EW
ELLIS&WINTERS LLP

Presented by:

Alex M. Pearce
Sean Fernandes

Alex M. Pearce

Alex Pearce concentrates his practice in Privacy and Data Security law. He partners with organizations to provide strategic and practical guidance on matters that implicate domestic and international privacy and data security considerations.

Alex's broad and varied experience includes counseling clients on compliance with state and federal privacy, consumer protection and breach notification laws; designing and implementing global data protection compliance strategies; negotiating cloud computing, data license and data sharing agreements, and representing clients in disputes centering on privacy and data security issues. He frequently writes and speaks on privacy and data security and is an editor of What's Fair?, a blog on the law of unfair trade practices.

Alex has been certified by the International Association of Privacy Professionals (IAPP) as a Certified Information Privacy Professional/United States (CIPP/US) and as a Certified Information Privacy Technologist (CIPT). In 2017 the IAPP recognized him as a Fellow of Information Privacy (FIP).

Alex rejoined Ellis & Winters in 2017 after serving for six years as in-house counsel for SAS, a global provider of analytics, business intelligence and data management software and services. While practicing at SAS he served as the company's lead Privacy Counsel. In that role he managed the company's global privacy program and advised on domestic and international privacy and data security issues arising throughout the company's operations.

During his initial tenure at Ellis & Winters, from 2007 through 2010, Alex maintained a complex litigation practice and represented clients in state and federal trial and appellate courts. His diverse litigation experience includes representing technology companies in complex commercial contract and intellectual property disputes.

Alex earned his law degree from Stanford Law School. Following law school he served as a law clerk for the Honorable Milton I. Shadur in the United States District Court for the Northern District of Illinois, and then began his career in private practice at Winston & Strawn LLP in Chicago. He earned his undergraduate degree in political science from Wake Forest University.

A native of Santa Fe, New Mexico, Alex lives in Raleigh with his wife and two daughters. He is a locally competitive runner and enjoys racing distances from the 5K to the marathon.

Professional Associations and Memberships

- International Association of Privacy Professionals (IAPP)
- Sedona Conference Working Group 11, Data Security and Privacy Liability - Drafting Team on Data Security and Privacy Issues in Civil Litigation
- Sedona Conference Working Group 6, International Electronic Information Management, Discovery and Disclosure
- North Carolina Bar Association, Privacy and Data Security Committee
- North Carolina Bar Association, Future of Law Committee
- ABA Section of Litigation, Privacy and Data Security Committee
- ABA Section of Antitrust Law, Consumer Protection and Privacy and Information Security Committees
- Carolina Privacy Officials Network

Admissions

- North Carolina, 2007
- United State District Courts
    - Western District of North Carolina (2009)
    - Middle District of North Carolina (2009)
    - Eastern District of North Carolina (2007)

Sean Fernandes

Sean Fernandes is a member of the firm's Privacy & Data Security and Litigation practice groups. In both practices, he counsels clients on compliance and works to resolve lawsuits when they arise.

In his Privacy & Data Security practice, Sean has advised clients on compliance with state and federal privacy, consumer protection and breach notification laws, including HIPAA, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and state identity theft laws. He is also an active member of the Privacy and Data Security Committee of the ABA's Litigation Section. In 2017, Sean became certified by the International Association of Privacy Professionals (IAPP) as a Certified Information Privacy Professional/United States (CIPP/US).

In his Litigation practice, Sean handles complex cases in state and federal courts, representing clients in matters ranging from contract disputes to class actions. Sean advises clients on compliance with consumer product, labor and employment, and insurance regulations and also counsels higher education institutions on matters ranging from Title IX compliance to student employment regulations. Sean also remains active in *pro bono* matters in which he has counseled education non-profits on regulatory and compliance issues.

Sean earned his law degree from the University of Chicago law school, where he was a Victor McQuistion Scholar. He earned his undergraduate degree from UNC-Chapel Hill, where he graduated with honors and distinction. Prior to law school, Sean worked in Student Affairs at UNC-Chapel Hill as a Community Manager.

Sean is from Asheville and lives in Raleigh with his wife. In his free time, he enjoys running on the American Tobacco Trail and the Raleigh Greenways. In the summer, he can also be found surfing on North Carolina beaches.

Professional Associations and Memberships

- American Bar Association
  - Litigation Section, Privacy and Data Security Committee
  - Young Lawyers Division
- North Carolina Bar Association
  - Education Law Section
  - Young Lawyers Division
  - Privacy and Data Security Committee
- International Association of Privacy Professionals (IAPP)

Admissions

- North Carolina, 2016
- United State District Courts
    - Western District of North Carolina (2016)
    - Middle District of North Carolina (2016)
    - Eastern District of North Carolina (2016)
- United States Courts of Appeals
    - Fourth Circuit

Data Breach Response: Reducing Litigation Risk

February 2, 2018
Alex M. Pearce[1]
Sean W. Fernandes
Ellis & Winters LLP
Raleigh, North Carolina

When a company experiences a data breach, it can suffer a variety of operational, financial, reputational, and legal consequences. These can include expensive and time-consuming forensic investigations, negative publicity, and inquiries and enforcement actions by government regulators.

In addition to—and often as a direct result of—these other consequences, companies often face private litigation. Spurred by large class-action settlements in data-breach lawsuits such as those brought against Anthem, Home Depot, and Ruby Corp. (the owner of the Ashley Madison adultery website), the plaintiffs' bar is increasingly focused on suing breached companies.

Data-breach plaintiffs, which may include a company's customers, business partners, and employees, may pursue any of several different legal theories. These can include negligence, misrepresentation, breach of contract, unfair and deceptive trade practices, and asserted violations of state and federal statutes.

A company's ability to defend itself against these claims can depend on actions it takes both before a breach occurs and in its immediate aftermath. The success of its defense also depends heavily on how the company responds after a complaint has been filed.

This manuscript provides an overview of common claims asserted by data-breach plaintiffs, and the issues these claims present. It then offers some practical steps that companies and their counsel can take in each of phase of the data-breach lifecycle to increase the likelihood of a successful defense.

I. Common Claims Asserted in Data-Breach Litigation

Private civil actions brought against companies that have suffered a data-security breach can assert a range of claims. The claims can vary according to the

[1] Portions of this manuscript contain material published on What's Fair?, a blog on the law of unfair trade practices, privacy, and data security. Mr. Pearce and his colleagues Stephen Feldman, George Sanderson, and Jeremy Falcone serve as the blog's editors.

claimants, the nature of the data, and the industry in which the company operates. These claims typically fall into four broad categories.

A. Tort Claims

Plaintiffs often assert tort claims in data-breach lawsuits. Negligence and misrepresentation-based claims are among the most common.

Negligence claims typically assert that the company owed plaintiffs a duty to exercise reasonable care in protecting information that the company received from or about them. According to this theory, the company breaches that duty when it fails to implement reasonable safeguards to protect that information.

A key threshold requirement for negligence claims is the existence of a duty owed to the plaintiff. Plaintiffs typically try to satisfy this requirement in one or both of two ways.

First, plaintiffs may allege that the company owed them a common law duty of care to protect their information. Because the existence of such a duty depends on state law, courts have reached different results as to whether this duty exists.[2] Courts are more likely to find such a duty where there is a direct relationship between the plaintiff and the breached company—such as might exist when the individual is a customer or employee.[3] If, by contrast, there is only an indirect relationship—for example in which the breached company acts as a service provider to the company that originally collected the information from the plaintiff—it may be harder to satisfy this element.[4]

---

[2] *Compare Sackin v. TransPerfect Glob., Inc.*, No. 17 CIV. 1469 (LGS), 2017 WL 4444624, at *4 (S.D.N.Y. Oct. 4, 2017) (holding that under New York law, employers have a common-law duty to take reasonable precautions to protect the PII that they require from employees) *and In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014), *order corrected*, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014) (finding that California and Massachusetts law imposed a common law duty to safeguard a consumer's confidential information entrusted to a commercial entity) *with USAA Fed. Sav. Bank v. PLS Fin. Servs., Inc.*, 260 F. Supp. 3d 965, 969–70 (N.D. Ill. 2017) (observing that Illinois does not recognize a common law duty to safeguard an individuals' personal information or protect it from disclosure) *and Dittman v. UPMC*, 2017 PA Super 8, 154 A.3d 318, 325, *reargument denied* (Mar. 20, 2017), *appeal granted*, 170 A.3d 1042 (Pa. 2017) (reaching same conclusion under Pennsylvania law).

[3] *See, e.g., Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 167 (1st Cir. 2011) (reversing dismissal of negligence claims brought by customers of a national grocery chain whose credit card information was stolen in a data breach); *Sackin*, 2017 WL 4444624, at *5 (declining to dismiss negligence claim brought be employees against an employer who suffered a data breach involving the employees' personal information).

[4] *See, e.g., Willingham v. Glob. Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702, at *17–18 (N.D. Ga. Feb. 5, 2013) ("[C]ourts have found that no duty of care exists in the data breach context where . . . there is no direct relationship between the plaintiff and the defendant.").

Second, plaintiffs may assert negligence or negligence per se claims that allege the breached company violated a specific duty imposed by statute. To that end, plaintiffs have pointed to statutes such as Section 5 of the Federal Trade Commission Act[5] and the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations.[6] Although those statutes do not themselves provide a private right of action, plaintiffs sometimes allege that the statutes establish the standard of care for purposes of a negligence claim. The viability of these claims can vary depending on the statute at issue and on the law of the state where the claim is asserted.[7]

In addition to negligence claims, data-breach plaintiffs often assert misrepresentation-based tort claims. These claims typically allege that the company represented that it employed safeguards to protect the plaintiff's information, but that those representations were misleading because the safeguards were insufficient. Plaintiffs can base these claims on statements in a company's advertising, privacy policy, or customer agreements. A key threshold issue in these claims is whether the plaintiff justifiably relied on the alleged misstatements.[8]

B. Contract Claims

Data-breach plaintiffs also commonly assert contract-based claims that rely on promises—express or implied—made by companies to protect the plaintiffs' information. The grounds for these claims depend heavily on the relationship between the plaintiff and the breached company.

Where the plaintiff is a customer of the breached company, these claims can rely on security-related promises made by the company in its privacy policy, terms

---

[5] 15 U.S.C. § 45.

[6] 42 U.S.C. § 1320d et seq.; 45 C.F.R. § 164.306.

[7] *See, e.g., Veridian Credit Union v. Eddie Bauer, LLC,* No. C17-0356JLR, 2017 WL 5194975, at *10-12 (W.D. Wash. Nov. 9, 2017) (finding that under Washington law, duty element of negligence claim could be predicated on Washington state statute governing the liability of businesses to financial institutions for failing to protect payment card data, but not on Section 5 of the FTC Act); *Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.*, 314 Conn. 433, 459, 102 A.3d 32, 49 (2014) (holding that HIPAA and its implementing regulations could be used to inform the standard of care applicable claims of negligence in the disclosure of patients' medical records).

[8] *See, e.g., In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 975 (S.D. Cal. 2014), *order corrected,* No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014) (dismissing negligent misrepresentation claim stemming from breach of online service because alleged misrepresentations were made after plaintiffs purchased console allowing access to service); *In re Target Corp. Customer Data Sec. Breach Litig.,* 64 F. Supp. 3d 1304, 1312 (D. Minn. 2014) (dismissing negligent misrepresentation claim where plaintiffs failed to sufficiently allege reliance on defendant's alleged misrepresentations by omission about its data security systems).

of use, or customer agreements.[9] To that end plaintiffs often allege that the price paid for a company's goods or services included a payment for the company's data-security promises. These plaintiffs argue that they "overpaid" or were deprived of the "benefit of the bargain" when the company fails to protect their information against a data breach.[10]

Employees of breached companies also often rely on contract-based theories. Their claims may be based on express terms in an employment agreement or an employer's internal security and privacy policies.[11] These claims might also be based on implied contract theories. These claims contend that by requiring employees to provide sensitive personal information as a condition of employment, companies implicitly—even if not expressly—agree to take reasonable measures to protect that information against unauthorized disclosure.[12]

Finally, contract-based claims feature prominently in business-to-business data breach lawsuits. Examples include litigation between breached retailers and financial institutions whose customers' payment cards are affected by a data breach[13] and between breached service providers and their corporate customers.[14]

C. Consumer Protection and Unfair Trade Practices Claims

State consumer protection and unfair trade practices laws provide another common source of claims in data-breach lawsuits. These statutes can be particularly attractive to data-breach plaintiffs where they provide enhanced remedies such as treble damages or the recovery of attorneys' fees.[15]

---

[9] *See, e.g., Kuhns v. Scottrade, Inc.,* 868 F.3d 711, 717 (8th Cir. 2017) (addressing investor's breach of contract claims premised on securities brokerage firm's brokerage agreement, which incorporated brokerage's privacy policy and security statement).

[10] *See, e.g., In re VTech Data Breach Litig.*, No. 15 CV 10889, 2017 WL 2880102 (N.D. Ill. July 5, 2017) (plaintiffs, buyers of internet-connected toys whose personal information was compromised in a data breach, asserted breach-of-contract claims based on seller's failure to provide bargained-for security measures).

[11] *See, e.g., Enslin v. Coca-Cola Co.*, No. 2:14-CV-06476, 2017 WL 1190979, at *12-13 (E.D. Pa. Mar. 31, 2017) (appeal pending) (considering breach-of-contract brought by employee based on employer's alleged violation of corporate code of conduct and information technology policies).

[12] *See, e.g., Sackin*, 2017 WL 4444624, at *6.

[13] *See, e.g., Cmty. Bank of Trenton v. Schnuck Mkts.*, 210 F. Supp. 3d 1022, 1044 (S.D. Ill. 2016).

[14] *See, e.g., Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc.*, No. 1:12-cv-2513-SCJ, 2014 WL 11164763 (N.D. Ga. Feb. 18, 2014).

[15] *See, e.g.,* N.C. Gen. Stat. §§ 75-16 & -16.1 (allowing persons injured by unfair or deceptive trade practice to maintain an action for treble damages and for courts to award attorneys' fees to the prevailing party).

Some states' laws provide that the violation of a separate breach notification or data security statute is automatically an unfair trade practice.[16] For example, a recent opinion in the Western District of North Carolina held that the disclosure of employees' social security numbers in a phishing scheme establishes an unfair and deceptive trade practices claim.[17]

When such "per se" theories are unavailable, Plaintiffs might instead argue that the failure to secure their personal information falls within these statutes' general prohibition on "unfair" or "deceptive" practices. These types of claims often find support in enforcement actions brought by the Federal Trade Commission under Section 5 of the FTC Act.

Even though Section 5 of the FTC Act does not mention data security, the FTC has for some time used its authority under that statute to bring enforcement actions against companies that fail to protect consumers' personal information.[18] In these actions, the FTC argues that the failure to protect that information constitutes an "unfair" or "deceptive" trade practice. The FTC then treats these enforcement actions—which are usually resolved through consent orders that the FTC publicizes—as a form of "common law" that tells other companies what data-security practices Section 5 requires.[19]

Private litigants have in turn sought to use this same "common law" against companies in private litigation through state unfair and deceptive trade practices statutes. Many of these statutes were modeled on Section 5 and some specifically state that they are to be interpreted the same way.

For example, in a recent decision from a federal court in Washington, the court refused to dismiss a claim under that state's consumer protection act that alleged a retailer's failure to protect the plaintiff's personal information was an unfair practice.[20] In support of that claim, the plaintiff pointed to the FTC's data security cases against other companies, and observed that Washington's consumer

---

[16] *See, e.g.,* N.C. Gen. Stat § 75-65(f) (providing that violation of security breach notification statute is a violation of section 75-1.1, North Carolina's unfair trade practices statute); Md. Code Ann., Com. Law §14-3508 (providing that a violation of Maryland's Personal Information Protection Act is an unfair or deceptive trade practice under state's Consumer Protection Act).

[17] *Curry v. Schletter Inc.*, No. 1:17-CV-0001-MR-DLH, 2018 WL 1472485, at *5-7 (W.D.N.C. Mar. 26, 2018).

[18] *See, e.g.*, Complaint, *U.S. v. VTech Electronics Ltd.*, 1:18-cv-114 (N.D. Ill.) (Dkt. No. 1); Complaint, *F.T.C. v. D-Link Corporation*, 3:17-cv-00039 (N.D. Cal.) (Dkt. No. 1); Complaint, *F.T.C. v. Bayview Solutions, LLC.*, 1:14-cv-01830-RC (D.D.C.) (Dkt. No. 1).

[19] *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia Law Review 583 (2014).

[20] *Veridian*, 2017 WL 5194975, at *12 (W.D. Wash. Nov. 9, 2017).

protection act specifically stated it was to be interpreted in light of the FTC's orders.[21]

D. Statutory claims

In addition to claims based on state unfair and deceptive trade practice statutes, data-breach plaintiffs also bring claims for violations of other state and federal statutes.

As one example, some state data breach notification statutes allow for a private right of action when a company fails to provide notification as required after a breach.[22] Plaintiffs bringing these claims, however, often have trouble showing that any failure by the company to notify is the cause of a cognizable injury.[23]

As another example, Plaintiffs have also frequently pursued claims under the federal Fair Credit Reporting Act (FCRA).[24] These claims typically involve two threshold issues: (1) whether the breached company qualifies as a "consumer reporting agency" for FCRA purposes, and (2) whether the company violated the FCRA's requirement to establish "reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes" permitted by the statute.[25] These claims have seen limited success.[26]

II. Before the Breach: Planning to Reduce Data-Breach Litigation Risk

Companies can take certain steps to reduce litigation risk before a breach ever occurs. These include (1) avoiding unnecessary representations about the company's security in external statements that could support deception or breach-of-contract claims; (2) implementing a breach-response plan that meets affected individuals' expectations and avoids creating new avenues for recover after a breach; and (3) procuring insurance coverage that provides protection both for first party losses, and third-party claims, that arise from a data breach.

---

[21] *Id.* at *13 n.14.

[22] *See, e.g.,* Alaska Stat. Ann. § 45.48.080(b); N.C. Gen. Stat. Ann. § 75-65; Va. Code Ann. § 18.2-186.6(I).

[23] *See, e.g., Rogers v. Keffer, Inc.*, 243 F. Supp. 3d 650, 663 (E.D.N.C. 2017) (dismissing claim under data breach notification statute where plaintiff could not show that any damage he suffered was caused by the lack of notification—as compared to underlying identity theft).

[24] 15 U.S.C. §§ 1681 et seq.

[25] 15 U.S.C. §§ 1681e(a).

[26] *See, e.g., Galaria v. Nationwide Mut. Ins. Co.,* No. 2:13-CV-118, 2017 WL 4987663, at *4 (S.D. Ohio Aug. 16, 2017) (dismissing data-breach plaintiffs' FCRA claim because their complaint alleged personal information was stolen by a third party, not furnished to the third party in violation of the FCRA).

A. Review Security-related Representations in Marketing and Terms of Use

As explained above, a company's representations about its privacy and data security practices can often support claims alleging breach of contract, fraud, misrepresentation, and breach of common law duties. Thus avoiding unnecessary security representations, and ensuring that any representations a company does make are well-crafted, can help a company defeat these claims in the early stages of litigation.

In one recent case, for example, an employee claimed that his employer breached its code of conduct by failing to safeguard his personal information after the company suffered a data breach. The court, however, granted summary judgment for the employer based on language of the code.[27] The court held that the following language did not establish a duty to safeguard employees' personal information:

> The Company will safeguard the confidentiality of employee records by advising employees of all personnel files maintained on them, collecting only data related to the purpose for which the files were established and allowing those authorized to use a file to do so only for legitimate Company purposes.[28]

This language, said the court, limited the scope of the company's responsibilities to (1) advising employees of the personnel files maintained on them, (2) collecting only data relevant to the purpose for which the files were established, and (3) allowing use of the files only for legitimate company purposes.[29] The term did not impose "a sweeping contractual duty" to safeguard employee data against misappropriation.[30]

As this case shows, careful drafting of security-related representations can make all the difference when plaintiffs seek to make out a breach-of-contract claim after a data breach.

B. Develop and Implement an Effective Incident Response Plan

Irrespective of the potential for data-breach litigation, companies should develop and implement an incident response plan to address the operational, regulatory, and reputational risks associated with data breaches. But recent events

---

[27] *Enslin*, 2017 WL 1190979, at *12-13.

[28] *Id.*

[29] *See id.* at *10.

[30] *Id.* at *12.

show that failing to properly execute these plans can create litigation risk beyond that which flows from the underlying breach itself.

In particular, recent consumer data-breach class actions have included claims and allegations that point to companies' failure to properly execute incident response protocols.

One of the many recent class actions filed against Equifax, for example, asserts negligence and unfair and deceptive trade practice claims that are based in part on alleged failures to "timely and accurately disclose" the breach, and to the company's "fumbling" of its response, which included publicizing a website that purported to enable consumers to determine whether they were impacted by the breach, but which did not in fact do so.[31] Consumer class actions against Yahoo! and Target contain similar allegations.[32]

As these complaints show, missteps that occur as part of a company's response to a breach can create additional litigation risk above and beyond claims premised on the breach itself.

C. Evaluate and Optimize Cyber Insurance Coverage

Cyber insurance is an essential consideration in an overall cyber risk management strategy. A full discussion of cyber insurance considerations is beyond the scope of this paper.

To reduce data-breach litigation risk, however, companies and their counsel would be well-advised to evaluate their existing coverage with respect to two specific issues, including whether: (a) losses associated with a data breach are covered; and (b) whether any such coverage includes third-party claims.

First, the company should determine whether and the extent to which its existing coverage will even cover a data breach. A company's commercial general liability ("CGL") policy may or may not fit the bill.

The Fourth Circuit held in a recent case that a commercial general liability ("CGL") policy applied to losses suffered in a data breach. [33] The policy-specific nature of the Fourth Circuit's analysis, however, means insureds should not assume their own CGL policy will substitute for a cyber-specific policy. Indeed, at least one

---

[31] *See generally* Complaint, *Allen, et al. v. Equifax, Inc.*, 1:17-cv-04544-CAP (N.D. Ga) (Dkt. No. 1).

[32] *See generally* Complaint, *McMahon v. Yahoo! Inc.*, 5:16-cv-05466 (N.D. Ca) (Dkt. No. 1); Consolidated Class Action Complaint, *In re Target Corporation Customer Data Security Breach Litigation*, 0:14-md-02522-PAM (D. Minn) (Dkt. No. 163).

[33] *Travelers Indem. Co. of Am. v. Portal Healthcare Sols., L.L.C.*, 644 F. App'x 245, 248 (4th Cir. 2016) (per curiam) (insurer had duty to defend insured against data-breach class action where CGL covered "publication" of private medical information).

other court has found a CGL policy with different wording did not require the insurer to provide a defense in a data-breach case.[34]

Second, the company should carefully evaluate whether any coverage that might cover a data breach extends both to first-party losses and third-party claims. As coverages vary widely between insurers and between policies, companies must carefully evaluate whether and the extent to which their policies include third-party liability coverage commensurate with any litigation risk the company may face as a result of a data breach.

III. Post-Breach Response

Actions a company takes in the immediate aftermath of a breach can also impact its ability to defend against litigation after the dust settles. In particular, companies should (1) take care to preserve evidence associated with the breach and the company's investigatory and remedial efforts, (2) preserve—to the greatest extent possible—the protections of the attorney-client privilege and work product doctrines; and (3) notifying affected parties as required by applicable law.

A. Conduct a Forensically-sound Investigation to Preserve Evidence and Avoid Side Issues in Litigation

After a breach occurs, the company's primary task is to move quickly to secure its system and to remediate vulnerabilities that may have caused the breach. In many, if not most, cases it is also advisable to engage help from forensic investigators to help determine the source and scope of the breach.

However the company carries out its investigation, it is critical to avoid modifying or destroying system logs and other forensic evidence that might later become relevant in litigation. Failing to preserve this sort of evidence can inhibit the company's ability to defend itself. It can also lead to spoliation motions and the attendant sideshows they create.[35]

B. Preserve the Attorney-client Privilege

Engaging counsel immediately after discovery of the breach and involving them in the post-breach response is critical to preserve attorney-client privilege over

---

[34] *See Zurich American Ins. Co. v. Sony Corp. of America*, 2014 WL 3253541, at *1 (N.Y. Sup. Ct. Feb. 24, 2014).

[35] *See Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, No. 3:10 CV 1590, 2013 WL 2151779, at *1 (N.D. Ohio May 16, 2013), *aff'd,* 774 F.3d 1065 (6th Cir. 2014) (considering, but ultimately denying, spoliation motion in data-breach case because moving party failed to adequately specify particular log files or datasets that were relevant to its case).

the breach investigation. Some recent cases that address the issues of privilege and work product in the context of data breaches provide helpful lessons for litigants.

One important lesson is to properly structure the company's investigation and response efforts to avoid mixing non-privileged activities with privileged ones. In litigation arising from the well-known breach that Target suffered in 2013, Target used a two-track approach to investigating the breach: one track designed to address payment card industry requirements and another track designed to aid Target and its counsel in addressing the company's legal exposure. A class of financial institution plaintiffs sought discovery of Target's internal data breach investigation materials.[36] One basis for seeking the discovery was that the financial institutions and Target had used the same vendor to perform both tracks of its investigation. The trial court, however, held that a substantial majority of the information from Target's investigation was privileged because of the methodical "two-track investigation" approach that Target took. The court held that materials created by the "legal track," whose purpose was to help Target obtain legal advice and prepare its defense, were privileged. The court paid particular attention to the fact that Target had carefully separated the team working on that track from the team working on behalf of the financial institutions.[37]

Outside counsel should also be closely involved in hiring breach response vendors such as forensic investigators and consultants—and should if possible hire them directly. In cases where the breached company hired outside counsel and outside counsel in turn hired breach response vendors, the vendors' work was found to be subject to work product protection.[38] In contrast, where the company hires the vendor directly, work product protection is less likely to extend to the vendor's work.[39]

Finally, it is important to ensure that materials sent to counsel over which an entity intends to assert privilege involve legal analysis. In data-breach litigation, some courts have held that breach response functions that a company would have performed regardless of litigation, such as "press releases, media interactions, and

---

[36] *In re Target Corp. Customer Data Sec. Breach Litig.*, No. MDL142522PAMJJK, 2015 WL 6777384, at *1 (D. Minn. Oct. 23, 2015).

[37] *Id.* at *2.

[38] *See, e.g.*, *In re Experian Data Breach Litig.*, No. 8:15–cv–01592–AG–DFM, 2017 WL 4325583 , at *2-3 (C.D. Cal. May 18, 2017) (holding that where third party forensic consultant was retained by outside litigation counsel to investigate data breach, consultant's report was protected from discovery under the work product doctrine).

[39] *See In re Premera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-MD-2633-SI, 2017 WL 4857596, at *7-8 (D. Or. Oct. 27, 2017) (holding that report prepared by third-party forensic consultant was not protected by the attorney-client privilege or the work-product doctrine where consultant had been hired by company before data breach and continued investigation of breach under same scope of work).

notices" of the breach are not privileged just because they involve an attorney.[40] A similar "dual-purpose test" has been applied for purported work product.[41]

C. Notify as Necessary (But Carefully)

One of counsel's fundamental tasks in representing companies that have experienced a data breach is to evaluate and advise on the notification requirements that apply under applicable data security and data-breach notification statutes.

When notification is required, the company should pay close attention to both the timing and content requirements of breach notification statutes. Violations of these statutes, including both timing and notice-content requirements, can create claims for unfair and deceptive trade practices in several states, including North Carolina.[42] And as discussed in Section II.B, delayed and late notice can create another basis for negligence claims beyond the breach itself.[43]

The content of breach notices should also be carefully crafted to avoid inaccuracies, which could create additional claims for misrepresentations, and to avoid inadvertently making damaging admissions. For example, offering free credit monitoring to affected consumers in a notice has been construed by some courts to support plaintiffs' claims that a breach poses an imminent risk of identity theft. To that end, both the Sixth Circuit and the Seventh Circuit have held that offers of free credit monitoring in a breach notice can help establish injury-in-fact for standing because they suggest some acknowledgement that a substantial risk of harm exists.[44]

IV. Defending Data-breach Litigation

After a complaint is filed, a company's success or failure can depend on key defenses that are asserted at the pleadings stage. The most common among these are lack of standing and the economic loss rule. Other related defenses—including

---

[40] *Id.* at *6.

[41] *Id.* at *8.

[42] *See, e.g.,* N.C. Gen. Stat. §§ 75-65.

[43] *See generally, e.g.*, Complaint, *Allen, et al. v. Equifax, Inc.*, 1:17-cv-04544-CAP (N.D. Ga) (Dkt. No. 1); Complaint, *McMahon v. Yahoo! Inc.*, 5:16-cv-05466 (N.D. Ca) (Dkt. No. 1); Consolidated Class Action Complaint, *In re Target Corporation Customer Data Security Breach Litigation*, 0:14-md-02522-PAM (D. Minn) (Dkt. No. 163).

[44] *See Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 694 (7th Cir. 2015). The Fourth Circuit, however, has rejected this reasoning, because it would discourage breached entities from mitigating a breach's impact. *See Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir. 2017).

especially those premised on failure to state a claim for a lack of injury, can also be successful.

A. Standing Challenges

In a typical data-breach case, individuals sue the breached company before thieves have misused their data. The alleged injury, then, is usually an increased risk of *future* fraud or identity theft.

Future harm, however, is often not enough to establish Article III standing in federal court. In *Clapper v. Amnesty International*, the U.S. Supreme Court confirmed that an alleged "future injury" constitutes an injury-in-fact—and satisfies Article III standing—only if that future injury is "certainly impending."[45]

This standard, the Supreme Court explained, does not always mean "literally certain." Instead, a court may find standing based on a showing of "substantial risk" that harm will occur, "which may prompt the plaintiffs to reasonably incur costs to mitigate or avoid that harm."

Federal courts assessing standing in recent data-breach cases have turned to *Clapper* and the "substantial risk" standard—and reached different results. These cases have created a deepening circuit split that has made the success of standing challenges difficult to predict. It also presents forum-selection issues for data-breach litigants.

In that regard, the Sixth Circuit, Seventh Circuit, Ninth Circuit, and D.C. Circuit have held that an increased risk of future identity theft is an injury sufficient to establish standing in consumer data breach litigation under *Clapper*.[46] Collectively, these cases hold that the theft of sensitive information creates a risk of identity theft that is substantial enough to satisfy Article III—even if the plaintiff does not allege that his or her personal information has been misused in a way that creates present harm.

The Second Circuit, Fourth Circuit, and Eighth Circuit, by contrast, have rejected arguments that the increased risk of future harm to consumers whose data has been compromised in a breach was enough to establish standing.[47] While the

---

[45] 568 U.S. 398, 408 (2013).

[46] *See, e.g. Galaria*, 663 F. App'x at 391; *Remijas*, 794 F.3d at 697; *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 970 (7th Cir. 2016); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 630 (D.C. Cir. 2017).

[47] *See Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 91 (2d Cir. 2017); *Beck*, 848 F.3d at 278; *In re SuperValu, Inc.*, 870 F.3d 763, 772 (8th Cir. 2017) (allegations of future harm could not establish injury-in-fact, but plaintiff had standing because he alleged a present injury in the form of a fraudulent credit card charge).

standing inquiry in each of these cases was fact-intensive and case-specific, together these cases tend to suggest that unless an actual misuse of breached data is alleged or shown, plaintiffs lack standing under Article III.

Given the importance of this split to data breach litigants, it seems increasingly likely that the U.S. Supreme Court will weigh in on data breach standing.

B. The Economic-loss Rule

Unlike consumers, a company's business partners are much more likely to suffer readily identifiable direct financial losses that can establish Article III standing.

In these cases, however, the economic-loss rule can provide defendants a powerful shield against tort claims where data-security and breach response rights and responsibilities are governed by or addressed in a contract.[48]

The economic-loss rule can also be a powerful defense in cases brought by employees against their employers. In some states, courts have held that the economic-loss doctrine bars employees' data-breach tort claims against their employers.[49] Even in those states where the economic loss doctrine is subject to exceptions, such as for a "special relationship" between the plaintiff and the defendant, a pure employment relationship may be insufficient to invoke it.[50]

C. Other Defenses

When other defenses fail, defendants should scrutinize the allegations of the complaint to determine whether they allege sufficient facts to show a breach of a specific duty owed to the plaintiffs. This analysis can provide effective defenses at the Rule 12(b)(6) stage even when a plaintiff's injury allegations are enough to support Article III standing.

For example, as noted above plaintiffs have advanced "overpayment" or "benefit of the bargain" theories to avoid Article III standing issues. This theory rests on the premise that the price of a product or service includes a payment for data security measures.[51] When a data breach happens, buyers allege they have

---

[48] *See SELCO Community Credit Union v. Noodles & Company*, No. 16-CV-02247-RBJ, 2017 WL 3116335 (D. Colo. Jul. 21, 2017).

[49] *See, e.g., Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654, 672-73 (E.D. Pa. 2015); *Dittman v. UPMC*, 154 A.3d 318, 325 (Pa. Super. Ct. 2017) (appeal pending).

[50] *Id.*

[51] *See Carlsen v. GameStop, Inc.*, 833 F.3d 903, 909 (8th Cir. 2016).

overpaid for the product or service because the seller failed to provide the agreed-upon measures, which provides them an immediately measurable injury.[52]

Nevertheless, this type of claim has often been dismissed under Rule 12(b)(6). In one case, the court held that a plaintiff's overpayment allegations were enough to establish standing.[53] But those allegations—which did not identify a specific data security promise for which the plaintiff actually paid—could not state a breach of contract claim.[54]

In another case, the Eighth Circuit affirmed the dismissal of a claim that failed to draw a connection between a data breach and the company's alleged data-security failures.[55] There court reasoned that the mere fact that a data breach occurred did not supply the requisite factual basis for a breach of contract claim. Instead, the plaintiff needed to allege facts that established how the company's data security practices were deficient. Without specific allegations in that regard, the court explained, "the implied premise that because data was hacked [the defendant]'s protections must have been inadequate" amounted to a "naked assertion devoid of further factual enhancement" that could not survive a motion to dismiss under the Supreme Court's ruling in *Ashcroft v. Iqbal*.[56]

---

[52] *See id.*

[53] *In re VTech Data Breach Litig.*, No. 15 CV 10889, 2017 WL 2880102, *5 (N.D. Ill. July 5, 2017)

[54] *Id.* at *7-8.

[55] *Kuhns*, 868 F.3d at 717.

[56] *Id.*

Notes: