Bloomberg BNA

Privacy and Security Law Report®

Litigation

Recent decisions in data breach cases provide an important source of guidance for in-house counsel looking for ways to reduce breach-related legal exposure, the authors write, highlighting some important practical tips for in-house counsel from such actions.

Practical Tips for In-House Counsel From Recent Private Data Security Breach Litigation



BY SETH HARRINGTON, DAVID T. COHEN AND LINDSEY SULLIVAN

Seth Harrington is a partner in Ropes & Gray's privacy & data security practice in Boston. He has counseled clients through the array of legal issues arising from a data breach, including some of the largest U.S. companies.

David T. Cohen is counsel in Ropes & Gray's privacy & data security practice in New York. He is a certified privacy professional, CIPP/US, and focuses on complex consumer protection litigation, particularly in the area of privacy and data security.

Lindsey Sullivan is an associate as Ropes & Gray in New York and a member of the firm's Privacy & Data Security practice.

With cybercrime on the rise and plaintiffs' lawyers becoming more aggressive in the data security space in recent years, corporate victims of data security breaches have faced an onslaught of private litigation. The positions taken and decisions rendered in these actions provide an important source of guidance for in-house counsel looking for ways to reduce data breach-related legal exposure, supplementing the guidance that can be gleaned from more conventional sources such as regulatory enforcement actions. This article highlights some of the most important practical tips that in-house counsel can take away from these recent private actions:

- Remember that anything your company says publicly about the strength of its data security measures may be used to support deception-based claims against the company in litigation resulting from a data security breach.
- In the wake of a data security breach, keep in mind that anything your company says about the

 ISSN 1538-3423

extent of the breach may be relied on by courts to determine whether consumers were sufficiently ''injured'' to have standing to sue. For this reason, among many others, it is important to carefully consider what information to disclose and to ensure such disclosures are accurate.

- In the wake of a data security breach, courts may treat an offer of credit monitoring to consumers whose information may have been compromised as an admission that those consumers face a sufficiently imminent risk of injury to have standing to sue.
- How your company structures an internal investigation into a data security breach can significantly impact whether related documents and communications are protected by the attorney-client privilege or work product doctrine.
- The ability of companies that suffer data security breaches to obtain reimbursement for the costs associated with the response and with defense costs, settlements and/or judgments depends on whether adequate insurance coverage has been purchased in advance.

1. Anything your company says about the strength of its data security measures may be used to support deception-based claims. There can be legitimate business or legal reasons for some companies to disclose information about their data security practices. But when deciding whether and how to make such disclosures, companies should keep in mind that any such disclosures could well end up being cited by plaintiffs' lawyers and courts as supposed support for an allegation that the company overstated and misled consumers as to those practices.

For example, in *In re Zappos.com, Inc. Customer Data Securities Breach Litigation*, the company allegedly communicated to shoppers on its e-commerce site that ''shopping on Zappos.com is safe and secure—guaranteed.'' Compl. at ¶ 3, *In re Zappos.com, Inc. Customer Data Sec. Breach Litig.*, No. 12-325 (D. Nev. Nov. 13, 2012). After Zappos.com experienced a data breach incident, consumer plaintiffs relied on this alleged statement to assert that the company negligently misrepresented the safety of plaintiffs' financial information and violated California's unfair competition statute. *In re Zappos.com, Inc.*, No. 12-325, 2013 BL 239619 (D. Nev. Sept. 9, 2013). The court found the statement sufficient to form the basis for both counts at the motion to dismiss stage. *Id*.

There can be legitimate business or legal reasons for some companies to disclose information about their data security practices.

In other cases, plaintiffs relied on statements buried in privacy policies to assert deception-based claims. In *Grigsby v. Valve Corp.*, for example, a consumer plaintiff relied on statements allegedly made in the company's privacy policy to support a claim of unfair or deceptive practices. *Grigsby v. Valve Corp.*, No. 12-553, 2013 BL 96372 (W.D. Wash. Mar. 18, 2013) (12 PVLR 649, 4/15/13). Prior to the breach, the privacy policy purportedly indicated that ''Valve has taken reasonable steps to protect the information users share with us, including, but not limited to, setup of processes, equipment and software to avoid unauthorized access or disclosure of this information. . . .'' Plaintiff, characterizing this statement as a representation that users' information ''would be protected,'' alleged that he relied on this representation in choosing to purchase goods from the company.

According to the court, this assertion was sufficient, at the motion to dismiss stage, to allege that Valve acted unfairly or deceptively. *Id*. *See also In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014) (finding plaintiffs stated a claim by relying on a statement in the privacy policy that the company used ''reasonable administrative, technical, and physical security controls,'' despite separate language in the policy stating that no security measure is 100 percent effective) (13 PVLR 1604, 9/15/14).

It is important to remember that, even when plaintiffs survive a motion to dismiss, the company maintains the right to defend the accuracy of its statements once the facts are properly before the court. Nevertheless, the costs incurred in defending the statements' accuracy through litigation, or to settle a matter, can be significant. Those costs should be kept in mind when deciding whether and how to make statements about the company's data security measures. Any such statements should be carefully crafted and should match the company's actual data security practices.

2. Anything your company says about the extent of a breach may be relied on by courts to determine whether consumers were sufficiently ''injured'' to have standing to sue. In the wake of a data security breach, legal disclosure obligations or business considerations may lead a company to disclose the breach to individuals whose personal information may have been compromised, to regulators, or even to the public at large.

Recent decisions underscore the importance of carefully considering what information to disclose and of ensuring any such disclosures are accurate. In any private litigation by consumers over the breach, a key threshold legal issue will be whether the plaintiffs have been injured or face an imminent risk of injury. In the absence of such an actual or imminent injury from the breach, the plaintiffs lack standing to sue in federal court under Article III of the U.S. Constitution, and may lack standing in state court as well. *See, e.g.*, *Reilly v. Ceridian Corp.*, 664 F.3d 38, 41 (3d Cir. 2011) (concluding that ''Appellants' allegations of hypothetical, future injury do not establish standing under Article III'') (10 PVLR 1859, 12/19/11); *Maglio v. Advocate Health & Hosps. Corp.*, 40 N.E.3d 746, 753 (Ill. App. Ct. 2015) (finding ''plaintiffs' allegations of injury are clearly speculative, and therefore plaintiffs lack standing to bring suit'') (14 PVLR 1091, 6/15/15).

Moreover, actual damage is generally an element of the causes of action plaintiffs bring over data security breaches. *See, e.g.*, *Moyer v. Michaels Stores, Inc.*, No. 14 -561, 2014 BL 198944 (N.D. Ill. July 14, 2014) (13 PVLR 1276, 7/21/14); *Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010) (9 PVLR 1729, 12/20/10). At the motion to dismiss stage, one source of information courts may use to determine whether a suf-

  PVLR ISSN 1538-3423

ficient injury exists is the company's own statements, if any, about the extent and effect of the breach.

For example, in *Remijas v. Neiman Marcus*, Neiman Marcus posted public statements on its website to keep customers abreast of the data security breach it had suffered, including acknowledging that 350,000 cards were potentially exposed, and 9,200 of those cards had experienced fraud. *Remijas v. Neiman Marcus Grp. LLC*, 794 F.3d 688, 690 (7th Cir. 2015) (14 PVLR 1807, 10/5/15). Neiman argued in its motion to dismiss that the consumer plaintiffs did not face an actual or imminent risk of harm sufficient for Article III standing.

In ruling on that motion, the Seventh Circuit focused on Neiman Marcus's own public statements, particularly the statement that 9,200 of the potentially exposed payment cards had already suffered fraudulent charges, to conclude that future harm was sufficiently imminent to confer standing to the company's customers. *Id.* at 692–93. *See also*, *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011) (finding consumers' mitigation costs were reasonable following statements by the company that there had been ''theft'' of card information and ''approximately 1,800 cases of fraud resulting from the theft'') (10 PVLR 1519, 10/24/11); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. Apr. 14, 2016) (citing company's statements about the breach in concluding that plaintiffs had standing for purpose of motion to dismiss) (15 PVLR 821, 4/18/16); *c.f.*, *SuperValu, Inc., Customer Data Sec. Breach Litig.*, No. 14-4660, 2016 BL 3925 (D. Minn. January 7, 2016) (finding consumer plaintiffs lacked standing, rejecting Plaintiff's reliance on the company's press releases because those press releases in fact stated that there had been no determination that customer data had been stolen and no evidence that it had been misused).

Companies should carefully consider what information about the data breach to disclose, and ensure that any such disclosures are accurate.

This and similar cases make clear that a company's disclosures about a data security breach, including the extent and impact of the breach, can significantly affect a court's determination as to whether consumers face a sufficient injury to survive a motion to dismiss. For this reason, among many others, companies should carefully consider what information to disclose, and ensure that any such disclosures are accurate.

3. Your company's offer of credit monitoring to consumers whose information may have been compromised may be treated as an admission that those consumers face an imminent risk of injury. Many companies that suffer a data security breach offer free credit monitoring to consumers whose personal information may have been compromised. One effect of such offers is to reduce the possibility that consumers could argue in litigation that they are ''injured'' from having to purchase such monitoring themselves. For example, a California district court recently explained that ''[w]ithout specifically identifying what expenditures were necessary in excess of [free credit monitoring], Plaintiffs cannot establish what money was lost.'' *Falkenberg v. Alere Home Monitoring, Inc.*, No. 13-341, 2014 BL 281847 (N.D. Cal. Oct. 7, 2014) (13 PVLR 1786, 10/13/14).

In *Neiman Marcus*, however, the U.S. Court of Appeals for the Seventh Circuit treated Neiman Marcus' offer of credit monitoring to its customers as an effective admission that the customers faced a sufficiently imminent risk of fraud to give them Article III standing. *Neiman Marcus*, 794 F.3d at 694. The court found the offer ''telling,'' reasoning that ''it is unlikely that'' Neiman Marcus made the offer ''because the risk [to plaintiffs'] is so ephemeral that it can safely be disregarded. These credit-monitoring services come at a price that is more than *de minimis*.'' *Id.*

The reasoning of *Neiman Marcus* is highly problematic, but as a statement by a federal court of appeals, it should not be ignored. If you offer credit monitoring in the wake of a data security breach—and there can be legitimate reasons to do so in connection with certain breaches—consider including a statement clarifying the reason for the offer. Doing so may help to reduce the possibility that a court will erroneously view the offer as an admission that consumers face an imminent risk of harm.

4. How your company structures an internal investigation into a data security breach can significantly impact whether related documents and communications are protected by the attorney-client privilege or work product doctrine. Whether companies that suffer data security breaches may claim attorney/client privilege and work product protection for certain breach-related documents and communications is often disputed but rarely litigated.

A recent decision in litigation over the data security breach suffered by Target Corp. sheds important light on the scope of such protection. *In re Target Corp. Customer Data Sec. Breach Litig.*, No. 14-2522 (D. Minn. Oct. 23, 2015). In the wake of the cyberattack, Target set up a two-track response program. The first track involved a team of forensic experts who were engaged on behalf of several credit card brands (the PFI Investigator). The purpose of the second track was to assist counsel in conducting an investigation of the data breach to enable counsel to provide legal advice to Target. This track involved two key groups: (i) the Data Breach Task Force, which was made up of, *inter alia*, internal counsel and information technology specialists, and (ii) forensic experts engaged by Target's outside counsel. During discovery, Target produced all communications with the PFI Investigator, but withheld communications with, and the work product of, the Data Breach Task Force and the experts engaged by counsel.

Financial institutions pressing class actions against Target filed a motion to compel Target to produce, among other things, documents generated by the Data Breach Task Force and the forensic experts engaged to support counsel. The U.S. District Court for the District of Minnesota denied the motion as to documents generated by the Data Breach Task Force and the forensic experts engaged by counsel. *Id.*

The court found that Target submitted ''several declarations and exhibits to substantiate Target's privilege and work-product claims.'' *Id.* These declarations established ''that the work of the [second track] was focused not on remediation of the breach, as plaintiffs contend, but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could pro-

vide the company with legal advice and prepare to defend the company in litigation.'' *Id*. Moreover, the court found that plaintiffs could not overcome Target's work product protection because Target ''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.'' *Id*.

This opinion provides an instructive roadmap for in-house counsel and highlights that properly executing an internal investigation can solidify the company's claim to privilege.

5. The ability of companies that suffer data security breaches to obtain reimbursement for the costs associated with the response and with defense costs, settlements, and/or judgments depends on whether adequate insurance coverage has been purchased in advance. The market for products covering the wide array of losses associated with ''cyberrisk'' is relatively immature, but companies that suffer data security breaches often have failed to ensure that they have adequate coverage for costs and claims connected with data security incidents and privacy violations.

Before an incident occurs, it is important to review the current insurance portfolio to ensure that potential risks are adequately covered and, if you do not have a specialty cyberrisk policy, consider purchasing one. While there have been decisions regarding coverage available under traditional insurance policies, such as property or Commercial General Liability (CGL), litigation over specialty cyberrisk insurance policies is more rare. *See, e.g.*, *Zurich Ins Co. v. Sony*, No. 651982/2011 (N.Y. Sup. Ct. Feb. 24, 2014) (dispute regarding whether CGL insurance policy providing coverage for publication in violation of right to privacy covered losses from unauthorized access by third party).

However, recently filed disputes highlight key areas for focus in reviewing potential cyberrisk insurance policies. In *Columbia Casualty Co. v. Cottage Health Sys.*, the insured suffered a data security breach that allegedly exposed confidential medical records and agreed to fund a $4.2 million settlement to a class-action lawsuit brought against Cottage as a result of the breach. *Columbia Casualty Co. v. Cottage Health Sys.*, No. 2:15-cv-03432 (C.D. Cal. May 7, 2015).

In denying coverage for the settlement, the insurer relied upon an exclusion in the policy that allowed the insurer to void the policy based upon any misrepresentation in the insurance application ''which materially affects either the acceptance of the risk or the hazard assumed by the Insurer under the Policy.'' *Id*. Here, the insurer claimed that Cottage had provided false responses regarding its information security, specifically regarding security patches, default settings, annual security assessments and third-party audit and management. The court dismissed the complaint on the basis that the parties had not exhausted alternative dispute resolution under the terms of the policy. *Columbia Casualty Co. v. Cottage Health Sys.*, No. 2:15-cv-03432 (C.D. Cal. July 17, 2015). After the required alternative mediation process failed to result in a settlement, the insurer re-filed its suit seeking a declaration that coverage was lacking, and the litigation remains pending. Compl., *Columbia Casualty Co. v. Cottage Health Sys.*, No. 2:16-cv-03759-JAK-SK (C.D. Cal. May 31, 2016).

Companies that suffer data security breaches often fail to ensure that they have adequate coverage for costs and claims connected with data security incidents and privacy violations.

In addition, in *State National Ins. Co. v. Global Payments*, Global Payments, a payment processor, had suffered a data security breach in which payment card data was potentially accessed. *State National Ins. Co. v. Global Payments*, No. 1:13-cv-01205-CAP (N.D. Ga. Apr. 12, 2013). The payment card brands imposed and collected millions in fines and assessments under their respective operating regulations, and Global Payments sought reimbursement for these amounts from its carrier. The insurer sought declaratory judgment that no coverage was available under the policy because the fines and assessments were excluded from the definition of damages (because they did not represent actual damages but were the result of a liquidated damages calculation) and because the policy excluded coverage for liability under contract.

In addition, the insurer claimed that any coverage would be limited to a $250,000 sublimit. This action was resolved by settlement among the parties without a court decision, but a similar dispute in the District of Arizona involving different parties recently resulted in the court holding that the insured lacked coverage under a cybersecurity policy for certain assessments and fees imposed by the payment card brands because, in the court's view, the policy's exclusions and definition of loss barred coverage for contractual obligations assumed by the insured. *P.F. Chang's China Bistro, Inc. v. Federal Ins. Co.*, 2016 WL 3055111 (D. Ariz. May 31, 2016).

  PVLR ISSN 1538-3423