PROTECTING PRIVILEGE IN A CYBER BREACH INCIDENT RESPONSE

By Carole J. Buckner

When a data breach occurs, legal counsel may be called on to advise the company on a wide range of issues from media relations to customer notification, remediation and regulatory requirements. Because class action litigation and regulatory scrutiny can follow a data breach, it is critical to understand and properly address attorney-client privilege and attorney work product during the course of an incident response. Planning for the myriad issues beforehand is an important part of executing a competent incident response.

OUTSIDE COUNSEL

Hiring outside counsel at the inception of a data breach incident response can preserve the attorney-client privilege. Business advice from in-house counsel may not be privileged. *Aetna Cas. & Sur. Co. v. Sup. Ct.*, 153 Cal. App. 3d 467 (1984) (dominant purpose test). Some foreign countries do not extend privilege protection to communications between companies and their in-house attorneys.*Akzo Nobel Chem. Ltd. v. European Comm'n*, Case C-550/07 P, 26 Law. Man. Prof. Conduct 584 (Euro. Ct. Justice, Sept. 14, 2010).

DUAL INVESTIGATIONS & FORENSIC REPORTS

Running dual investigations can also help preserve privilege. In Target's payment card data breach, one incident response team worked on the business response, focusing on operational concerns, while a second team directed by Target's legal counsel directed a separate response task force. *In re Target Corp. Customer Data Security Breach Litig.*, 2015 WL 6777384 (D. Minn. Oct. 23, 2015). The plaintiffs argued that communications between the Target task force and the forensic consultant were not privileged because Target would have had to address the data breach regardless of any litigation. Target asserted that the forensic consultant had been engaged to educate the task force run by Target's in-house and outside legal counsel about aspects of the breach to enable counsel to provide informed legal advice, in part to defend against multiple class action lawsuits filed against Target. One set of documents in question involved email updates from the CEO to the Target board of directors in the aftermath of the data breach. The court ordered such communications produced because they did not involve any confidential attorney-client communications or contain requests for legal advice nor provide legal advice. *Id.* at 3. As to documents related to the work of the task force focused on informing Target's in-house and outside counsel about the breach for the purpose of obtaining legal advice and preparing to defend the class-action litigation, the court found Target met its burden of demonstrating these documents were protected. *Id.* at 3-4.

Disputes can develop over discovery of forensic consultant's reports. In *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230 (D. Or. 2017) (*Premera I*), the consultant hired by the company produced a remediation and intrusion report. After discovery of a breach, the statement of work was amended to provide for supervision by outside counsel. Premera argued that the subsequent report was privileged and protected as work product. However, the court found that report was discoverable because the consultant was hired by Premera, not by outside counsel, and the scope of work did not change after the consultant was directed to report to outside counsel and label the reports privilege. *Premera I*, at 1245.

In *In re Experian Data Breach Litig.,* 2017 U.S. Dist. LEXIS 162891 (C.D. Cal. 2017), a class-action followed the company's data breach announcement. The company hired outside legal counsel who in turn hired the forensic consultant to provide information to legal counsel to allow legal counsel to advise the company. The consultant provided a report to outside counsel only, who then shared the report with in-house counsel, all designed to facilitate legal advice by outside counsel. The full report was not shared with the company's incident response team. When the class-action plaintiffs sought discovery of the report, the court found that it was prepared in anticipation of litigation and thus protected by the work product doctrine. The court rejected the argument that the hardship exception to the work product doctrine applied to allow plaintiff's discovery of the report, because plaintiffs had the exact same access to mirrored images of the servers as the consultant had.

PUBLIC RELATIONS

A public relations consultant is a key member of the data breach incident response team. In California, there is no public relations privilege. *Behunin v. Sup. Ct.*, 9 Cal. App. 5th 833 (2017). Thus privilege may turn on whether a public relations consultant was the "functional equivalent of an employee of the client." *U.S. v. Chen*, 99 F.3d 1495, 1500 (9th Cir. 1996). Communications seeking legal advice about how a particular article may impact the company or litigation, or how, from a legal perspective, the company should respond, are privileged. *In re Premera Blus Cross Customer Data Sec. Breach Litigation,* 2019 U.S. Dist. LEXIS 20279 *11 (D. Or. 2019) (*Premera II*). If, however, the communication involves merely the facts of the article, or how others are responding to the article, without a request for or provision of legal advice, merely including attorneys on the email does not render the email privileged. *Id.*

Communications with a public relations consultant during a data breach investigation, even those incorporating advice of counsel, may not be protected by the attorney client privilege. *Premera I,* 296 F. Supp. 3d at *1241-42.* Documents prepared by employees and third-party vendors, even at the request of counsel, are not privileged if not prepared because of litigation. *Id*. at 1242. The court looks at whether the primary purpose is to address the data breach, a business function or to obtain legal advice. *Id*. at 1243. However, communications sent to and from legal counsel seeking or providing actual legal advice or the possible legal consequences of a proposed text are privileged. *Id*.

Handling communications appropriately during a data breach incident response can preserve privilege in later litigation.

Carole J. Buckner (carole.buckner@procopio.com) is Partner and General Counsel at Procopio, Cory, Hargreaves & Savitch LLP.

Procopio

2019 UPDATE ON STANDING IN DATA BREACH CLASS ACTIONS

By Carole J. Buckner, Partner and General Counsel, Procopio, Cory, Hargreaves & Savitch LLP

To demonstrate standing to sue under Article III of the United States Constitution, in general a plaintiff must show injury in fact that is concrete and particularized, actual or imminent, and that is not conjectural or hypothetical, is fairly traceable to the conduct of the defendant, and likely subject to redress by a favorable decision. *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (2016). Allegations of future injury will suffice for standing only if it is certainly impending and there is a substantial risk of harm.

This article surveys some of the most significant recent federal decisions on standing in class action data breach cases decided in 2019 to date. Federal circuits are split regarding what is required to be alleged by plaintiffs in a data breach class action in order to establish standing. The Ninth Circuit, along with the Sixth, Seventh and D.C. Circuits follow a more generous, plaintiff-friendly approach to standing in data breach cases, holding that an increased risk of future harm from identity theft following a data breach and expenses in mitigation of a data breach can confer standing in certain cases. In contrast, the Second, Fourth and Eighth circuits take a more limited approach to the issue and require concrete harm in order to establish standing.

The circuit split regarding standing in data breach cases remains after the United States Supreme Court decided not to take up the petition in *In re Zappos.com,* 888 F.3d 1020, 1027-29 (9th Cir. 2018) in March of 2019. The *Zappos* matter involved two groups of class action plaintiffs: those who had suffered financial losses from identity theft caused by the Zappos data breach, and those who alleged that identify theft was imminent but had not suffered any harm. The *Zappos* court found that even the plaintiffs who had not suffered any financial harm had established standing, where the customers' information was breached and obtained by hackers, and the customers alleged that their personal information could be used to commit identity theft and placed them at higher risk for phishing and pharming, allowing hackers to get further personal information. The fact that some of the Zappos consumers had already suffered financial harm resulting from the hacking undermined Zappos' claim that the consumer information could not be used for fraud or identity theft.

Un-truncated Credit Card Numbers and Identity Theft

Printing a receipt with customer credit card information may trigger a class action. Several recent class action cases address whether the issuance of receipts with un-truncated credit card information creates an increased risk of identity theft sufficient for the consumer to demonstrate standing, with mixed results depending on the specifics.

In March of this year, the Third Circuit filed its decision in *Kamal v. J. Crew Group Inc.,* 918 F.3d 102 (3rd Cir. 2019), the plaintiff's class action complaint alleged violation of the Fair and Accurate Credit Transactions Act (FACTA) after he received three receipts that included the first six digits (identifying the issuer and type of card) and last four digits of his credit card number. Kamal alleged that the printing of the receipts increased the risk of identity theft, citing legislative findings to that effect by Congress, the Federal Trade

Commission and the Department of Justice. The court acknowledged that FACTA was enacted to prevent identity theft by requiring truncation of credit card numbers and removal of expiration dates. However, Kamal had not alleged any third party access, nor had he alleged that the receipts included sufficient information to facilitate identity theft, given that the identity thief would have to obtain the other six digits, as well as additional information required in order to use the card, such as the expiration date, security code and/or zip code. The court dismissed the class action due to lack of standing on the grounds that Kamal did not suffer a "concrete injury" caused by the alleged FACTA violation, finding that the chain of future events that must occur for an identity theft was too speculative and attenuated, and therefore, that a material risk of harm did not exist.

In July of this year, the D.C. Circuit in *Jeffries v. Volume Services America, Inc.,* 2019 WL 2750856 (D.C. Cir. July 2, 2019), reached the opposite conclusion on a FACTA class action claim where the defendant provided credit card receipts that displayed her sixteen digit credit card number as well as the expiration date for the credit card, in violation of FACTA's truncation requirements. The plaintiff alleged that the receipt exposed her to an increased risk of identity theft and that she was forced to take steps to safe-guard the non-compliant receipt. The district court dismissed due to lack of standing, finding the alleged harms inadequate as an injury in fact. On appeal, the court indicated that "not *every* violation of FACTA's truncation requirement creates a risk of identity theft." However, the court held that the receipt in question contained sufficient information for a criminal to defraud her. Further, the court indicated that most people throw away receipts, and there was no way to know whether a customer receiving such receipts would notice that they contained such information. A person could throw away the receipt without noticing the harm and a thief, employee or fellow customer could retrieve it in order to use the information. Accordingly, on appeal, the court found she was unable to use her credit card without incurring an increased risk of identity theft and that this established a concrete injury in fact. The court distinguished *Kamal* based on the information contained on the receipt.

In April, the Eleventh Circuit decided a standing case involving FACTA in a class action following the Godiva data breach in *Muransky v. Godiva Chocolatier, Inc.,* 922 F.3d 1175 (11th Cir. 2019), finding the plaintiff suffered a concrete injury as required for standing when the retailer provided a customer receipt containing untruncated credit card numbers, in violation of FACTA. Muransky's receipt showed the first six and last four digits of his credit card number, and alleged this exposed the class members to a heightened risk of identity theft. The *Muransky* decision found that the heightened risk of identity theft did constitute an injury in fact which rose to the level of a concrete risk, based in part on Congressional intent in conferring the rights granted under FACTA. *Muransky* disagreed with the Third Circuit in *Kamal,* indicating that *Spokeo* recognized that the risk of harm may satisfy the concreteness requirement, given the specific Congressional findings supporting the FACTA truncation requirements. The *Muransky* decision also distinguished earlier decisions finding the printing the expiration date on a receipt in violation of FACTA did not support a finding of standing. Further, the court found that Muransky had standing based on the similarity of his conduct with the common law tort of breach of confidence.

Espionage and Standing Based on Risk of Identity Theft

If the data breach results from foreign government hacking, which may not be motivated by the potential use of the information for identity theft, does an employee have standing? A recent decision addressed this issue and also more generally discussed the type of evidence that shows an increased risk of identity theft.

In June, the D.C. Circuit issued its decision in the *U.S. Office of Personnel Management Data Security Breach Litigation,* 2019 WL 2552955 (D.C. Cir. June 21, 2019) (*OPM)*, in which the appellate court reversed the lower court's dismissal based on standing and held that federal employees whose personal information was exposed in a data security breach alleging a heightened risk of identity theft and other injuries had standing to state a claim. Among the harms alleged was improper use of Social Security numbers,

unauthorized charges to bank accounts, fraudulent openings of credit cards and filing of fraudulent tax returns. In addition, some plaintiffs alleged they purchased credit card monitoring services, and spent time and money trying to unwind fraudulent transactions made in their names. In challenging standing, OPM argued, and the district court accepted, that the risk of identity theft was not a sufficient basis for standing because the Chinese government was behind the particular data breach, negating any inference of intent to steal the victim's identities for purposes of identity theft.

On appeal, the *OPM* decision held that although a governmental attack may suggest other purposes for a cyberattack, it remained plausible to infer that identity theft was at least one of the hackers' goals and that espionage and identity theft were not mutually exclusive. This inference found further support from the fact that several victims already experienced identity theft and fraud following the data breach. The court also found that the passage of two years' time was not adequate to render the threat of future harm insubstantial. The *OPM* court further found that expenses incurred in mitigating the risk of identity theft qualified as "injury in fact." As to causation, the court held that the fact that some of the data was actually used to enable several forms of identity theft following the breach met the relatively modest burden of showing that the risk of future data theft was fairly traceable to the data breach.

Time and Expense to Address the Breach

Are mitigation efforts sufficient to support a claim for standing? In addition to the *OPM* decision, several other recent decisions address this, delving into detail regarding efforts required to mitigate a data breach.

In *Bass v. Facebook,* 2019 WL 2568799 (N.D. Cal. June 21, 2019), the court addressed the clams of two plaintiffs in response to Facebook's motion to dismiss due to lack of standing, finding one plaintiff had established standing, while another had not. The court evaluated standing based on the *Zappos* test of whether the data taken "gave hackers the means to commit fraud and identity theft." Following authority in the Sixth and Seventh Circuits, the court indicated that there was a reasonable inference that the hackers took the data for fraudulent purposes. This was further established, the court said, by the plaintiff's receipt of phishing emails following the hack. The court also found that the information taken "gave hackers the means to commit fraud or identity theft," citing *Zappos.* The court also held that lost time rectifying a data breach suffices as harm for purposes of standing based on the plaintiff's receipt of 30 emails, noting that although 30 emails may be *de minimus,* the consequences of the breach were yet to end, as more phishing emails will pile up.

In contrast, with regard to the second plaintiff, the court found that the circumstantial evidence alleged did not trace back to the data breach at all, and were so common as to foreclose plausibility. Specifically, the second plaintiff (Bass) indicated he had received fake Facebook friend requests, spam emails, pornographic links on his Facebook messenger service, that he had been forcibly logged out of his Facebook account and had received phone calls from people purporting to be his family members. The court indicated that "zero evidence demonstrates that hackers call their victims purporting to be family," and found that no reasonable inference could be drawn to indicate that the logouts and calls were connected with the data breach. In addition, the court described the emails and fake friend requests as too common to establish causation and therefore insufficient to support standing as to the data breach. Finally, Facebook did not notify Bass he was a victim of the data breach. The court said Bass could not assume that to be the case.

In May, in *Rudolph v. Hudson's Bay Company,* 2019 WL 2023713 (S.D. N.Y. 2019), a New York federal district court addressed the Saks Fifth Avenue data breach of its point of sale system which had gone undetected for a year until hackers had announced the intrusion. Although the plaintiff in the putative class action failed to allege a substantial risk of future injury, the court held that the time and expense incurred in obtaining a replacement debit card were sufficient to meet the low threshold required to allege injury-in-fact as required to demonstrate standing under Article III. The complaint alleged she spend 20 minutes on the phone with her bank, and drove 25 miles to visit a branch to obtain a new debit card. She spent about four hours reviewing her account for suspicious charges and updating her payment information with retailers, and spent $4.68 on the gasoline to get to the bank.

The plaintiff in *Rudolph* also alleged imminent and impending risk of future fraud and identity theft. The court recognized that "Whether the risk of identity theft is sufficiently material to create an injury in fact is 'a question for lower courts to determine in the first instance on a case- and fact-specific basis." The court further noted the distinction between breach of payment card data, particularly where the card can be replaced, vs. disclosure of social security numbers, birth dates and driver's licenses, which can be used for identity theft, and therefore can support an allegation of substantial risk of future harm. The court held that Rudolph's complaint did not plausibly allege a risk of harm from identity theft or identity fraud, given the card was canceled and the account immediately frozen. But, to the extent her claims were based on the time and expense of responding to the breach, she was injured and therefore had adequately alleged facts to meet the low threshold required for standing.

Procopio

ETHICAL OBLIGATIONS AND THE RIGHT OF ERASURE

By Carole J. Buckner, Partner and General Counsel, Procopio, Cory, Hargreaves & Savitch LLP

Privacy law provides clients and former clients with the right to request that all information held by a business be deleted. For example, the General Data Protection Regulation (GDPR) of the European Union, effective May 25, 2018, provides for what has been referred to as the "right to be forgotten." The California Consumer Privacy Act (CCPA), effective January 1, 2020, similarly provides consumers the right to request deletion of any personal information, with certain exceptions,[1] colloquially referred to as the "right of erasure." A recent ethics opinion addresses how these privacy rights impact a lawyer's ethical obligations, including ongoing obligations to check for conflicts of interest.

First, it is important to analyze when the GDPR or CCPA apply, given that there are various exemptions that may allow a business not to erase a client's information, even if the client makes such a request. Under the GDPR, a customer can request erasure of personal information under specified circumstances, including when the data is no longer necessary in relation to the purposes for which it was collected and/or processed.[2] Typically such a request could be made to a law firm when the engagement for which the client hired the firm has ended. However, such data can be retained by a law firm if necessary to comply with an obligation under EU law, or the law of an EU member, or where necessary for the establishment of or defense of legal claims.[3]

Under the CCPA, an exception exists for "internal uses" of personal information, which allows for the user to continue to use the information "internally, in a lawful manner compatible with the context in which the consumer provided the information." A second exception allows for internal uses "reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business." These exceptions may allow for retention of the information a customer is requesting to be deleted.

California does not yet have guidance for attorneys to follow regarding implementation of the right to be forgotten. California's ethics rules provide that ethics opinions of other jurisdictions and bar associations may be consulted for guidance on professional conduct.[4] Maryland's Ethics Opinion[5], addressed a lawyer's ethics obligations in view of the GDPR's "right to be forgotten." The Maryland Ethics Opinion provides that compliance with the GDPR would not excuse the lawyer from compliance with conflict of interest rules. The same can be said as to the CCPA. The Maryland Ethics Opinion provides that a request for deletion under the GDPR could serve as a waiver of and consent to a former client conflict of interest that could have been discovered by a law firm, had the deleted information been maintained.

Pursuant to the guidance provided in the Maryland Ethics Opinion, for such a waiver to be enforceable, the firm must provide written advice to the former client so that the former client is fully informed that the deletion of information pursuant to the GDPR could result in the firm having a conflict of interest. The

[1] Cal. Civ. Code § 1798.105
[2] GDPR, Article 17(1).
[3] GDPR, Article 17(3).
[4] Cal. Rules of Prof'l Conduct, rule 1.0, *Comment [4].*
[5] Maryland State Bar Association, Inc., in Ethics Docket No. 2018-06 (the Maryland Ethics Opinion).

explanation to the former client should advise regarding the reasons that the firm tracks client and matter information. As the opinion points out, there is very little practical risk to the client that the client's interests would be harmed under such circumstances, because if the firm deletes the client's information, it has likely eliminated most of the firm's knowledge of the client.

The remaining problem arises from the possibility that the attorneys working on the matter have retained knowledge of the deleted information of the former client which could be used against the former client. Under Maryland rules, as the Maryland Ethics Opinion points out, screening those attorneys with such knowledge might suffice. But the firm would still need to evaluate whether further informed written consent from the former, forgotten/deleted client would be appropriate, given the attorneys' retained knowledge. How this would be done as a practical matter is not explained.

Under California's Rules of Professional Conduct, screening would not be allowed unless the attorneys did not have substantial participation in the former client's matter and the conflict arose from a lawyer's association with a prior law firm.[6] In view of this, advance consent from the client requesting deletion to screen any attorneys with retained knowledge may be appropriate. In addition, notification to the former/forgotten client of the implementation of an ethical screen under such circumstances should be considered, and an evaluation of whether further informed written consent should be obtained would be appropriate.

The Maryland Ethics Opinion recommends that firms consider including a discussion of the right to be forgotten in the engagement letter, with a discussion of the impact of that right and the consequences of the exercise of that right. In addition, the Maryland Ethics Opinion recommends that the firm's policy for handling conflict issues be updated, and that the firm's policy for handling such situations be included with the letter to the client.

[6] Cal. Rules of Prof'l Conduct, rule 1.10(a)(2).

Pegah K. Parsi

Campus Privacy Officer
UC San Diego

Pegah K. Parsi is the campus privacy officer at UC San Diego where she spearheads the privacy and data protection efforts for the 70,000-person strong research, educational, and health enterprise. She manages a complex portfolio of privacy initiatives related to employees, students, applicants, alumni, and research participants and provides guidance on the GDPR, FERPA, HIPAA, California privacy laws, and research privacy/Common Rule. She provides thought leadership on privacy values, principles, and philosophy. Her day may involve anything from a consult on license plate readers to research involving smart devices to using predictive analytics to support student success.

Prior to San Diego, Pegah was a privacy manager at Stanford University, where she focused on medical studies and international collaborations. She has extensive experience in federal contracts, clinical trials, and research compliance.

Pegah is an attorney and holds an MBA. She is certified in information privacy for the US, EU, and program management (CIPP/US/EU, CIPM). She provides advisory services to the International Association of Privacy Professionals and works with other universities, federal agencies, libraries, and publishers to create a model for open access to research data.

In her spare time, she advises clients on immigration and asylum matters. She is a Veteran, who, among other things, was the Honor Grad of Army Truck Driver school!