prepared post-breach after outside counsel was hired to investigate, were not protected work product because they served a primarily business purpose); see also *Premera II*, 329 F.R.D. 656, 666 (D. Or. 2019) (similar).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



more circumspect than they otherwise would be about what internal statements they make and what internal actions they take in the course of their breach response efforts, and such circumspection could make those efforts slower and less effective than they otherwise would have been.

The post-breach context sometimes raises another perverse incentive. Ideally the rules for disclosure of CI would promote robust cooperation between the victims of criminal cyberattacks and the criminal law enforcement authorities responsible for investigating such crimes and catching the perpetrators. Yet under the limited protections the existing regime affords against disclosure of attorney-client privileged and work-product protected materials to third parties resulting in a waiver of the privilege or protection as to other third parties, cyberattack victims may be reluctant to disclose privileged or protected CI to law enforcement. Such cyberattack victims may justifiably be concerned that such disclosures will waive as to their actual and potential litigation and regulatory adversaries the privilege/protection that the CI otherwise would have enjoyed. To the extent such concerns result in criminal law enforcement authorities being denied access to CI that would have assisted their efforts to bring cyberattack perpetrators to justice (and/or delaying access while the victim figures out a “workaround” to share the CI without waiving the privilege or protection), the current regime will have operated against, rather than in support of, the goal of promoting robust cooperation between those authorities and the victims of the crimes they are investigating.

#### b. The Disadvantages of Involving Counsel in Creating CI

Courts addressing the protectability of CI have distinguished between reports developed under the direction of counsel (especially outside counsel) for purposes of legal advice or litigation, and those directed by security professionals. As a result, a consensus is emerging that to the extent that organizations want to shield CI from being discovered in litigation, they should seek to “cloak” all pre- and post-incident cybersecurity work under privilege and/or work-product protection by retaining outside counsel or using inside counsel to hire and direct these efforts.

There are some obvious disadvantages to so closely linking CI protection to attorney involvement. Specifically, the practice raises several practical and analytical problems:

*Risk That Work Will Not Be Protected.* Even when counsel that is retained to provide legal advice and/or in anticipation of litigation with regard to a company’s cybersecurity conducts or commissions the activities that generated the CI in question, the risk remains that those activities will be viewed by a court as primarily operational rather than legal, and therefore the CI is not protected from disclosure (as was the case with respect to several categories of CI in the *Premiera* decisions). This risk is heightened in the pre-incident context because, as noted above, the

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Space Before: 0 pt, After: 0 pt, Add space between paragraphs of the same style, Don't suppress line numbers

Formatted: Normal



activities that generate CI are not tied to any specific pending or anticipated legal action or investigation. Some have argued that the increasingly pervasive risk of a breach strengthens the case that all security-planning activities are tied to assessing legal and regulatory risks, but no court has yet embraced that view. Moreover, that view undermines a core premise of both the work-product protection and the attorney-client privilege that courts can and should carefully distinguish between operational activities and legal advice and strategy when applying those doctrines. Routinely involving counsel in more data-security-related activities, especially activities with little or no concrete legal dimension, increases the risk that some or all of the CI generated by such activities will not be protected under either doctrine.

*Increased Cost.* Involving counsel, in particular outside counsel, in generating CI often increases the costs of the activity in question. Retaining outside counsel incurs fees; involving inside counsel redirects resources.

*Potential Duplication.* Even where an organization involves counsel to strengthen the case for protection of CI, there inevitably will be some duplication between the operational and legal processes. The dual track process that was used in the *Target* litigation is a prime example.

*Inappropriate Expertise.* Inside and outside counsel may not always be the best qualified to lead many cybersecurity activities. The internal information-technology personnel or an outside security firm is a more appropriate choice to lead the effort in some instances.

#### c. The Disadvantages of Depriving Law Enforcement of Access to Privileged/Protected CI

To the extent that data holders withhold from criminal law enforcement authorities attorney-client privileged or work-product protected CI relevant to a cyberattack (or delay providing CI until they can figure out a “workaround” to share the CI without waiving its privilege or protection), law enforcement’s efforts to investigate the attack could be significantly hampered. Such CI, either pre- or post-attack, is highly likely to provide detailed insights into the cybersecurity measures the attacked entity had in place, the vulnerabilities in those measures that the attacker exploited, and the data the attacker succeeded in compromising by means of those vulnerabilities. Such insights could be extremely valuable to the authorities investigating the crime and, just as important, quite difficult for those authorities to obtain from any source other than the privileged/protected CI. Depriving authorities of access to that CI, or delaying their access, thus stands to have a substantial negative impact on their investigatory efforts.

**Formatted:** Space Before: 0 pt, Add space between paragraphs of the same style, Don't suppress line numbers

**Formatted:** Space Before: 6 pt, Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Normal



#### d. To What Extent the Current Regime Promotes Relevant Interests

Predictably, when it comes to protecting (or not protecting) CI from disclosure, the interests of data holders, law enforcement, the public, civil regulators, and individuals affected by a cyberattack cut in different and sometimes opposing ways. For data holders, the current regime may create incentives to avoid creating potentially damaging CI<sup>310</sup> that could be used by a litigation adversary or a regulator to impose liability. Those same risks incentivize structuring information security programs to protect as much information as the current regime allows, even where doing so involves the above-mentioned negatives of incurring the additional cost of retaining counsel, potentially duplicating other information security efforts, and placing leadership of certain information security efforts in the hands of lawyers rather than technologists. At the same time, the relative difficulty of protecting CI created at the pre-breach stage and the still uncertain scope of privilege and work-product protection for even post-breach CI arguably should incentivize robust and proactive security efforts to avoid the heightened risk of liability and minimize the negative effects of disclosure. However, the potential discoverability of CI may discourage companies from conducting assessments of their security posture over and above those that are legally required, and in the post-breach context—where efforts to address the breach are normally a business imperative and often a legal one—the potential discovery of CI may cause companies to be unduly circumspect regarding the internal statements they make and internal actions they take in the course of their breach response efforts, making those efforts slower and less effective than they would have been had the companies not been worried about the chance of their post-breach CI being discovered.

Data holders' and criminal law enforcement authorities' interests, in theory, should largely align. Many data breaches are the result of criminal activity where data holders are the victim and therefore should have an interest in disclosing information necessary to identify and apprehend the perpetrator. But the pervasive risk of civil liability and/or penalties imposed by a civil regulator following a security incident, and the risk of privilege waiver, especially the possibility for a broad subject-matter waiver, cuts strongly in favor of strictly limiting the information shared with law enforcement to non-privileged/protected CI and may disincentivize data holders from involving law enforcement at all when a breach occurs. Even where a concern about waiver does not result in withholding attorney-client privileged or work-product protected CI from law

---

<sup>310-310</sup> For example, often there is a misperception that engaging in a security assessment will be futile at best because it will be too expensive to meaningfully address any security gaps and counterproductive at worst because the assessment itself will provide damaging evidence in potential future litigation. Likewise, some regulators have reported incidents where there is reason to believe that an entity involved in a breach has taken steps to actively avoid documenting the results of a forensic investigation specifically to avoid creating potentially damaging CI.

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



enforcement, it sometimes complicates the sharing of such CI. Data holders may request a formal subpoena before sharing such CI, so as to enhance the argument that the disclosure was compulsory and thus did not effect a waiver; data holders also may want to take additional time to separate privileged from non-privileged CI, again so as to reduce the risk of a waiver being found. To the extent law enforcement does not view data holders as adversaries, it may be inclined to allow data holders to take whatever steps appear necessary to protect CI from disclosure to others.

Civil regulators and plaintiffs present still different issues. These parties seek to enforce the law against data holders and therefore are both interested in CI and more likely to have requests for CI rebuffed. Companies, however, may have strategic incentives to disclose otherwise protected CI to regulators in the course of an investigation—for instance, in hopes that their cooperation will bring about a lighter sanction.<sup>311</sup> In addition, through pre-lawsuit subpoenas, civil regulators have tools for seeking CI that are not available to private plaintiffs. Nonetheless, the possibility that a private civil action will accompany an investigation, and the clear risk that disclosure in a regulatory investigation likely will waive privilege and work-product protection, combine to create significant incentives for data holders to resist disclosure of CI to regulators as much as possible.

Private plaintiffs lack the pre-litigation tools of civil regulators in seeking disclosure of CI. As the discussion in Part C explains, if defendants carefully structure post-incident analyses of security incidents, in particular by retaining counsel to direct those processes, they should be able to protect from disclosure much of the CI generated by those post-incident activities. On the flip side, the few decisions analyzing application of attorney-client privilege and work-product protection in this context suggest that courts will carefully distinguish between documents that are intended to assist in providing legal advice and/or preparing for litigation and those that are created for strategic and business purposes. Moreover, most pre-incident documents will be difficult to protect from disclosure, thus giving access to a potentially large amount of CI.

### e. The Unique Importance of Cybersecurity and Cybercrime

American businesses and government agencies are under cyberattack twenty-four hours a day, seven days a week, from criminal third parties, and the federal government has declared this global cybercrime wave a compelling national security concern, particularly in the area of critical infrastructure. In this context, any regime regarding the discoverability of CI that creates disincentives for companies to engage in behavior that

---

<sup>311-311</sup> See Eric J. Gorman and Brooke A. Winterhalter, *Protecting Attorney-Client Privilege and Attorney Work Product While Cooperating with the Government: Strategies to Minimize Risks During Cooperation (Part Two of Three)*, 3:4 CYBERSECURITY LAW REPORT (2017).

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



could enhance their network security, or interferes with law enforcement's efforts to catch the third-party criminals, arguably poses particularly significant threats to the national economy and public safety. Under this line of argument, broader protections regarding the discoverability of CI are warranted in the cybersecurity context. At the same time, it is arguably more important in the cybersecurity context than in other public protection contexts for regulators and private litigants to be able to obtain companies' documents and communications so that laws governing cybersecurity can be enforced and companies have appropriate incentives to enhance the security of their networks. Under this line of argument, while the current regime's limited protections on the discoverability of a company's documents and communications might be acceptable in the context of enforcing laws as to the physical safety of consumer products, the cleanliness of the environment, and other potential dangers to public health and safety, those limits are not acceptable in the more important context of protecting the public against the economic and intangible (e.g., emotional) injuries people may incur from the misuse of their personal information.

The unique importance of cybersecurity and cybercrime raises the question whether the current regime's limited protections, by means of the attorney-client privilege and work-product protection, on the discoverability of a company's documents and communications, while acceptable in some other contexts, should either be broadened or narrowed in the cybersecurity context. In the section that follows, we assess some proposals under which the current regime might be modified to account for the unique importance of cybersecurity and cybercrime.

## 2. Proposals for Modifying the Current Regime

As discussed above, the current regime for determining the discoverability of CI makes the creation of CI more expensive for those who seek to ensure it will be protected from disclosure, and chills companies from creating the sort of CI that would be most efficacious in furthering their cybersecurity efforts. At the same time, in many cases this model puts the creation of such documents in the wrong hands—attorneys know a lot about cybersecurity law, but perhaps not as much about other aspects of cybersecurity. In addition, even where it would be beneficial for law enforcement to view some CI, the current regime makes such disclosure less likely by increasing a data holder's liability exposure when it decides to disclose such information. These disadvantages may pose a greater threat to the public in the cybersecurity context than in other contexts because of the particularly compelling national interests in protecting the networks of American businesses and government agencies, catching cybercriminals, enforcing cybersecurity laws, and thereby protecting members of the public against injuries from the misuse of their personal information. All of these considerations warrant at least some

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Font color: Black

Formatted: Font color: Black

Formatted: Normal



consideration of whether an alternate regime should potentially govern the discoverability of CI.

In spite of the limitations just identified, the existing regime has some clear benefits. Most notably, because it is grounded on relatively settled attorney-client privilege and work-product protection, the current regime provides a fairly predictable framework within which to assess the actions that are likely to lead to documents and communications being protected, or not, from discovery. The various proposals for modifying the existing regime in the CI context discussed here inevitably bring with them uncertainty, simply because there are no precedents explaining precisely how the protection will work in this context.

a. Absolute Stand-Alone Cybersecurity Privilege Rejected

The unique issues that data breaches raise have led some to call for an independent, unqualified cybersecurity privilege as to at least some CI. The basic premise is that cybersecurity investigations raise a similar set of concerns and require the same kind of confidential relationship that privileges in other contexts protect, such as attorney-client, therapist-patient, and others.<sup>312</sup> As discussed below, the unique mix of interests implicated by the increasing and pervasive risk of a data breach provides several persuasive arguments in favor of recognizing a new privilege in this area. But the conflicting nature of the relevant interests also provides counterarguments in favor of the status quo. At minimum, these conflicting interests counsel against making such a privilege unqualified and instead support careful calibration, including significant qualifications permitting disclosure of some otherwise protected CI under the right circumstances.

The case for an unqualified stand-alone cybersecurity privilege rests on the complex mix of concerns and the issues identified above: (1) the dramatic increase in cybersecurity attacks has created a significant and growing public interest in both preventing data breaches and ensuring prompt discovery and remediation of breaches when they occur; (2) existing privileges, including the attorney-client privilege, fail to adequately protect the full range of documents produced by a robust, proactive cybersecurity program against disclosure in litigation; and (3) the net result creates perverse incentives for organizations to tailor their efforts in ways that will reduce potential disclosure in litigation rather than pursue the most thorough and effective prevention and remediation measures. This situation, combined with the unique importance of cybersecurity and

<sup>312</sup> See, e.g., Jeff Koseff, *The Cybersecurity Privilege*, 12:2 I/S J.L. & POL'Y FOR INFO. SOC'Y 261 (2016). Koseff develops the most extended argument in favor of an independent privilege for cybersecurity investigations. He proposes that courts should recognize a broad, unqualified privilege for all legal cybersecurity activities under Federal Rule of Evidence 502 or that Congress and state legislatures should do so through statute. *Id.* at 298–303.

**Formatted:** Outline numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75", Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Normal



cybercrime, it can be argued, creates a compelling case for a new privilege that closely tracks the justifications for, and hence the unqualified nature of, other common-law privileges, including the attorney-client privilege.<sup>313</sup>

As noted above, the case for an unqualified cybersecurity privilege is premised on the contestable assumption that the risk of disclosure in litigation creates disincentives for entities to develop robust and effective cybersecurity policies and practices. The opposite view assumes that these incentives align relatively well under the current regime because the substantial risk of disclosure of CI should make organizations more likely to expend sufficient resources and take proactive measures to prevent data breaches, because their security planning and implementation processes will be closely scrutinized in litigation if they suffer a breach. Which assumption is correct ultimately is an empirical question, the answer to which almost certainly will shift over time and likely depends on the relative maturity of an organization's cybersecurity posture.

Equally important, an unqualified cybersecurity privilege would take no account of the offsetting policy considerations just identified, including the data owner's interest in recourse for an entity's failure to take legally required security measures, and the risk that a lack of transparency would substantially frustrate the ability of regulators to enforce existing cybersecurity laws. For these reasons, we believe any proposal for a stand-alone cybersecurity privilege should include qualifications on the privilege, including some restrictions on the CI that could qualify for the privilege, as well as some qualification that would permit opposing parties to obtain protected information under certain circumstances.

#### b. Proposed Qualified Stand-Alone Cybersecurity Privilege

We believe any stand-alone cybersecurity privilege should include the following features and qualifications:

- Workable standards (and limits) on what CI could qualify for the privilege
- Some ability to require disclosure (at least in a redacted form) of CI that qualifies for the cybersecurity privilege and is not otherwise privileged where a substantial need can be shown by the party seeking disclosure
- Documentation by the party asserting the privilege sufficient for an opposing party and the court to determine the basis for the privilege and to challenge that assertion

---

<sup>313</sup> *Id.* at 285–98. Notably, this article goes on to recognize that an absolute privilege may not be feasible and argues that in such a case “a qualified privilege would be an acceptable starting point.” *Id.* at 303. As the author states in the article, while he would prefer an absolute privilege, even a qualified privilege “would help to encourage companies to invest in cybersecurity work and increase the likelihood that the cybersecurity professionals’ work product would be protected from discovery.” *Id.*

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Space Before: 0 pt, After: 0 pt, Add space between paragraphs of the same style, Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



The attributes of a qualified stand-alone privilege just described track the kind of qualified protection provided to trial preparation materials by the work-product doctrine. But the existing work-product doctrine is unlikely to extend to the pre-incident context because of the “in anticipation of litigation” requirement. And even in the post-incident context, existing work-product doctrine requires some involvement of a lawyer in the creation of the document or communication in question for the protection to apply, whereas the idea of any stand-alone cybersecurity privilege, be it “broad” or “nuanced,” is to eliminate the protectability of CI being dependent on legal involvement.

Apart from its being limited to materials generated in anticipation of litigation, the work-product doctrine is a better model than the attorney-client privilege for a stand-alone cybersecurity privilege because unlike the attorney-client privilege, a requesting party can access otherwise protected documents where it can demonstrate both (a) substantial need and (b) undue burden in obtaining substantially equivalent information. One approach for developing a qualified stand-alone cybersecurity privilege would be to apply something akin to work-product protection to the CI context by eliminating or softening the work-product doctrine’s requirement that materials must be created “in anticipation of litigation;” for instance, by reframing the requirement as “in anticipation of or in response to a cyberattack.” This could happen through recognition of the endemic and pervasive risk of cyberattacks that would permit companies to assert protection for pre-incident and post-incident CI or some subset of them regardless of litigation concerns or what involvement lawyers had in creating it.

Having said that, a qualified stand-alone privilege that extended to *all* documents and tangible things prepared in anticipation of or in response to a cyberattack would potentially create a presumptive protection from discovery for any and every document concerning a company’s cybersecurity efforts. This would include ordinary-course documents such as computer-generated logs and the results of automated vulnerability and anti-virus scans that do not in and of themselves disclose or reflect the *human* analyses, evaluations, and decisions that the current regime arguably chills and/or weakens. Addressing the concerns created by the current regime does not necessitate affording such ordinary-course documents enhanced protection against discovery. Rather, those concerns can be addressed by limiting any such enhanced protection to documents and tangible things that reflect a person’s (or its representative’s) mental impressions, conclusions, opinions, assessments, evaluations, or theories concerning a cyberattack on that person, or the person’s actual or potential actions in anticipation of or response to a cyberattack—in much the same way that Federal Rule 26(b)(3)(B) affords enhanced work-product protection to documents reflecting such mental impressions and the like.

Formatted: Space Before: 0 pt, Don't suppress line numbers

Formatted: Don't suppress line numbers

Formatted: Normal



Taking all of the foregoing into account, we propose that a qualified stand-alone cybersecurity privilege use the language of Federal Rule 26(b)(3) as a starting point and provide as follows:

Materials Prepared in Anticipation of or in Response to a Cybersecurity Threat

(A) *Documents and Tangible Things*. Ordinarily, a person may not utilize legal process to compel or require production of documents and tangible things that are prepared in anticipation of or in response to a cybersecurity threat by or for another person or its representative (including the other person's attorney, consultant, surety, indemnitor, insurer, or agent) and that are within the protection from disclosure set forth in Paragraph (B) below. But those materials may be discovered if:

- (1) they may otherwise be compelled or required to be produced by means of legal process under applicable law; and
- (2) the person seeking production shows it has substantial need for the materials and cannot, without undue hardship, obtain their substantial equivalent by other means.

(B) *Protection Against Disclosure*. The protection against disclosure created by this rule shall extend only to the mental impressions, conclusions, opinions, assessments, evaluations, or theories of a person or its representative concerning (i) a cybersecurity threat or (ii) that person's actual or potential actions in anticipation of or in response to a cybersecurity threat. A court or other body having appropriate jurisdiction shall uphold a person's refusal under this rule to produce documents and tangible things that are prepared in anticipation of or in response to a cybersecurity threat only to the extent necessary to protect against disclosure of such mental impressions, conclusions, opinions, assessments, evaluations, or theories.

(C) *Information Withheld*. When a person withholds from production otherwise producible information by claiming that the information is subject to protection as material prepared in anticipation of or in response to a cybersecurity threat, the person must:

- (1) expressly make the claim; and
- (2) describe the nature of the documents or tangible things not produced or disclosed — and do so in a manner that, without revealing the protected information itself, will enable the person seeking production to assess the claim.

**Formatted:** Space Before: 0 pt, After: 0 pt, Add space between paragraphs of the same style, Don't suppress line numbers

**Formatted:** Space Before: 0 pt, Don't suppress line numbers

**Formatted:** Don't suppress line numbers

**Formatted:** Normal



#### (D) Definitions

(1) “Cybersecurity threat” has the meaning given the term in section 102(5) of the Cybersecurity Information Sharing Act of 2015 (CISA), including the definition of the related term “information system,” given in section 102(9) of CISA.<sup>314</sup>

Any stand-alone cybersecurity privilege modeled on the work-product doctrine need not, in our view, include a more liberal undue-burden/substantial-need exception than the work-product doctrine’s version of that exception. To begin with, much of the CI generated by a company will not fall within the above draft rule’s limited presumptive protection against disclosure because it will not disclose a person’s mental impressions and the like, and thus will not satisfy the requirements of Paragraph B of the proposed rule. Moreover, while we recognize that some kinds of CI within the draft rule’s presumptive protection against disclosure will be essential and difficult to replicate through other evidence, the recent discussion of the undue-burden/substantial-need exception in the *Experian* case illustrates how the equivalent exception under our proposed rule can enable plaintiffs to obtain such CI when necessary.<sup>315</sup> There, the court denied plaintiffs access to the forensic report created by the defendants’ outside expert *only* because it recognized that the plaintiffs could readily replicate the report themselves, since the report relied solely on server images that the plaintiffs could obtain in discovery.<sup>316</sup> By contrast, under both the work-product doctrine and the proposed

<sup>314</sup> CISA’s definitions fit the scope of activity we intend the qualified privilege to cover and also would allow for judicial interpretations of CISA’s definitions to provide relevant authority for interpreting the scope of the privilege. We reproduce the full text of the relevant sections below.

##### Section 102(5) CYBERSECURITY THREAT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term “cybersecurity threat” means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION.—The term “cybersecurity threat” does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

##### Section 102(9) INFORMATION SYSTEM.—The term “information system”—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

<sup>315</sup> See Order Denying Motion to Compel Production of Documents, *In re Experian Data Breach Litigation*, No. SACV 15-01592 AG (DFMx), (C.D. Cal. May 18, 2017).

<sup>316</sup> *Id.* at 5.

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



qualified stand-alone cybersecurity privilege, where an organization generates materials that otherwise would be protected by the doctrine/privilege, but an opposing party has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain a substantial equivalent by other means, the party generating the materials could be required to provide that information to the opposing party.

In addition to providing a balanced alternative to an unqualified stand-alone cybersecurity privilege, a qualified stand-alone cybersecurity privilege modeled on the work-product doctrine could result in parties more selectively asserting the blanket protection of attorney-client privilege to pre- and post-incident CI and would provide courts with a more nuanced set of tools to deal with competing arguments over the application of privilege in the cybersecurity context.

One concern raised in response to the public comment version of this proposal is that courts will need to determine what constitutes a “cybersecurity threat” as well as “mental impressions, conclusions, opinions, assessments, evaluations or theories” of nonlawyers, which could result in ancillary discovery disputes and inconsistent decisions by different courts.<sup>317</sup> As with any new legal rule, it will take some time for parties and courts to ascertain the precise boundaries of the qualified privilege, and disputes inevitably will arise in some instances.

The proposed language deliberately draws on existing legal models to reduce the risk of confusion. Moreover, as we discuss at length above, there already are substantial uncertainties surrounding the application of traditional attorney-client privilege and work-product protection in the cybersecurity context. This privilege could eliminate many of those disputes by providing a clear avenue to protect materials as to which parties otherwise might seek to stretch the boundaries of those doctrines and, thus, has the potential to reduce confusion in the aggregate.

Having said all that, while a qualified stand-alone cybersecurity privilege would provide more limited protection than an unqualified privilege modeled on traditional attorney-client privilege principles, and thereby better address the mix of interests implicated in the cybersecurity context, such a privilege would still protect a much greater range of CI from disclosure than does the current regime. The argument in favor of a qualified standalone cybersecurity privilege thus still rests on the contestable proposition that some currently unprotected CI really should be protected, even though it does not qualify for the attorney-client privilege or work-product protection. The new rule also inevitably will invite ancillary disputes regarding the appropriate scope of the

<sup>317,317</sup> See Matthew Hamilton and Donna Fisher, *Evaluating Stand-Alone Privilege for Cybersecurity Info*, LAW360 (2019), <https://www.law360.com/articles/1168625/print?section=technology>; <https://www.law360.com/articles/1168625/print?section=technology>.

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



protection both as a general matter and in individual cases where parties will take contrary views as to whether particular CI should be protected. Ultimately, then, the argument for even a qualified stand-alone cybersecurity privilege depends on whether concerns about cybersecurity and cybercrime are both unique and substantial enough to justify drawing the protection/non-protection line differently in the cybersecurity and CI context than where the current regime draws that line in all other contexts.

We are persuaded that concerns about cybersecurity and cybercrime are sufficient to justify a qualified stand-alone cybersecurity privilege along the lines of the above draft. The key foundation for this conclusion is our belief that (1) the language of Paragraph (B) of the draft rule would result in most of an organization's CI not even qualifying for the rule's presumptive protection against disclosure in the first place, and (2) the "substantial need" exception to the privilege would prevent the privilege from being used in a fashion that would impose undue hardship on regulators and private litigants in building and bringing cases against the victims of cyberattacks.

The narrow limitations the proposed privilege would impose on the discoverability of relevant CI in such cases are outweighed by the benefits the privilege would achieve. First, the proposed qualified privilege would enable parties to take robust actions to protect themselves against and respond to third-party cyberattacks with greater (though not absolute) assurance that the CI they generate in the course of those efforts will not be used against them at some point down the road. In our view, affording parties such greater assurance treats the victims of third-party cyberattacks more fairly than does the current regime.

Second, the proposed qualified privilege would enable parties to obtain significant (though not absolute) protection against the discoverability of CI without using attorneys to lead their efforts to protect themselves against, and respond to, third-party cyberattacks. In our view, providing parties with greater discoverability protection lessens the incentive that the current regime creates for putting attorneys in charge of efforts to address being victimized by such criminal activities and/or taking other measures to avoid creating a discoverable record concerning those efforts (such as not conducting certain assessments that are not otherwise legally required, conducting such assessments less thoroughly, or not reducing them to writing). Thus, it lessens the risk that the current regime creates of those efforts being less efficacious and/or more costly than they would otherwise have been.

In this way, the proposed qualified privilege is analogous to the medical peer-review privilege recognized by the vast majority of U.S. states (although generally not by federal common law), which lessens hospitals and physicians' disincentives to thoroughly investigate medical incidents by shielding reports and other documents of their medical



staff committees in connection with such investigations from discovery.<sup>318</sup> We recognize that in *University of Pennsylvania v. EEOC*, the U.S. Supreme Court declined to recognize a qualified common-law privilege against the disclosure of confidential university faculty peer-review materials.<sup>319</sup> We also recognize that several lower federal courts have relied on the Court’s reasoning in that decision to refuse to recognize an analogous “self-critical analysis” or “self-evaluative” privilege that would protect confidential, nonfactual deliberative material such as opinions or recommendations that result from internal investigations, reviews, or audits conducted by public and private entities.<sup>320</sup>

The limited privilege we propose stands on much different footing than either the faculty peer-review process or the self-critical analysis privilege. The Supreme Court in *University of Pennsylvania* noted that confidentiality is not the norm in all faculty peer-review systems and expressed skepticism that disclosure of faculty peer reviews would actually have a chilling effect on the candidness of such reviews.<sup>321</sup> By contrast, corporations closely safeguard the confidentiality of their candid assessments of their own information security. As noted above, the current regime incentivizes companies to maintain that confidentiality by putting attorneys in charge of their efforts to address being victimized by cyberattacks and/or taking other measures to avoid creating a discoverable record concerning those efforts, thereby raising the risk that those efforts will be less efficacious and/or more costly than they would otherwise have been.

The self-critical analysis privilege requires confidentiality and, like our proposal, limits the scope of protection to nonfactual information. Public interest in thorough and candid identification and assessment of potential shortcomings within an organization also justifies both privileges. Despite these similarities, the case for a qualified CI privilege is stronger for two reasons. First, the privilege covers a very narrow and specific situation—a “cybersecurity threat” as defined by CISA—that raises a set of public interests distinct in nature and urgency from the broad range of general compliance contexts covered by the self-critical evaluation privilege. Cybersecurity threats frequently involve criminal activity and, in some cases, foreign-nation-state support or tacit approval. Attacks that result in subsequent litigation where the privilege might be invoked always involve alleged compromise of third-party private information. As a

<sup>318-318</sup> See LEONARD ET AL., THE NEW WIGMORE: A TREATISE ON EVIDENCE § 7.8 (3d ed. 2017).

<sup>319-319</sup> 493 U.S. 182 (1990).

<sup>320-320</sup> See, e.g., *Lund v. City of Rockford*, Case No. 3-17-cv-50035, 2017 WL 5891186 (N.D. Ill. Nov. 29, 2017), at \*5–16 (relying on *Univ. of Pa. v. EEOC*, 493 U.S. 182 (1990), to reject the self-critical analysis privilege and surveying the “spotty history” of the privilege in federal court decisions).

<sup>321-321</sup> *Univ. of Pa.*, 493 U.S. at 200–01 (noting that if peer reviews are discoverable, some academics, rather than being less candid, may simply ground their evaluations in specific examples and illustrations in order to deflect potential claims of bias or unfairness).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



result, the shared public interest in fostering robust proactive and remedial measures to improve cybersecurity is arguably much stronger than for other contexts.

Second, we propose that this qualified privilege be established through legislation at the federal and state level, rather than through common law. Courts understandably are reluctant to recognize new common-law privileges and generally cite the high burden for such recognition when rejecting the self-critical analysis privilege.<sup>322</sup> Establishing the privilege through legislation removes those concerns. While it is no simple task to pass legislation, there is growing bipartisan consensus that cybersecurity is a critical national priority that requires new and creative approaches.<sup>323</sup>

Accordingly, we are persuaded that the benefits of lessening the security risk that the current regime creates, coupled with the benefits of reducing the unfair manner in which the current regime treats victims of cyberattacks, are sufficient to justify the proposed qualified privilege, given that the privilege would not in our view impose undue hardship on regulators and private litigants in building and bringing cases against the victims of cyberattacks.

#### c. Proposed “No Waiver” Rule for Criminal Cybersecurity Investigations

One partial reform proposal that would address the current regime’s disincentives for companies to share CI with criminal law enforcement is the creation of a limited form of protection against the waiver of attorney-client privilege and work-product protection for information shared in the course of a criminal investigation of a possible cybersecurity breach.

The arguments in favor of limiting waiver in this situation are not unique to the cybersecurity context. Others have advocated for a version of this protection, often called “selective waiver,” for information shared in the course of civil regulatory investigations, and federal law provides a broad protection against privilege and work-product waiver for information shared with banking regulators.<sup>324</sup> Several courts have recognized

<sup>322-322</sup> See Lund, 2017 WL 5891186, at \*5.

<sup>323-323</sup> States in particular have been very active in seeking to address these issues. Through Nov. 6, 2018, at least 22 states had passed 52 cybersecurity-related bills, and at least 35 states, D.C. and Puerto Rico introduced/considered more than 265 bills or resolutions related to cybersecurity. See *Cybersecurity Legislation 2018*, NATIONAL COUNCIL OF STATE LEGISLATURES, <http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx> (last visited Nov. 20, 2019).

<sup>324-324</sup> 2 PAUL R. RICE, ET AL., ATTORNEY-CLIENT PRIVILEGE IN THE U.S., LIMITED WAIVER — LOGIC OF LIMITED WAIVER § 9:91 (2018).

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



selective waiver on the basis that it encourages companies to fully investigate potential illegal conduct and to cooperate with regulatory agencies, thus protecting shareholders, customers, and the public.<sup>325</sup>

The majority of courts that have addressed whether to apply selective waiver in civil regulatory investigations, however, have not found either “the rationale of encouraging corporations to seek outside review of allegedly illegal corporate activities, nor that of encouraging them to cooperate with [regulatory] investigations” sufficient to justify the doctrine.<sup>326</sup> Courts that reject the doctrine note that organizations have ample incentive to seek candid advice from legal counsel regardless of whether a government regulator may require it to disclose that advice in an investigation. Moreover, the benefits an organization obtains from voluntary disclosure, in the form of more lenient sanctions resulting from an investigation, in most cases is sufficient incentive for cooperation with the regulator and not likely to be undermined by the risk of waiver of privilege or work-product protection.<sup>327</sup>

The case for selective waiver for disclosures in the course of a law enforcement investigation into a cybersecurity incident is arguably stronger than for civil regulatory investigations. The public’s interest in obtaining complete information following a cybersecurity incident extends beyond ensuring full disclosure of potential legal violations to identifying information regarding potential cyber threats and actors that could help prevent those threats from affecting other organizations, individuals, and data. Compromises of the confidentiality, integrity, or availability of information or systems frequently result from criminal conduct by a third party. Permitting the affected entity to fully disclose information regarding a potential breach to law enforcement authorities without risk of waiving attorney-client privilege or work-product protection

<sup>325-325</sup> The seminal case supporting selective waiver is *Diversified Indus., Inc. v. Meredith*, 572 F.2d 596 (8th Cir. 1977) (en banc). In *Diversified*, a corporation responded to allegations that it had paid bribes to obtain business by forming an independent audit committee and retaining outside counsel to prepare an internal report on the issue. The internal report was subsequently produced to the Securities and Exchange Commission (SEC). The Eighth Circuit held that this disclosure constituted only a “limited waiver” that did not preclude the corporation from withholding the report from private litigants on the grounds of attorney-client privilege. *Id.* at 611. The Eighth Circuit explained: “To hold otherwise may have the effect of thwarting the developing procedure of corporations to employ independent outside counsel to investigate and advise them in order to protect stockholders, potential stockholders and customers.” *Id.*; see also *United States v. Shyres*, 898 F.2d 647, 657 (8th Cir. 1990) (applying the reasoning of *Diversified*); *McDonnell Douglas Corp. v. EEOC*, 922 F. Supp. 235, 243 (E.D. Mo. 1996) (applying the reasoning of *Diversified*); *Schnell v. Schnall*, 550 F. Supp. 650, 652–53 (S.D.N.Y. 1982) (illustrating public policy of encouraging disclosure to SEC compels finding of selective waiver).

<sup>326-326</sup> RICE, *supra* note 191.

<sup>327-327</sup> See, e.g., *In re Steinhardt Partners, L.P.*, 9 F.3d 230, 236 (2d Cir. 1993); *Permian Corp. v. United States*, 665 F.2d 1214, 1221 n.13 (D.C. Cir. 1981).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



in a subsequent civil lawsuit or regulatory investigation would likely encourage such disclosures. This, in turn, could assist law enforcement in apprehending the criminal actors involved in the incident, thereby preventing that actor from similarly attacking other organizations.<sup>328</sup>

A company that is the victim of a criminal cyberattack also sits in a much different position than one faced with an investigation into potential civil liability. First, the primary incentive for sharing information with law enforcement authorities is the possibility that law enforcement will apprehend the criminal actor, even though the victim may also receive some incidental benefits from the disclosure, such as being viewed slightly more favorably by regulators and the public, and/or receiving information from law enforcement to assist the victim's investigation and remediation efforts that it otherwise might not have received if it had not cooperated. But apprehension of cybercriminals is notoriously difficult and unlikely to undo the damage from the incident in any case. Second, permitting cybercrime victims to share otherwise privileged or protected information with law enforcement without fear of waiver would lessen the disincentive to do so created by the current regime, because such sharing would not increase the victim's potential liability exposure. Similar incentives do not exist when discussing selective waiver in the context of regulatory investigations.

#### i. Statutory Models

A statute providing selective waiver of privilege and work-product protection for information disclosed to criminal law enforcement could draw on waiver protections that exist in other contexts. Congress has created statutory limits on the waiver of the attorney-client privilege in two contexts: (1) a broad protection against waiver as to submissions made to banking regulators, and (2) as discussed in part C above, a protection against waiver for specific information shared through the processes prescribed by CISA.<sup>329</sup>

<sup>328</sup> Our collective experience suggests that many organizations either do not engage law enforcement or delay engagement following a data breach for a range of reasons, including concerns about waiver of attorney-client privilege and work-product protection. Our shared intuition is that while that reluctance in most instances is not driven primarily by waiver concerns, eliminating those concerns likely will encourage at least timelier, and possibly greater overall, cooperation and information sharing. Informal discussions with several federal law enforcement personnel actively involved in cybercrime matters confirmed that, in their experience, organizations often are reluctant to share information with law enforcement, and that legal liability concerns, including potential waiver of attorney-client privilege, frequently cause delays in the ability of law enforcement to obtain information.

<sup>329</sup> Consolidated Appropriations Act, 2016, H.R. 2029, 114th Cong. (2015) (enacted).

**Formatted:** Outline numbered + Level: 1 + Numbering Style: i, ii, iii, ... + Start at: 1 + Alignment: Right + Aligned at: 0.75" + Indent at: 1", Don't suppress line numbers, Hyphenate

**Formatted:** Don't suppress line numbers

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Font: 10 pt, Font color: Black

**Formatted:** Font color: Black

**Formatted:** Normal



### Bank Examiner Waiver Protection

The protection against waiver of privilege for disclosing information to a bank examiner is provided by 12 U.S.C. § 1828(x):

- (x) Privileges not affected by disclosure to banking agency or supervisor
- (1) In general

The submission by any person of any information to the Bureau of Consumer Financial Protection, any Federal banking agency, State bank supervisor, or foreign banking authority for any purpose in the course of any supervisory or regulatory process of such Bureau, agency, supervisor, or authority shall not be construed as waiving, destroying, or otherwise affecting any privilege such person may claim with respect to such information under Federal or State law as to any person or entity other than such Bureau, agency, supervisor, or authority.<sup>330</sup>

Very few courts have interpreted this provision, and it lacks any significant legislative history. The text leaves open several important questions, including whether the bank examiner can waive an entity's privilege by disclosing the privileged material provided to it and how broadly to interpret "submission[s]," including whether material provided to a regulator during an enforcement action should be treated the same as submissions of more routine information.

Notably, bank regulators take the position that the bank-examiner regime does not merely permit, but requires, banks to disclose privileged information when requested by the regulator, given the compelling public interest in ensuring compliance with banking regulations.<sup>331</sup>

### CISA Waiver Protection

CISA creates a specific procedure for private organizations to share specific cyber threat information directly or indirectly with the Department of Homeland Security (DHS). As noted in Part C above, to incentivize voluntary information sharing with DHS, CISA provides a limited protection against waiver of privilege and other legal protections:

Section 1504(d)(1) Information Shared With Or Provided To The Federal Government:

- (1) No waiver of privilege or protection. The provision of cyber threat indicators and defensive measures to the Federal Government under this

<sup>330</sup> 12 U.S.C. § 1828(x)(1).

<sup>331</sup> See, e.g., Consumer Financial Protection Bureau Final Rule, Confidential Treatment of Privileged Information (June 28, 2012) (effective Aug. 6, 2012), 77 FR 39617 (July 5, 2012).

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Space Before: 0 pt, After: 0 pt, Add space between paragraphs of the same style, Don't suppress line numbers

Formatted: Space Before: 0 pt, Don't suppress line numbers

Formatted: Don't suppress line numbers

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Space Before: 0 pt, After: 0 pt, Add space between paragraphs of the same style, Don't suppress line numbers

Formatted: Space Before: 0 pt, Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



subchapter shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.<sup>332</sup>

As a practical matter, CISA's limits on the information that can be shared and the procedure required for sharing make it unlikely that either attorney-client privilege or work-product protection would apply to any shared information. The statute requires the entity sharing the information to strip out personally identifiable information and other protected information for its protections to apply. Nonetheless, like the bank-examiner provision, this protection recognizes the broad public interest in facilitating prompt and voluntary disclosure of certain kinds of CI—here cybersecurity threat information—to cybersecurity regulators and the need to adapt existing legal regimes, at least in limited ways, to protect and advance that interest.

#### ii. “No Waiver” Proposal and Explanation

We are persuaded that concerns about cybersecurity and cybercrime are sufficient to justify adoption of a “no waiver” rule in the cybersecurity context that would apply to disclosures made by a cyberattack victim to the criminal law enforcement authorities investigating the attack. A key foundation for this conclusion is our belief that such disclosures do not significantly undermine the policy rationale for finding a waiver of the attorney-client privilege and/or work-product protection in certain circumstances where the privileged/protected material in question is disclosed to a third party. Specifically, a frequently cited reason for such third-party disclosures being deemed to waive the privilege/protection to which the disclosed information otherwise would have been entitled is that the party making the disclosure usually has a self-interested motive in doing so—the self-interest usually being that the disclosing party believes the disclosure will advance its position in the proceeding in which the disclosure is being made.<sup>333</sup> In that circumstance, it is not perceived as “unfair” to find that the disclosure waived the privilege/protection both as to the recipient of the information and as to other third parties; and both as to the disclosed information and other related information that otherwise would have qualified for the privilege/protection.<sup>334</sup> As the saying goes, finding

<sup>332-332</sup> 6 U.S.C. § 1504(d)(1).

<sup>333-333</sup> See *In re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289, 302 (6th Cir. 2002) (rejecting selective waiver on grounds that permitting such a selective waiver would “transform[] the attorney-client privilege into ‘merely another brush on an attorney’s palette, utilized and manipulated to gain tactical or strategic advantage.’” (citing *In re Steinhardt Partners, L.P.*, 9 F.3d 230, 235 (2d Cir. 1993)).

<sup>334-334</sup> See *Permian Corp. v. United States*, 665 F.2d at 1214, 1221 (refusing to recognize selective waiver because “the client cannot be permitted to pick and choose among his opponents, waiving the privilege for some and resurrecting the claim of confidentiality to obstruct others, or to invoke the privilege as to communications whose confidentiality he has already compromised for his own benefit. . . . The attorney-client privilege is not designed for such tactical deployment.”).

Formatted: Don't suppress line numbers

Formatted: Don't suppress line numbers, Hyphenate

Formatted: Don't suppress line numbers

Formatted: Font: 10 pt, Font color: Black

Formatted: Font: Times New Roman, 10 pt, Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



a waiver of the privilege/protection in that circumstance is necessary to prevent the disclosing party from using the privilege/protection “both as a sword and a shield.”<sup>335</sup> Whatever merit that policy rationale may have in the usual context of a self-interested disclosure of attorney-client privileged or work-product protected material, we do not see such a disclosure as being fairly thought of as “self-interested” when it is made by the victim of a criminal cyberattack to criminal law enforcement authorities investigating that attack, even though the victim may receive some incidental benefits from the disclosure—such as being viewed slightly more favorably by regulators and the public, and/or receiving information from law enforcement to assist the victim’s investigation and remediation efforts that the victim otherwise might not have received if it had not made the disclosure. As a result, we do not see that policy rationale as being significantly undermined by adoption of a “no waiver” rule in that circumstance. This same rationale does not exist for disclosure in regulatory investigations, where the disclosing party is waiving the privilege specifically to protect its interests.

We also do not believe that adoption of such a “no waiver” rule would impose undue hardship on regulators and private litigants in building and bringing cases against the victims of cyberattacks. To be sure, adoption of a no-waiver rule of this sort would result in regulators and private litigants being denied access to certain CI disclosed to law enforcement that, under the current regime, they would have access to. And we acknowledge that the CI in question could well be quite valuable to regulators and private litigants in the cases they are trying to build. But the reality is that even under the current regime, regulators and private litigants would in all likelihood not have access to the CI in question, because the cyberattack victim would be unlikely to disclose it to law enforcement out of concern that such disclosure would operate as a waiver of the privilege/protection as to regulators and private litigants. As a practical matter, then, we believe that adoption of a no-waiver rule will leave regulators and private litigants no worse off in their ability to obtain access to relevant CI than they are under the current regime.

Based on the above thinking, we conclude that whatever limitations such a no-waiver rule would impose on the discoverability of relevant CI in the cybersecurity context are outweighed by the benefits that such a rule would achieve. And we see those benefits as being substantial. Adoption of a no-waiver rule that would apply to disclosures made by a cyberattack victim to criminal law enforcement authorities investigating the attack would result in authorities receiving a greater flow of CI regarding the attack than is

---

<sup>335</sup> See *In re Columbia/HCA*, 293 F.3d at 307 (refusing to recognize selective waiver for work-product doctrine because, “like attorney-client privilege, there is no reason to transform the work product doctrine into another ‘brush on the attorney’s palette,’ used as a sword rather than a shield.” (internal quotation and citation omitted)).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



currently the case. Moreover, because the CI included in the increased flow is highly likely to provide detailed insights into the cybersecurity measures the attacked entity had in place, the vulnerabilities in those measures that the attacker exploited, and the data the attacker succeeded in compromising by means of those vulnerabilities, the CI could provide substantial assistance to law enforcement in bringing the perpetrators to justice. Accordingly, we are persuaded that the benefits of a no-waiver rule of this sort are sufficient to justify its adoption, given that such a rule would not in our view impose undue hardship on regulators and private litigants in building and bringing cases against the victims of cyberattacks or provide those victims with any unfair advantage in defending those cases.

We therefore propose adoption of a “no waiver” rule in the cybersecurity context containing the following language:

*No waiver of privilege or protection for information shared with law enforcement—*

The submission by any person of any information to a law enforcement agency for any purpose in connection with a potential or existing criminal investigation or proceeding by the agency regarding the potential or actual unauthorized access, or attempted unauthorized access, to computerized data or systems shall not constitute a waiver of any applicable privilege or protection provided by law or otherwise affect any privilege or protection such person may claim with respect to such information under Federal or State law as to any person or entity.

“Law enforcement agency” means any government agency that has authority to investigate or prosecute a crime regarding the potential or actual unauthorized access, or attempted unauthorized access, to computerized data or systems.

In developing this language, we carefully considered each of the following questions:

*What entities are covered.* Both the Bank Examiner and CISA statutes apply only to specific federal entities. Given the broad patchwork of cybersecurity laws, a proposed rule in this area could cover either the whole gamut of agencies that might request the relevant information or only those that more frequently conduct such investigations. For the reasons discussed in Part D.2.c, we are proposing waiver protection limited to information shared in connection with an existing or potential criminal investigation of a potential cybersecurity breach. The rationale for encouraging information sharing with law enforcement regarding a potential criminal attack applies to any law enforcement agency at both the state and federal level, and so we chose not to include a specific list of the agencies covered.

*What incidents are covered.* The operative language describing the incidents covered (“regarding the potential or actual unauthorized access, or attempted unauthorized access, to computerized data or systems”) is adapted from similar language in the

**Formatted:** Space Before: 0 pt, After: 0 pt, Add space between paragraphs of the same style, Don't suppress line numbers

**Formatted:** Space Before: 0 pt, Don't suppress line numbers

**Formatted:** Don't suppress line numbers

**Formatted:** Normal



Computer Fraud and Abuse Act (CFAA).<sup>336</sup> We looked to the CFAA as a model for defining the relevant criminal conduct related to data access that would trigger the waiver protection but updated the CFAA’s somewhat dated reference to “computers.”

The rule we have proposed extends only to incidents involving access to computer records, and not paper, because the specific problem we seek to address is the pervasive and growing risk of cyberattacks.

*What information is covered.* We propose to protect against waiver “any information” disclosed “by any person” and “for any purpose in connection with a potential or existing criminal investigation or proceeding.” This language is modeled on the similarly broad language in the Bank Examiner statute. Although the limited legislative history sheds no light on this issue, we surmise that the drafters chose not to attempt to limit the information that could be protected against waiver for two reasons: (1) the difficulty in defining the scope of information in the abstract; and (2) the relative lack of any incentive to disclose irrelevant information.

The universe of information this protection is aimed at is likely to be quite small: documents that both (1) are likely to be useful for apprehending the criminals involved and/or for other organizations to defend against similar attacks; and (2) are likely to qualify for attorney-client privilege and/or work-product protection. The imprecise nature of both the CI and the scope of privilege and work-product protection, however, combine to make it extremely difficult to define that universe in the abstract.

Equally important, we could identify no meaningful potential downside to extending the no-waiver rule broadly to “any information” otherwise meeting the statutory test. The rule we propose does not create a new privilege or substantively expand the scope of privilege or work-product protection; it merely prevents waiver of them for documents that are otherwise protected. Therefore, it does not create any incentive to disclose information that is not useful to the investigation, because doing so does not protect otherwise unprivileged or unprotected information from disclosure. To be sure, as noted above, adoption of a no-waiver rule of this sort would result in regulators and private litigants being denied access to certain CI disclosed to law enforcement that, under the current regime, they would have access to upon its disclosure. But as discussed, even under the current regime, regulators and private litigants would in all likelihood not have access to the CI in question, because the cyberattack victim is unlikely to disclose that CI to law enforcement out of concern that it would operate as a waiver of the privilege/protection as to regulators and private litigants.

*Compelled vs. voluntary disclosure.* We propose a no-waiver rule that does not compel disclosure to law enforcement. A no-waiver rule could provide, as bank regulators

---

<sup>336</sup> 18 U.S.C. § 1030 ((a) Whoever—(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— . . . ).

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Normal



contend is the case in the bank-examiner context, that a data holder is *required* to provide attorney-client privileged or work-product protected CI to the government entities covered by the statute when requested to do so, and that no waiver of the privilege/protection as to other persons or entities will result from doing so. Or it could provide that a data holder is free to decide whether to disclose information and does not risk waiver by doing so. The policy justifications and potential consequences of each approach are dramatically different. A voluntary disclosure regime would focus on the needs of data holders, seeking to address their perceived concerns with disclosing or not disclosing otherwise protected CI to the government. A mandatory disclosure regime would focus on the needs of government, seeking to address its perceived concerns with enforcing the law. While the rationale for waiver protection arguably could support mandatory disclosure, doing so would transform a protection intended to create incentives to voluntarily share information with law enforcement into a powerful tool for demanding cooperation in circumstances where there otherwise is neither a legal requirement nor a strong incentive to do so.<sup>337</sup> Our proposed rule, accordingly, does not mandate disclosure to law enforcement of attorney-client privileged or work-product protected information, but instead is limited to permitting non-waiving disclosure of such information to law enforcement in connection with a potential or existing criminal investigation and is designed to encourage greater and more timely voluntary sharing of such information with law enforcement agencies.

*Confidentiality agreement with law enforcement; subsequent disclosure by law enforcement.* A hallmark of attorney-client privileged or work-product protected documents is that they are developed confidentially and shared as narrowly as possible. One issue sometimes raised in the court decisions discussing the selective-waiver doctrine is whether the doctrine requires that the disclosing party enter into a confidentiality agreement with a regulatory agency to effectively prevent waiver and, if so, what form that agreement should take.<sup>338</sup> Our proposed rule clearly establishes that disclosure to

<sup>337-337</sup> Even the voluntary cybersecurity threat information-sharing provisions in CISA raised significant concerns over individual privacy and civil liberties because of the possibility that the Department of Homeland Security might share private information with law enforcement without a warrant. *See, e.g., CISA Security Bill Passes Senate with Privacy Flaws Unfixed*, WIRED (Oct. 27, 2015, 5:30 p.m.), available at <https://wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/>; <https://wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/>. A mandatory disclosure regime that permits law enforcement to directly demand similar information following a cyberattack would raise even stronger potential objections.

<sup>338-338</sup> *See, e.g., In re Mutual Funds Inv. Litig.*, 251 F.R.D. 185 (D. Md. 2008) (discussing *In re Doe*, 662 F.2d 1073 (4th Cir. 1981) and noting that the Fourth Circuit in that decision “explained that waiver of work

Formatted: Font: 10 pt, Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Font color: Black

Formatted: Font: 10 pt, Font color: Black

Formatted: Normal



law enforcement in connection with an existing or potential criminal investigation of a potential cybersecurity breach does not waive privilege or work-product protection. Therefore, in our view, no additional measure, including entering into a confidentiality agreement, is necessary to prevent waiver under the rule we propose. For similar reasons, in our view, subsequent disclosure of the CI would not waive the attorney-client privilege or the work-product protection, as the privilege/protection would belong to the party that disclosed the information to law enforcement, not to law enforcement. Therefore, no unilateral action taken by law enforcement (such as disclosure of that information to a third party) could operate to waive the disclosing party's privilege/protection as to that information.

*Who should adopt the rule, and how should they adopt it?* For our proposed rule to achieve its maximum benefit, it would need to provide maximum certainty to data holders that their disclosure to law enforcement of attorney-client privileged or work-product protected CI would not waive the privilege or protection in question. To maximize such certainty, our proposed rule would need to be adopted in all U.S. states and inhabited territories, in Washington, D.C., and by the U.S. federal government. While that is our recommendation, we do not believe our proposed rule has no utility unless it is widely adopted. Rather, we are saying that our proposed rule will have more utility the more widely it is adopted. In terms of how our proposed rule should be adopted, we do not think it is reasonable to expect courts to judicially adopt our proposed rule through application of common-law principles. Instead we think it will be necessary for our proposed rule to be codified by the relevant authorities, presumably by means of amendments to their existing rules of civil procedure and/or evidence.

---

product protection may occur in circumstances where the attorney 'cannot reasonably expect to limit the future use of the otherwise protected material.'" *Id.* at 187).

**Formatted:** Font color: Black

**Formatted:** Normal



## E. CONCLUSION

Through an examination of how courts have and presumably will apply traditional attorney-client privilege and work-product protection law to CI, the *Commentary* discusses whether such application will incentivize and protect CI in accordance with the policy considerations accompanying the cybersecurity context. The *Commentary's* consideration of various proposals explores the tradeoffs between the current regime and a modified one and arrives at suggesting two proposals that would remedy what appear to be issues with the current regime's operation in the cybersecurity context. As discussed above, a qualified stand-alone privilege could help address the current regime's chilling effect on conducting frank and pointed analyses of (or even undertaking) various cybersecurity measures. Second, because of the significant hazards—including the risk of waiver—for data holders in sharing CI with law enforcement, as well as the public interest in prompt and complete knowledge about cybersecurity incidents, the *Commentary* proposes that state and federal law recognize a “no waiver” doctrine providing that disclosure of CI to law enforcement would not waive any privilege or protection that might otherwise be claimed as to such CI in future civil litigation. The *Commentary* provides a roadmap to discuss these critical issues facing the discoverability and protection of CI and to provide concrete proposals for how policymakers and courts may wish to use current or new law to align the incentives with policy goals.

Formatted: English (United States)

Formatted: Don't suppress line numbers

Formatted: Font color: Black

Formatted: Normal, Indent: First line: 0.5", Space After: 12 pt, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border)

Formatted: Normal



Page 1: [1] Formatted WG11 4/11/2022 9:57:00 AM

Normal

Page 1: [2] Style Definition WG11 4/11/2022 9:57:00 AM

preface spacing

Page 1: [3] Style Definition WG11 4/11/2022 9:57:00 AM

Heading 3\_RunIn

Page 1: [4] Style Definition WG11 4/11/2022 9:57:00 AM

Outline 1

Page 1: [5] Style Definition WG11 4/11/2022 9:57:00 AM

RTP TOC Page

Page 1: [6] Style Definition WG11 4/11/2022 9:57:00 AM

RTOC Title

Page 1: [7] Style Definition WG11 4/11/2022 9:57:00 AM

RTH TblHead

Page 1: [8] Style Definition WG11 4/11/2022 9:57:00 AM

RTB Title

Page 1: [9] Style Definition WG11 4/11/2022 9:57:00 AM

RTaP TblPara

Page 1: [10] Style Definition WG11 4/11/2022 9:57:00 AM

RSU Subtitle

Page 1: [11] Style Definition WG11 4/11/2022 9:57:00 AM

RSBC Subtitle

Page 1: [12] Style Definition WG11 4/11/2022 9:57:00 AM

RQI Block Qu Ind

Page 1: [13] Style Definition WG11 4/11/2022 9:57:00 AM

RQ Block Quote

Page 1: [14] Style Definition WG11 4/11/2022 9:57:00 AM

RNS Para No Ind S

Page 1: [15] Style Definition WG11 4/11/2022 9:57:00 AM

RNH Para No Ind H

Page 1: [16] Style Definition WG11 4/11/2022 9:57:00 AM

RND Para No Ind D

Page 1: [17] Style Definition WG11 4/11/2022 9:57:00 AM

RHH Para 1/2" 1-1/2



**Page 1: [18] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

RH Para 1" 1-1/2

**Page 1: [19] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

RB Basic

**Page 1: [20] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

R2 Para 1"D

**Page 1: [21] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

R1 Para 1"S

**Page 1: [22] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

Macro Text

**Page 1: [23] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

Revision

**Page 1: [24] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

Footnote: Font: (Default) Palatino Linotype, 12 pt

**Page 1: [25] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

RB2 Bullets

**Page 1: [26] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

RB3 Bullets

**Page 1: [27] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

RB4 Bullets

**Page 1: [28] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

RB5 Bullets

**Page 1: [29] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

RB6 Bullets

**Page 1: [30] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

RB7 Bullets

**Page 1: [31] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

RB8 Bullets

**Page 1: [32] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

RB9 Bullets

**Page 1: [33] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**

Outline 3

**Page 1: [34] Style Definition**      **WG11**    **4/11/2022 9:57:00 AM**



Outline 4

<b>Page 1: [35] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

Outline 5

<b>Page 1: [36] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

Outline 6

<b>Page 1: [37] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

Outline 7

<b>Page 1: [38] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

Outline 8

<b>Page 1: [39] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

Outline 9

<b>Page 1: [40] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

Outline 2

<b>Page 1: [41] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

TOC 9

<b>Page 1: [42] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

TOC 8

<b>Page 1: [43] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

RHS Para 1/2" S

<b>Page 1: [44] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

RHD Para 1/2" D

<b>Page 1: [45] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

RSB Subtitle

<b>Page 1: [46] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

RT Title

<b>Page 1: [47] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

RBU Bullets: Font: (Default) Palatino Linotype, 12 pt

<b>Page 1: [48] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

RBN Basic No Space

<b>Page 1: [49] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

alpha list: Tab stops: Not at 0.5"

<b>Page 1: [50] Style Definition</b>	<b>WG11</b>	<b>4/11/2022 9:57:00 AM</b>
--------------------------------------	-------------	-----------------------------

Num List



**Page 1: [51] Style Definition      WG11    4/11/2022 9:57:00 AM**

\_Subhead5: Indent: Left: 2.75", Hanging: 0.25"

**Page 1: [52] Style Definition      WG11    4/11/2022 9:57:00 AM**

\_Subhead4

**Page 1: [53] Style Definition      WG11    4/11/2022 9:57:00 AM**

\_Subhead3: Indent: Hanging: 0.25"

**Page 1: [54] Style Definition      WG11    4/11/2022 9:57:00 AM**

\_Subhead2: Indent: Hanging: 0.25"

**Page 1: [55] Style Definition      WG11    4/11/2022 9:57:00 AM**

\_Subhead1: Indent: Hanging: 0.25"

**Page 1: [56] Style Definition      WG11    4/11/2022 9:57:00 AM**

\_BulletList2-TXT: Indent: Left: 1"

**Page 1: [57] Style Definition      WG11    4/11/2022 9:57:00 AM**

\_BulletList1-TXT: Indent: Left: 0.25"

**Page 1: [58] Style Definition      WG11    4/11/2022 9:57:00 AM**

\_BulletList2-FN

**Page 1: [59] Style Definition      WG11    4/11/2022 9:57:00 AM**

\_BulletList1-FN

**Page 1: [60] Style Definition      WG11    4/11/2022 9:57:00 AM**

App1Bullets

**Page 1: [61] Formatted      WG11    4/11/2022 9:57:00 AM**

Don't suppress line numbers