CYBERSECURITY

How Safe Are You?

By Pamela W. Carter and Francine M. Giugno

In 2012, former FBI Director Robert Mueller said, "[T]here are only two types of companies, those that have been hacked and those that will be." Such vulnerability is evidenced by the Equifax hacking in 2017 that affected the data of 143 million Americans and exposed them to the threat of identity theft and fraud; the 2013 data breach of Target which resulted in the leak of tens of millions of credit and debit cards; and the record breach at Anthem in early 2015.

Cyber Risks

The cloud is a major focus in cybersecurity and it is oftentimes ignored. Open authorization risks and poor management of single privileged user accounts can create security risks. According to the Internet Crime Complaint Center, $5.3 billion was stolen due to business email compromises (BEC) between October 2013 and December 2016. These attacks send emails purportedly by someone in authority at the company to employees in the financial department who directs them to wire transfer funds.

The Internet of Things (IoT) is the network of physical objects — devices, vehicles, buildings and other items — embedded with electronics, software, sensors and network connectivity that enables these objects to exchange data. Businesses need to be aware of what devices are connected to their network and have measures in place to secure them; botnets have already launched which shut down networks of companies including Internet performance management company DynDNS. Old spam emails with exploit kits have been used to contain attachments that are macro-laden malicious documents. Modern ransomware is being placed into emails that employees are downloading inadvertently and they are costing businesses millions of dollars in lost data and recovery efforts.

Legal Update

Organizations that have not purchased cyber insurance have tried to argue that their traditional coverages apply to a cyber-event. While many insureds have turned to their crime or commercial general liability insurance policies for coverage, they have experienced mixed success, particularly as insurers clarify the coverage through new language or specific cyber exclusions.

Three cases have been handed down on the application of traditional coverage with respect to a cyber-event wherein the court found coverage for the losses. In *Medidata Solutions, Inc. v. Federal Insurance Co.*, 729 Fed. Appx. 117 (2 Cir. 2018), the 2nd Circuit upheld a lower court ruling awarding plaintiff Medidata Solutions, Inc. $5,941.787.37 from its insurer, Federal Insurance Co., on a coverage dispute on whether a commercial crime insurance policy covers wire transfer losses resulting from a spoofing attack. The spoof email directed employees to wire transfer funds to an account and the spoof email appeared to be sent from the company's president and outside counsel. The fraudsters did not hack the computer system but rather manipulated the company's email system. The language of the policy defined computer fraud as the "unlawful taking or fraudulently induced transfer of money, securities or property resulting from a computer violation." The provision covered losses stemming from "any entry of Data into" or "change to Data Elements or program logic of" a computer system. The court determined that the email system was a computer system and the email element was changed to mislead the company's employees that the email was from a high-ranking company official. Finding that there was a causal relationship between the spoofing attack and the losses incurred, the court found that there was proximate cause between the attack and the losses.

The 2nd Circuit reversed the district court in *American Tooling Center Inc. v. Travelers Ins. Co.*, 895 F.3d 455 (2 Cir. 2018), and determined that an insured's business insurance policy covered its loss stemming from fraudulent emails causing its employees to wire money to a party impersonating its Chinese vendor because the insured suffered a "direct loss" caused by "computer fraud" under the policy. A Michigan tool and die firm, American Tooling Center (ATC) wired approximately $800,000 in funds to a fraudster's account based on the fraudster's impersonating one of ATC's vendors. ATC sought coverage under its Wrap Business Policy issued by Travelers. The 2nd Circuit determined that the computer fraud directly caused ATC's "direct loss" and no exclusion applied. The policy language provided that "[t]he Company will pay the Insured for the Insured's direct loss of, or direct loss from damage to, Money, Securities and Other Property caused by Computer Fraud." The court determined that ATC lost the money when it transferred it to the fraudster. At issue was the definition of computer fraud in the policy, which stated that "Computer Fraud means: the use of any computer to fraudulently cause a transfer of Money, Securities, or Other Property from inside the premises or Financial Institution Premises: 1) to a person (other than a Messenger) outside the premises or Financial Institution Premises or 2) to a place outside the Premises or Financial Institution Premises." Travelers argued that the definition of computer fraud required that the computer fraudulently caused the transfer rather than simply be used. The court found that the fraudster sent ATC fraudulent emails using a computer and those emails fraudulently caused ATC to transfer the money to the fraudster and that the Travelers' policy did not require that that fraud cause any computer to do anything. Travelers sought to limit the definition of computer fraud to hacking or other type of behaviors where a party gains access to and controls the insured's computer; however, the court did not agree. Since the court did not find that any exclusion in the policy precluded coverage, it reversed the district court and found that the Travelers' policy provided coverage for the loss.

In *Spec's Family Partners Limited v. The Hanover Ins. Co.*, 739 Fed. Appx. 233 (5 Cir. 2018), the 5th Circuit held that an insurer had a duty to defend its insured, a retailer, in a data breach case with respect to costs assessed to it by a credit card payment processing company with whom it contracted under a Merchant Agreement. The insurer issued a Private Company Management Liability

Insurance Policy which contained an exclusion for contractual liability. The 5th Circuit found that the allegations in the underlying complaint implicated theories of negligence and general contract law that implied the insured's liability of assessments from its credit card processor separate and apart from any obligations based upon or attributable to any actual or alleged liability under the Merchant Agreement.

Other cases demonstrate the mixed results on coverage issues in traditional policies. In *Camp's Grocery, Inc. v. State Farm Fire and Casualty Co.*, 2016 U.S. Dist. LEXIS 147361, 4:16-cv-0204 (N.D. Alabama 10/25/16), Camp's Grocery sought defense and indemnity coverage from State Farm in a suit filed by three credit unions against Camp's and its franchisor, Piggly Wiggly. The three credit unions alleged that Camp's computer network was hacked, compromising confidential data on its customers, including their credit card, debit card and check card information. The three credit unions sought damages for their losses relating to reissuance of cards, reimbursement for its customers for fraudulent charges, lost interest and transaction fees, diminished good will and the administrative expenses associated with investigating, correcting and preventing fraud. The court granted State Farm's motion for summary judgment, finding that the Inland Marine Endorsements, which Camp's claimed provided coverage, is a first-party insuring agreement, not a third-party insuring agreement, that affords a defense and indemnity where the insured is sued to redress a loss suffered by another party. The court found that Coverage L for Business Liability did contain a third-party agreement for "property damages" but also noted that "property damages" was limited to "tangible property" and not "electronic data." The court noted that, even if the credit and debit cards were tangible property, there was no coverage because the credit unions did not allege that Camp's actions caused physical damage to the cards but rather that Camp's lax computer network security allowed the intangible electronic data contained on the cards to be compromised, thereby causing purely economic harm flowing from the need to issue replacement cards with new electronic data. *See, also e.g., Recall Total Information Mgmt, Inc. v. Fed. Ins. Co.*, 317 Conn. 46, 115 A.3d 458 (Conn. 2015) (no coverage under CGL for data breach because loss of computer tapes with personal identifying information on them did not constitute a "personal injury" as defined by the policies because there had been no "publication" of the information stored on the tapes resulting in a violation of a person's right to privacy.); *RVST Holdings, L.L.C. v. Main Street Am. Assurance Co.*, 136 A.D. 3d 1196 (N.Y. App. Cir. 2016) (no coverage under a CGL policy because the policy expressly excluded electronic data from covered losses); *Zurich Am. Ins. Co. v. Sony Corp. of Am.*, (2014 NY Misc LEXIS 5141) (no coverage under CGL for claims asserted against policyholder by customers whose data was stolen during data breach). *But see, Ellicott City Cable, L.L.C. v. Axis Ins. Co.*, 196 F. Supp. 577 (D. Md. July 22, 2016) (the court found the term "data" in multimedia liability policies ambiguous within the meaning of the unauthorized access exclusions and also noted that data appeared to relate to Internet, not television, programming so the court construed the policy in favor of the policyholder and found coverage).

Insureds are more likely to find coverage for cyber-events under cybersecurity policies than traditional policies, but even so, coverage is not guaranteed and depends on the policy language. For example, in *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, 2016 U.S. Dist. LEXIS 70749, No. CV-15-01322-PHX-SMM (D. Ariz. May 26, 2016), the court found that there was no coverage for nearly $2 million in expenses for credit card association assessments due to an exclusion for contractual liability in the cybersecurity policy. The court also noted that the insurer had reimbursed P.F. Chang's for $1,700,000 pursuant to the policy for costs incurred because of the data breach including conducting a forensic investigation and costs of defending litigation by customers whose data was breached and one bank that issued credit cards.

Defending Consumer Data Breach Class Actions

Rule 12 Motions

Currently, the federal circuits are split as to whether fear of identity theft in the wake of a data breach is sufficient to meet the standing requirements of Article III of the U.S. Constitution. Therefore, in addition to moving for dismissal for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6), defendants should consider moving to dismiss claims of plaintiffs who fear — but have *not* experienced — identity theft or fraudulent charges as a result of a breach for lack of standing under Rule 12(b)(1).

For example, the 4th and 8th Circuits have adopted a defense-friendly view, dismissing for lack of standing the claims of putative class representatives who fail to allege identity theft or fraudulent charges as a result of the purported breach. *See e.g., In re Supervalu, Inc.*, 870 F.3d 763 (8 Cir. 2017); *Beck v. McDonald*, 848 F.3d 262 (4 Cir. 2017), *cert. denied*, 137 S.Ct. 2307 (2018). These circuits held that fear of future harm as a result of a data breach is too speculative to meet the standing requirements of Article III, as interpreted by the Supreme Court in *Clapper v. Amnesty International USA*, 568 U.S. 398, (2013) (standing under Article III requires that any alleged "future harm" be "certainly impending" and that "allegations of possible future injury are not sufficient"). *See generally Beck*, 848 F.3d at 275-76 (relying on *Clapper* to hold that "substantial risk" requirement for standing was not met where the majority of those whose information was stolen in data breach would not suffer identity theft, and that plaintiffs could not manufacture standing by the alleged expenditure of resources to avoid identity theft).

Therefore, the 4th and 8th Circuits have allowed putative data breach claims to continue *only* if the named plaintiff alleges identity theft or fraudulent charges as a result of the breach. *See, e.g., Hutton v. Nat'l Board of Examiners in Optometry, Inc.*, 892 F.3d 613 (4 Cir. 2018) (standing require-

ment was met where named plaintiffs alleged that fraudulent credit card applications were submitted using their names and social security numbers); *In re Supervalu*, 870 F.3d at 773-74 (standing requirement was met as to the lone plaintiff who alleged that he incurred fraudulent credit card charges as a result of the data breach).

By contrast, the District of Columbia, 6th, 7th and 9th Circuits have adopted a plaintiff-friendly view, holding that plaintiffs who alleged fear of future identity theft in the wake of a data breach satisfied the injury-in-fact requirement for standing under Article III. *See, e.g.*, *In re Zappos.com, Inc., Customer Data Sec. Breach Litig.*, 888 F.3d 1020 (9 Cir. 2018) (distinguishing *Clapper*'s standing analysis as "especially rigorous" because it arose in the "national security context"); *Attias v. CareFirst*, 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S.Ct. 981 (2018); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6 Cir. 2016); and *Remijas v. Neiman Marcus Grp., L.L.C.*, 794 F.3d 688 (7 Cir. 2015).

However, even in these plaintiff-friendly circuits, some district courts have denied standing-based Rule 12(b)(1) motions only to dismiss claims under Rule 12(b)(6). *See, e.g., Moyer v. Michaels Stores, Inc*., No. 12014 U.S. Dist. Lexis 96588 (N.D. Ill. July 14, 2014) (finding Article III's standing requirement was met in a putative data breach class action notwithstanding *Clapper*, but granting motion to dismiss various claims because the plaintiffs failed to allege actual monetary damages — a required element of their claims — as neither an increased risk of identity theft nor the purchase of credit monitoring services constitute cognizable monetary damages).

Limiting Class Certification

Limiting the class claims to those who have suffered identity theft may significantly reduce the size of the potential class. In addition to the numerosity requirement, would-be representatives of an identity theft class may fail Federal Rule of Civil Procedure Rule 23(a)'s commonality and typicality requirements; classes seeking monetary relief under Rule 23(b)(3) may also fail to satisfy the predominance and superiority requirements. For example, in *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338 (2011), the Supreme Court held that Rule 23(a)'s commonality requirement requires not just common questions, but also common answers. Yet the answer to the question of whether the data breach in question caused each class member's identity theft may vary for each putative class member. Pursuant to the Rules Enabling Act, 28 U.S.C. § 2072(b), the class action device cannot abridge a defendant's substantive right to raise lack of causation, lack of damages and any other applicable defenses. Moreover, defendants may argue that an identity theft class seeking monetary relief under Rule 23(b)(3) is not ascertainable, as defendants presumably have no way of knowing what (if any) use third parties make of each consumer's data once it is stolen unless it has been used and damages are ascertainable. *See, e.g., Marcus v. BMW of N. Am., L.L.C.*, 687 F.3d 583 (3 Cir. 2012) (certification of Rule 23(b)(3) class action is appropriate only if the class members are "currently and readily ascertainable based on objective criteria;" cautioning against any method that would allow potential class members to self-identify); *but see, Mullins v. Direct Digital, L.L.C.*, 795 F.3d 654 (7 Cir. 2015) (rejecting any heightened ascertainability requirement; allowing class members to self-identify by affidavit is not *per se* improper). In addition, a named plaintiff who alleges identity theft or fraudulent charges may be inadequate to represent putative class members who have *not* suffered identity theft or unauthorized charges as a result of a breach.

Exposure to Other Types of Litigation Related to Data Breaches

Even if defendants are able to defeat consumer class actions filed in the wake of a data breach, other class action risks remain. For example, credit and debit card issuers have filed class actions against retailers in the wake of data breaches to recover the cost of reissuing credit cards and reimbursing cardholders for fraudulent charges. Such cases are generally not subject to dismissal based on lack of standing and may prove easier to certify and more costly to settle. *See, e.g., In re Target Corp. Customer Data Security Breach Litig*., 309 F.R.D. 482 (D. Minn. Sept. 15, 2015) (certifying a class of: "[a]ll entities in the United States and its Territories that issued payment cards compromised in the payment card data breach that was publicly disclosed by [defendant retailer] on December 19, 2013").

Also, defendants have been successful

in defeating tort claims asserted by card issuers pursuant to the economic loss doctrine where the contracts between the parties address and allocate the risk of loss in the event of a breach. *See, e.g., Cmty. Bank of Trenton v. Schnuck Markets, Inc*., 887 F.3d 803, 826 (7 Cir. 2018) (upholding dismissal of putative financial institution class action against defendant retailer based on the economic loss doctrine; finding tort claims were barred where the banks had already entered into voluntary and complex liability sharing agreements when entering into the credit card payment network).

In addition, publicly traded companies face derivative litigation exposure. Yahoo filed a proposed $80 million settlement of securities litigation pending in federal district court in San Francisco and stemming from defendant's 2013 and 2014 data breaches. The court granted the parties' motion for preliminary approval. *In re Yahoo! Inc. Sec. Litig*., No. 17-CV00373, slip op. (N.D. Cal. May 9, 2018). The proposed settlement comes in the wake of updated guidance on cybersecurity disclosure by the Securities and Exchange Commission (SEC). The SEC guidance calls on public companies to be more forthcoming when disclosing cybersecurity risks. Hence, publicly traded entities should pay particular attention to their disclosures in the event of a data breach, in anticipation that their statements will be scrutinized by both regulators and the plaintiff's bar.

In addition to card issuer and derivative litigation, a data breach may spur class actions by a defendant's employees if their personal information is compromised in the breach. *See e.g., Corona v. Sony Pictures Entm't, Inc.*, No. CV 14-09600, 2015 205 U. S. Dist. Lexis 85865 (C.D. Cal. Jun. 15, 2015) (denying motion to dismiss employees' putative class action negligence and state privacy claims and the court granted the preliminary approval of class action settlement, providing up to $4.5 million to reimburse employees for identity theft and credit monitoring, plus up to $3.5 million in attorneys' fees). In the wake

of the Supreme Court's decision upholding the use of class action waivers in employment arbitration agreements in *Epic Systems Corp. v. Lewis*, 138 S.Ct. 1612 (2018), employers may consider adding such provisions as a way to reduce employee class action litigation exposure.

Conclusion

Recent data breaches have made it clear that companies can no longer hope to simply avoid cyberattacks through IT security. Even organizations with top-of-the-line and robust security measures are not immune. As such, besides litigation and compliance with federal reporting requirements to federal agencies, most states, including Louisiana, have breach notification statutes for instances when personally identifiable information has become compromised, requiring the breached entity to notify the state and comply with the state notification requirements. Louisiana's Data Breach Notification Statute, La. R.S. 51:3071 *et seq.*, was amended to include biometric data, state identification card and passport, as well as social security, driver's license, financial information, birth date and medical information, and a mandatory notification of any breach to the state no later than 60 days from the breach.

Pamela W. Carter is the managing partner of Carter Law Group, L.L.C. Her practice focuses on general litigation with an emphasis on insurance defense, employment, transportation and product liability cases. She is active in the NAMWOLF, ABA and DRI legal communities. She is a former DRI National Director who has authored and coauthored many articles and publications, including a chapter in Truck Accident Litigation, *Third Edition (Laura A. Ruhl & Mary Kay Owen, eds., 2012). (pcarter@carterlawgroupllc.com; 9217 Jefferson Hwy., River Ridge, LA 70123))*

Francine M. Giugno is an attorney with the firm of Mickey S. deLaup, A.P.L.C. She has been a trial and insurance defense attorney for more than 22 years. Her practice focuses on general liability, insurance defense (coverage/bad faith), product liability construction and labor law. She represents management companies, insurers, business owners and commercial property owners in all aspects of civil defense. (fgiugno@delauplawfirm.com; 2701 Metairie Rd., Metairie, LA 70001)