

You've Been Hacked, and Now You're Being Sued:

The Developing World of Cybersecurity Litigation

by Michael Hooker and Jason Pill

Hardly a week goes by nowadays without headlines of yet another incident of corporate hacking or cybersecurity theft. Companies that electronically store sensitive information are facing the ever-changing challenge of guarding against unauthorized access to and misuse of such digital data. Critical computer-based assets increasingly have come under siege, and sophisticated hackers seem to be outpacing prophylactic measures designed to thwart their advance. As a result, digital data breaches have become almost commonplace today not only for multinational companies, but also for small and midsize companies. In short, cybersecurity has emerged as more than just an IT challenge — it is now a business and legal imperative.

Perhaps it is no surprise then that the recent scourge of cyber-theft has resulted in a proliferation of lawsuits brought by a variety of plaintiff groups. Shareholders, customers, and employees alike have joined the legal fracas, all claiming that the release of sensitive corporate information or personal data has caused some form of personal or business loss. Despite this groundswell of potential claimants, there is no single set of laws setting forth the legal duty of care or the bases for civil liability in data breach settings. Consequently, aggrieved individuals and their attorneys have been forced to resort to a patchwork of common law and state or federal statutory claims to obtain relief.

Judicial development in the cybersecurity arena is still evolving, as courts wrestle with how the theft of personal information, proprietary business data, or even someone's identity should be properly prosecuted and defended. This article explores emerging trends in the burgeoning field of cybersecurity litigation, including the types of claims typi-

cally asserted following digital data breaches, commonly asserted defenses to such claims, and the regulatory efforts to curb such breaches and protect consumers.

Types of Cybersecurity Litigation

Digital data breach litigation obviously does not trace its roots back to the English common law, and creative plaintiffs thus have been forced to shoehorn their claims into existing tort, contractual, and statutory theories of liability — with varying levels of success. The still-developing corpus of cybersecurity decisions provides limited judicial guidance and, as a result, new theories of liability are currently being vetted in state and federal courts across the country.

Most cybersecurity breach litigation today falls into one of four categories: 1) shareholder derivative suits to recover for losses in stock value; 2) securities fraud class actions to recover for the diminution in stock value following a cyber breach; 3) class action lawsuits by the breached company's outside customers or business partners whose sensitive or personal information was compromised during the breach; or 4) enforcement actions by governmental agencies invoking their regulatory authority under relevant state or federal laws. Although a single cyber breach incident might trigger more than one of the foregoing suits, and there is certainly overlap in the types of legal claims likely to be asserted in such actions, each category of suit nevertheless evinces some distinctive characteristics.

Shareholder Derivative Actions

Shareholders of corporations who have experienced a cybersecurity breach oftentimes file a shareholder deriva-

tive action. In a derivative action, a shareholder brings suit on behalf of the corporation against third parties, typically “insiders” such as executive officers or board members, asserting these individuals breached their duties of care to the corporation. In the cybersecurity context, the derivative claim typically alleges management failed to take adequate precautions to guard against a cyberattack and possibly compounded the problem by failing to give timely notice of the incident to affected third parties. This claim alternatively may be cast as a breach of loyalty for failing to act.

In October 2014, in *Palkon v. Holmes*, No. 2:14-CV-01234 SRC, 2014 WL 5341880 at *6 (D.N.J. Oct. 20, 2014), a New Jersey federal district court dismissed a derivative suit that had been filed against Wyndham Worldwide Corporation following a well-publicized cyberattack that allegedly involved the theft of over 619,000 payment card numbers.³ The court upheld the Wyndham board’s decision to reject the shareholder’s demand to sue, finding that this rejection had been based on a recommendation by outside counsel and the board’s own independent investigation. Although

a special litigation committee to investigate the claim and to make a recommendation as to whether the corporation should pursue legal action. The appointment of the committee — again a common defense strategy in shareholder derivative suit cases — resulted in a lengthy “stay” of the litigation, which remains pending as of this writing.

As these high-profile cases illustrate, shareholders pursuing derivative actions in the cybersecurity breach context face many challenges. Not only must the shareholders first make a demand on the corporation to file the suit, which the corporation might reject, but the corporate board’s conduct also is protected to a substantial extent from “second-guessing” by the business judgment rule. These obstacles may be particularly difficult to overcome when challenging corporate judgment calls regarding how to respond to cyber-threats involving complex and ever-changing computer systems. Nevertheless, directors do have an affirmative duty to oversee cybersecurity initiatives, and a failure to do so could trigger shareholder derivative liability.

Not only must the shareholders first make a demand on the corporation to file the suit, which the corporation might reject, but the corporate board’s conduct also is protected to a substantial extent from “second-guessing” by the business judgment rule.

These breach claims are also sometimes combined with a claim alleging management wasted corporate assets or abused its authority.¹ The recovery in a derivative action goes to the corporation itself, not the initiating shareholder.

A shareholder who wishes to sue on behalf of a corporation typically first must demand the board of directors bring the action. If the board refuses, its decision falls under the purview of what is known as the “business judgment rule.” Pursuant to this rule, courts presume board members refused the shareholder demand on an informed basis, in good faith, and with the honest belief that their actions were in the best interests of the corporation. The board also has the option of appointing what is known as a “special litigation committee,” whose purpose is to investigate the shareholder’s claims and to make a recommendation as to whether the corporation should file suit.²

Shareholder derivative suits in response to cybersecurity breaches thus far have yielded mixed results.

the Wyndham shareholder argued that the board’s investigation was predetermined and unreasonable, the court noted that “the business judgment rule’s strong presumption” authorizes courts to “uphold even cursory investigations by boards refusing shareholder demands.”⁴

Following the well-publicized 2014 cyber-theft of credit and debit card information belonging to more than 40 million Target Corporation customers, Target shareholders filed four separate shareholder derivative actions, all of which were later consolidated into a single federal court proceeding.⁵ The suits asserted that Target’s board violated its fiduciary duties and wasted corporate assets not only by initially failing to prevent the data breach, but also by later failing to disclose the breach.⁶ They also count among the damages “costs incurred from the [c]ompany’s internal investigation into the data breach...[and] for remediation activities.”⁷ Responding to yet another shareholder demand that was not part of the consolidated case, Target’s board later appointed

Securities Fraud Class Action Lawsuits

Perhaps the most frequently used form of lawsuit to recover for diminution in stock value following a cyber breach is securities class action litigation. In this type of suit, similarly situated shareholders contend that they relied to their detriment on a company’s material misrepresentations. The misrepresentation in the cybersecurity context might result from public statements by the company regarding its cyberattack readiness or the comprehensiveness or impact of an attack that already has occurred. Material misrepresentations sometimes stem from public statements made in press releases or, in the case of public companies, even the corporation’s Form 10-K reports. Unlike the shareholder derivative action discussed above, recovery in a securities fraud case inures to the suing shareholders, not the corporation.

In December 2007, Heartland Payment Systems, Inc., a Fortune 1000

A shareholder who wishes to sue on behalf of a corporation typically first must demand the board of directors bring the action. If the board refuses, its decision falls under the purview of what is known as the “business judgment rule.”

bank card payment processor, suffered a data breach impacting 130 million credit and debit card numbers.⁸ The plaintiffs alleged that the company finally admitted the full scope of the breach to the public more than a year later in 2009.⁹ When Heartland's stock price fell almost 80 percent, shareholders sued, alleging that the company had hidden the attack on its computer network and also had overstated its cybersecurity preparedness.¹⁰ Some of these statements derived from Heartland's Form 10-K filing, which touted Heartland's “emphasis on maintaining a high level of security.” In a victory for defendants, the trial court dismissed the lawsuit, holding that Heartland's failure to disclose the prior cyberattack was not a material omission and the mere fact that Heartland's system had been infiltrated did not necessarily mean that its public statements were false.¹¹

Damages in a securities fraud class action based on a cyber breach are typically manifest as a reduction in stock value.¹² Many courts require that there be a “statistically significant” decline in the company's stock price, often requiring the use of expert witnesses and complex valuation models.¹³ Accordingly, if a company victimized by a cyber breach does not suffer a concomitant decline in share value, it is less likely to be sued for securities fraud.

Consumer Class Action Lawsuits

The class action litigation form is invoked in cyber breach cases not only from within by shareholders of the impacted company, but also from without by customers of, or financial

institutions doing business with, the company. Consumers or aggrieved individuals bringing class actions typically contend common questions of law and fact pervade the hackers' unauthorized access to the consumers' sensitive personal information because this data was maintained or stored in the same manner by the defendant. Similarly, financial institutions occasionally assert the defendant company improperly allowed access to sensitive financial information such as bank account or payment card information.¹⁴ The causes of action asserted in these cases are many and varied, encompassing everything from common law tort claims to breach of contract and statutory claims. And courts sometimes struggle with whether these longstanding theories of liability are pliable enough to encompass the misappropriation of electronic information, signaling the need for additional legislation or guidance.

• *Common Law Claims* — Perhaps the most frequently asserted consumer class action claim is premised on simple common law negligence. The critical inquiry in data breach negligence cases is whether the breached organization owed the aggrieved individual a duty to exercise care in protecting the individual's personal information and breached this duty by failing to establish adequate safeguards to prevent such access.¹⁵ In many cases premised on negligence, defendants have been able to avoid liability by proving there was no threshold duty to protect their information from unauthorized access. Some courts have gone so far as to hold a duty to protect against data

security breaches exists only when a plaintiff voluntarily provides a defendant with personal information and thereby establishes a direct relationship with the defendant.¹⁶ A common defense to cybersecurity negligence cases is that the plaintiff had a preexisting relationship with the defendant and suffered only economic damages, barring the claim under the economic loss doctrine.¹⁷

Negligent misrepresentation claims also have been alleged where the defendant made representations it would take reasonable measures to protect the plaintiffs' information.¹⁸ The “misrepresentation” is usually found in advertisements, public filings, logos, websites, or marketing statements by the defendant. Defendants frequently seek to dismiss these claims by demonstrating the plaintiff's reliance on the defendant's representation was not justified.¹⁹

As an alternative to negligence claims, class action data breach plaintiffs often allege a defendant made an express contractual promise to protect their personal information and breached that obligation by failing to prevent the exposure of such information.²⁰ This claim obviously turns on establishing an explicit agreement to protect the plaintiff's sensitive information. Plaintiffs who are unable to prove the existence of such an express contract sometimes have alleged, alternatively, that the defendant's conduct created an *implied* contract to protect the data collected from the plaintiffs.²¹ Although an implied contract can be created when the parties' conduct manifests a mutual assent to be bound, courts frequently dismiss implied contract claims unless the

parties share a direct relationship.²²

Some plaintiffs also have pursued equitable theories, such as unjust enrichment, to seek redress for injuries resulting from a data breach.²³ A consumer class action lawsuit stemming from the Target breach discussed above set forth two distinct theories to support their unjust enrichment claim — the “overcharge theory” and the “would not have shopped theory.” First, plaintiffs alleged that a premium for adequate data security was included in the purchase price of the goods sold by Target and that Target’s failure to maintain that level of security resulted in an overcharge for goods received. Second, plaintiffs stated that if Target had timely notified its customers about the breach, plaintiffs would not have shopped at Target, thereby depriving Target of plaintiffs’ purchases after Target knew or should have known about the breach. The *In re Target* court, similar to sister courts, was persuaded by the viability of these theories and held that either theory can support a claim for unjust enrichment.

• **Statutory Claims** — The foregoing

common law claims are also increasingly being supplemented by statutory claims premised either on new legislation directed specifically at the cyber breach crisis or on long-standing statutory frameworks that were originally enacted to redress other wrongs. Notably, Florida’s legislature enacted a data breach notification statute in 2014 specifically aimed at addressing data breach issues, but the relief afforded by the statute — similar to many other state notification laws — is limited to the execution of a notice of the breach itself.²⁴ Looking elsewhere, plaintiffs have sought redress under existing statutes not directly aimed at cybersecurity concerns, and at least one federal district court allowed a data breach claim to proceed under the Florida Deceptive and Unfair Trade Practices Act. In *Burrows v. Purchasing Power, LLC*, No. 1:12-CV-22800-UU, 2012 WL 9391827 at *6 (S.D. Fla. Oct. 18, 2012), the plaintiff staved off dismissal by sufficiently alleged deceptive practices based on the defendant’s inadequate protection of personally identifiable information (PII) and failure to provide prompt no-

tification of the breach, which limited the plaintiff’s remedial actions.²⁵

Alternatively, Florida businesses victimized by hackers may find statutory relief to offset losses experienced as a result of a data breach — assuming, of course, they can locate the hackers. Effective October 1, 2015, Florida’s Computer Abuse and Data Recovery Act (CADRA) provides businesses with a new cause of action for unauthorized computer access.²⁶ The protections of CADRA are triggered when an individual “knowingly and with intent to cause harm or loss” 1) obtains information from a protected computer without authorization and, as a result, causes a harm or loss; 2) causes the transmission of a program, code, or command to a protected computer without authorization and, as a result, causes harm or loss; or 3) traffics in any technological access barrier through which access to a protected computer may be obtained without authorization. A business bringing suit under CADRA may recover actual damages, including lost profits and economic damages, recovery of the violator’s profits, injunctive relief to



accurateserve™

WHERE PERFECTION IS THE PROCESS

“We Give Attorneys Peace of Mind”

Your Florida Connection for Statewide:

Service of Process	Courier Service
Document Retrievals	Skip Traces

12 Offices Statewide:

Lakeland (863) 873-6691
www.accurateservefl.com

Tampa (813) 644-9368
www.accurateservefl.com

Jacksonville (904) 735-7810
www.accurateservejax.com

Tallahassee (850) 519-5494
www.accurateservetally.com

Orlando (407) 760-0880
www.accurateserveorlando.com

Fort Myers (239) 822-7299
www.accurateservefortmyers.com

Kissimmee (407) 906-9275
www.accurateserveorlando.com

Naples (239) 822-7299
www.accurateserveftmyers.com

Lake Mary (321) 430-7378
www.accurateserveorlando.com

Plantation (954) 770-9997
www.accurateserveplantation.com

Sarasota (941) 893-9991
www.accurateservesarasota.com

Bradenton (941) 216-2267
www.accurateservesarasota.com



Damages in a securities fraud class action based on a cyber breach are typically manifest as a reduction in stock value. Many courts require that there be a “statistically significant” decline in the company’s stock price, often requiring the use of expert witnesses and complex valuation models.

prevent further violations and recover the stolen information, and reasonable attorneys’ fees.

In addition to invoking state statutes, plaintiffs frequently attempt to extend federal statutes to afford private causes of action for cyber breaches. Such statutes include the Fair Credit Reporting Act (FCRA), the Stored Communications Act (SCA), the Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act of 1996. Perhaps the most widely litigated federal statute with respect to digital data breaches has been the FCRA, which creates duties for three different kinds of entities: 1) consumer reporting agencies; 2) furnishers of information to consumer credit reporting agencies; and 3) users of consumer credit reports.²⁷ These duties include the adoption of reasonable procedures, investigation of consumer disputes, and rectification of inaccuracies. However, cyber breach claims under the FCRA have been largely unsuccessful because most defendants do not qualify as “consumer reporting agencies.” For instance, in *Holmes v. Countrywide Financial Corp.*, No. 5:08-CV-00205-R, 2012 WL 2873892 at *15 (W.D. Ky. July 12, 2012), a federal court restricted “consumer reporting agencies” to credit reporting bureaus, such as Equifax, and dismissed a FCRA claim against the defendant because Countrywide Financial Corporation was a mortgage lender that did not assemble or evaluate credit information.²⁸

Plaintiffs also sometimes allege that the defendant’s data breach violated the SCA, which prohibits a person or entity providing an electronic

communication service to the public from knowingly divulging the contents of the communication while in electronic storage by the service.²⁹ The SCA further provides that a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication is carried or maintained on that service. Nevertheless, these claims usually are easily defended on the grounds that only telecommunications companies and internet providers are covered by the SCA.³⁰

• *Best Defenses: No Causation or Damages* — In consumer class action data breach claims, plaintiffs usually must prove their alleged injury was caused by the defendant’s failure to protect adequately plaintiffs’ personal information. As a result, courts are tasked with determining what kind of evidence is required to show that a particular misuse of data was perpetrated using data stolen from the defendant.³¹ Essentially, courts must determine whether an alleged misuse of a plaintiff’s data (*e.g.*, identity theft) was a result of the data breach, or merely a coincidence based on the timing of the events. This showing has been an insurmountable hurdle for some plaintiffs who struggle to demonstrate that a particular incident or harm was caused by, and not just correlated with, the data breach.³²

A plaintiff sufficiently proves a causal relationship when 1) a plaintiff gives the defendant his or her personal information; 2) the identity fraud incidents began within a short period of time after the plaintiff’s personal information was stolen; and 3) the plaintiff previously had not

suffered any such incidents of identity theft.³³ Courts have stated that these three facts, in combination with the inference a jury could make that the type of data stolen was the same type of data required to open fraudulent accounts, is sufficient to establish the causation requirement.³⁴ Even when an identity theft occurs shortly after an alleged breach, courts recognize that allegations of merely time and sequence are often insufficient to establish causation.³⁵ However, these standards for establishing causation undoubtedly will continue to evolve as future technological advances allow for more sophisticated tracking and logging of personal data.

Perhaps the biggest obstacle for data breach class plaintiffs has been proving that the exposure of their personal information resulted in actual damages.³⁶ Although a plaintiff’s Social Security number or other private information may have been improperly accessed, the plaintiff frequently cannot establish that this information actually was used by an unauthorized person in an unauthorized way.³⁷ Many data breach plaintiffs cannot show that they suffered identity theft, credit card fraud, or any other tangible monetary loss as a result of the breach.³⁸ Moreover, if the plaintiff’s bank or credit card company provides reimbursement for the unauthorized access, which often occurs in data breach cases, there is obviously no recoverable loss.³⁹

In addition to, or in the absence of, actual harm, data breach plaintiffs sometimes allege that the exposure of their personal information has resulted in an increased risk of *future* harm. Such plaintiffs typically allege

that a defendant's failure to adequately secure the plaintiffs' personal information raised the risk that this information will be misused to commit future fraud or identity theft.⁴⁰ For example, in *Grigsby v. Valve Corp.*, No. C12-0553JLR, 2012 WL 5993755 (W.D. Wash. Nov. 14, 2012), a class action for negligence and breach of contract was filed following a data breach involving the defendant's online video game platform that allowed users to purchase games and other software.⁴¹ Unknown third parties hacked the online platform and gained access to users' account information, including billing addresses, passwords, online handles, and credit card information. The breach caused Grigsby, the named plaintiff, to file a lawsuit against the defendant, on behalf of all video game users, claiming that the defendant failed to take reasonable security measures to protect user information. Grigsby alleged that he and the class plaintiffs may suffer harm in the future, including service interruptions, loss of financial information, inability to access the gaming network, and potential credit card fraud. Dismissing the plaintiffs' claims, the court held that these allegations of future injury, absent actual fraud or identity theft, do not constitute cognizable damages.

Similarly, plaintiffs frequently claim that the resources they must spend to contact credit reporting agencies and to place fraud alerts on their bank accounts suffice to establish a cognizable injury.⁴² To be sure, cyber breach victims may have expended money to purchase credit monitoring services or may have invested many hours of time restoring bank accounts or communicating with third parties in an attempt to limit any adverse impact. Most courts, however, have ruled that the time and expense of credit monitoring to lessen the risk of future harm is not a cognizable injury.⁴³

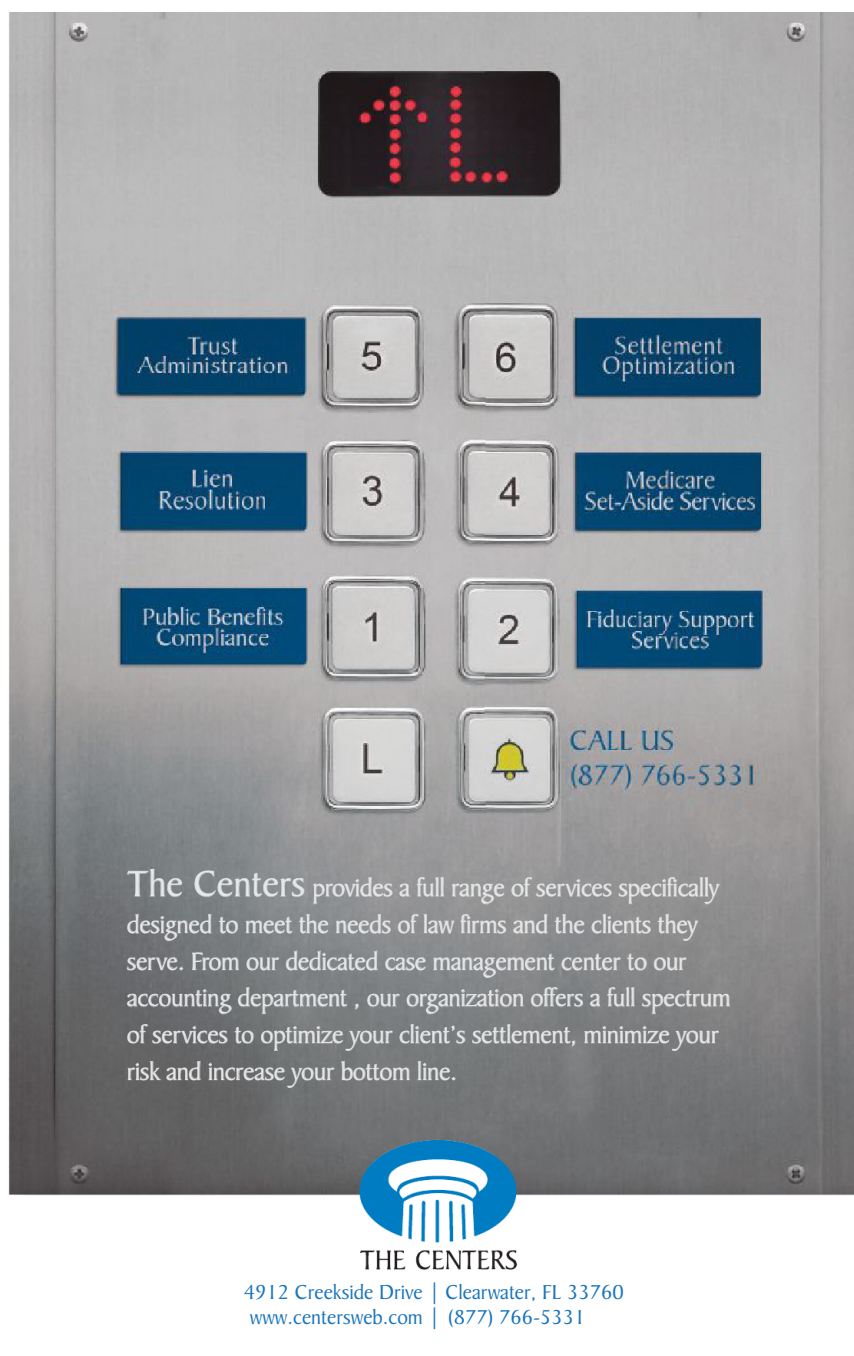
Finally, plaintiffs also sometimes claim that the unauthorized access or misuse of their personal information caused them anxiety or emotional distress.⁴⁴ However, courts across multiple jurisdictions have rejected emotional distress as a recoverable harm in the cyber security context.⁴⁵

Similarly, courts have held that a loss of privacy is not a cognizable injury, unless the invasion of privacy was egregious.⁴⁶

Federal Regulatory Actions

Beyond private causes of actions, federal governmental agencies also have gotten into the cybersecurity mix of late, demonstrating an increased propensity to bring various types of enforcement actions. A few of these regulatory initiatives have encountered stiff resistance due, in part,

to the absence of any overarching federal legislation to regulate cybersecurity liability and the lack of a uniform standard for private-sector cybersecurity programs. The National Institute of Standards and Technology (NIST) Cybersecurity Framework, which was released in early 2014, has been considered the leading federal authority to date for cybersecurity guidance.⁴⁷ However, it is not binding on private-sector businesses and provides no enforcement mechanism (although some commentators believe



The advertisement features a digital keypad interface with the following elements:

- Top Display:** A red LED display showing the number "12".
- Service Buttons:**
 - Trust Administration
 - Settlement Optimization
 - Lien Resolution
 - Medicare Set-Aside Services
 - Public Benefits Compliance
 - Fiduciary Support Services
- Navigation Buttons:**
 - 5, 6, 3, 4, 1, 2, L, and a bell icon.
- Contact Information:**
 - CALL US (877) 766-5331
- Text Description:**

The Centers provides a full range of services specifically designed to meet the needs of law firms and the clients they serve. From our dedicated case management center to our accounting department, our organization offers a full spectrum of services to optimize your client's settlement, minimize your risk and increase your bottom line.
- Logo and Footer:**
 - THE CENTERS** logo featuring a stylized classical building.
 - 4912 Creekside Drive | Clearwater, FL 33760
 - www.centersweb.com | (877) 766-5331

the Framework may create a de facto legal standard that ultimately is applied by the courts). In addition to the NIST, several other federal agencies, including the Department of Justice (DOJ), the Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC), have become more active in monitoring cybersecurity by issuing various protocols and guidelines.

In an effort to move beyond issuing mere guidance, some of these agencies are bringing enforcement actions against companies that have experienced data breaches, typically relying on statutory or other authority not originally intended for cybersecurity redress. The SEC, for example, increased its focus on cybersecurity issues over the last five years, signaling its intent to further expand these efforts for financial institutions and publicly traded companies. Although the SEC's initial foray into the realm of cybersecurity was limited to comment letters, the agency quickly intensified its focus over the last few years to pursue more enforcement actions. The agency's cybersecurity enforcement focus generally falls into two categories: 1) corporate disclosures regarding data security measures and prior data breaches; and 2) internal controls to prevent cyber incidents. To that end, the SEC's regulations contain a "safeguards rule" to require registered brokers, dealers, investment companies, and investment advisers to adopt written policies and procedures to reasonably protect client records and information.⁴⁸

As illustrated by the *R.T. Jones Capital Equities Management* matter, SEC Admin. Proceeding No. 3-16827, the SEC is bringing charges against public companies for failure to properly protect the PII of customers and clients — even though these companies were themselves victims of criminal behavior. *R.T. Jones*, an investment adviser, suffered a cyber-attack that enabled access to the PII of over 100,000 clients. At the time of the breach, the investment firm did not have any written policies or procedures to safeguard client data. Finding that *R.T. Jones* violated the safeguards rule, the SEC exacted, in

September 2015, a \$75,000 penalty and imposed other nonmonetary conditions.⁴⁹ Of particular note, the SEC took this enforcement action even though the clients had not suffered actual economic harm and the subject investment adviser had only seven employees — tacitly proclaiming that no firm or entity is too small to evade the SEC's radar.

Although the SEC has been active in the field of cybersecurity, the FTC has become the most prominent regulatory agency to occupy the space. Over the past 15 years, the FTC has brought more than 50 enforcement proceedings relating to data security and, much like the SEC, intensified its regulatory oversight in more recent years. The bulk of the FTC's enforcement efforts have been through administrative actions, which are typically resolved via consent orders requiring, among other things, increased data security measures. However, the FTC recently upped the ante by filing lawsuits in federal court, drawing upon its authority to prohibit "unfair or deceptive acts or practices in or affecting commerce" under §5 of the Federal Trade Commission Act.⁵⁰

Although most of these FTC lawsuits settle shortly after filing and, thus, offer scant judicial precedent, the crown jewel of the FTC's enforcement initiative to date is its federal case against the Wyndham hotel group.⁵¹ The multiple data breaches involving Wyndham spawned not only the shareholders derivative suit discussed above, but also an enforcement action by the FTC alleging that Wyndham's privacy policy misrepresented the security practices in place to protect customers' PII. Taking the path less traveled in enforcement actions, Wyndham declined to settle with the FTC, opting instead to challenge the FTC's putative lack of authority to pursue cyber breaches and failure to publish regulations that allegedly would have provided businesses with fair notice of the relevant data security standards. The district court held that the differences between the Wyndham's stated policies and actual practices were sufficient to support a claim under the FTC act. In a watershed decision, the Third Circuit affirmed the district

court in August 2015, holding that the FTC has authority to regulate "unfair" cybersecurity failures under §5 of the FTC act, and that the FTC act, along with Wyndham's prior data breach issues, provided sufficient notice to Wyndham of pertinent data breach standards.⁵²

The *Wyndham* ruling has cemented the FTC's unofficial role as the primary agency policing cybersecurity practices of domestic companies, and serves as a reminder to businesses that the consequences of data breaches include more than mere business disruption and reputational harm. Although there remains a dearth of statutory or regulatory guidance concerning reasonable cybersecurity practices, the *Wyndham* decision confirms the FTC's ability to bring enforcement actions for unreasonable or "unfair" cybersecurity practices "affecting commerce" and may embolden other federal agencies to become more active. With data breaches continuing to steal headlines, Congress and regulators likely will face mounting pressure from the public to develop a more comprehensive federal regulatory scheme for cybersecurity issues.⁵³

Conclusion

The field of cybersecurity litigation perhaps can be characterized as a situation in which technology forged ahead of the law, and the law is now struggling mightily to catch up. Devious and crafty hackers devised ways to infiltrate and damage sophisticated computer systems before there were many laws or regulations specifically designed to provide guidance to or recovery for the cyber victims. The miscellany of statutes, common law, and regulatory authority thus far used to litigate cybersecurity data breaches has provided a somewhat awkward and cumbersome means of redress, underscoring the need for additional guidance and uniformity. As the judiciary increasingly issues new decisions regarding the kinds of claims and defenses that are appropriate in digital data breach cases, greater clarity will be achieved. Similarly, the introduction of new statutes and regulations aimed particularly at cybersecurity breaches inevitably will

provide clearer legal standards and enhanced enforcement mechanisms. But whatever happens next in this field, one thing is for certain: The legal landscape involving cybersecurity is currently in flux and poised to shift dramatically over the coming years. □

¹ See, e.g., *In re Target Corp. Customer Data Sec. Breach Litig.*, No. MDL 14-2522 PAM/JJK, 2015 WL 5432115 at *1 n.1 (D. Minn. Sept. 15, 2015) (noting that the shareholder derivative actions (captioned *Kulla v. Steinhafel*, No. 14-203, D. Minn.) alleged waste of corporate assets and were stayed while a special litigation committee appointed by Target's board of directors investigated the claims).

² See *id.*

³ *Palkon v. Holmes*, No. 2:14-CV-01234 SRC, 2014 WL 5341880 at *6 (D.N.J. Oct. 20, 2014) (granting Wyndham's motion to dismiss based on the "business judgment rule's strong presumption" that pursuing the shareholder's demand was not in the corporation's best interest). See also *F.T.C. v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015).

⁴ *Id.*

⁵ *In re Target*, No. MDL 14-2522 PAM/JJK (D. Minn. 2014). To ease the administrative burden of the consolidated litigation, the case was separated into two "tracks" — one for consumers and the other for financial institutions — and the shareholders' action was stayed pending outcome of the special litigation committee's investigation; the consumer action settled in May 2015 for a reported \$10 million and the financial institutions action settled in December 2015 for a reported \$39 million. To date, Target has reportedly spent \$290 million related to the data breach. George Stahl, *Target To Pay \$10 Million in Class Action Over Data Breach*, WALL STREET J., Mar. 19, 2015, available at <http://www.wsj.com/articles/target-to-pay-10-million-in-class-action-over-data-breach-1426768681>; Reuters, *Target to Pay \$39 Million in Settlement with Banks Over Data Breach*, NBC News, Dec. 2, 2015, <http://www.nbcnews.com/tech/security/target-pay-39-million-settlement-banks-over-data-breach-n472996>. The shareholder litigation is ongoing and the company still faces probes by federal and state regulators.

⁶ See, e.g., Verified Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets, *Kulla v. Steinhafel, et al.*, No. 0:14cv203, 2014 WL 459982 (D. Minn. filed Jan. 21, 2014).

⁷ *Id.*

⁸ *In re Heartland Payment Sys., Inc. Sec. Litig.*, No. 09-1043 (D.N.J. filed Mar. 6, 2009). See also *Am. Consol. Class Action Complaint for Violations of the Federal Securities Laws*, 2009 WL 5197684 (filed Aug. 20, 2009).

⁹ *Am. Consol. Class Action Complaint for Violations of the Federal Securities*

Laws, No. 09-1043, 2009 WL 5197684 (D.N.J. filed Aug. 20, 2009).

¹⁰ *Id.*

¹¹ *In re Heartland Payment Sys., Inc. Sec. Litig.*, No. 09-1043, 2009 WL 4798148 at *8 (D.N.J. Dec. 7, 2009).

¹² See, e.g., *In re Goldman Sachs Grp., Inc. Sec. Litig.*, No. 10 CIV. 3461 PAC, 2015 WL 5613150 (S.D.N.Y. Sep. 24, 2015).

¹³ See *id.* at *1-2.

¹⁴ See note 5.

¹⁵ For example, in *Ruiz v. Gap, Inc.*, 380 F. Appx. 689 (9th Cir. 2010), the customer filed a negligence claim against a retailer alleging that the retailer owed him a duty to protect his Social Security number from unauthorized access, that the retailer breached its duty by allowing a third party to steal a laptop containing his Social Security number, and that the unauthorized access of his Social Security number caused him injury.

¹⁶ This distinction can be highlighted by comparing *Willingham v. Global Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702 at *18 (N.D. Ga. Feb. 5, 2013), in which the court recommended dismissal of a data breach negligence claim for lack of duty of care and concluded that there was no direct relationship between plaintiffs and defendant, with *Cumis Insurance Soc'y, Inc. v. Merrick Bank Corp.*, No. Civ. 07-374-TUC-CKJ, 2008 WL 4277877 at *34 (D. Ariz. Sep. 18, 2008), in which the court determined that plaintiffs could establish that defendant

owed a duty to safeguard voluntarily provided personal information if plaintiffs used defendant's product or were customers of defendant.

¹⁷ See *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 178 (3d Cir. 2008) (finding that because plaintiffs sought damages for fraudulent fees charged to their stolen credit cards, the economic loss rule barred plaintiffs' negligence claim); see also *In re Target Corp.*, 66 F. Supp. 3d 1154, 1171-76 (D. Minn. 2014). However, despite some defendants' successful reliance on the economic loss doctrine to avoid negligence-based data breach claims, other courts have carved out an exception to the economic loss rule bar where the plaintiff pleads a duty independent of any contract. See *In re Target Corp.*, 66 F. Supp. 3d at 1171-76 (holding that the economic loss rule did not bar plaintiffs' negligence claims in several states due to those states' independent-duty exception).

¹⁸ See, e.g., *In re Heartland Payment Sys. Customer Data Sec. Breach Litig.*, 834 F. Supp. 2d 566, 590 (S.D. Tex. 2011).

¹⁹ See *id.* (dismissing plaintiff's negligent misrepresentation claim for failure to prove that reliance on the representations was reasonable).

²⁰ See, e.g., *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1325 (11th Cir. 2012) (plaintiffs asserted, *inter alia*, a breach of contract claim against a health care plan provider alleging that the provider



LAW OFFICES OF SPICER & CHAMBERS, P.A.

The Law Offices of David W. Spicer, P.A. is pleased to announce that Jonathan W. Chambers has become a partner of the firm, now known as

The Law Offices of Spicer & Chambers, P.A.

Healthcare Law – Former Special Counsel for the Department of Professional Regulation focusing on personal representation of healthcare providers including Department of Health investigations, hospital credentialing matters, physician practice formation and dissolution, non-competition disputes, employment agreements, and Medicare and Medicaid investigations.

Personal Injury and Wrongful Death – AV Rated, Board Certified Civil Trial Law, Former Special Prosecutor for the Florida Judicial Qualifications Commission, with 36 years' experience in personal injury litigation. Supreme Court Certified Circuit Court Mediator.

429 S. Keller Road*
Suite 300
Orlando, FL 32810

8895 N. Military Trail
Suite 302E
Palm Beach Gardens, FL 33410

1637 Metropolitan Boulevard*
Suite C2
Tallahassee, FL 32308

WWW.DAVIDSPICERLAW.COM

d.spicer@davidspicerlaw.com
(561) 625-6066

Toll Free: (877) 34-SPICER
* available for consultation

breached its contract to provide health care by allowing the unauthorized access of their private medical information). In *Resnick*, the 11th Circuit vetted numerous Florida common law claims brought by the plaintiffs and the decision arguably serves as the most exhaustive judicial analysis of data breach claims premised on Florida common law causes of action.

²¹ See, e.g., *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 118 (D. Me. 2009) (customer alleging breach of implied contract against grocery store since the contract for the sale of goods did not include an express provision obligating the store to protect the customer's debit card information).

²² See, e.g., *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060, 2010 WL 2643307 at *38 (S.D.N.Y. 2010) (holding that when there are no direct dealings between plaintiff and defendant, the parties cannot create an implied contract).

²³ See, e.g., *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 329 (E.D.N.Y. 2005).

²⁴ The Florida Information Protection Act of 2014 (FIPA) imposes affirmative data protection duties upon covered entities and provides a detailed framework for providing notice in response to a data breach, but expressly states that it does not allow for a private cause of action. See, e.g., FLA. STAT. §501.171(10) (2015) ("This section does not establish a private cause of action."). While not affording aggrieved individuals a private cause of action, FIPA does provide enforcement mechanisms in the form of civil penalties up to \$500,000 per occurrence for noncompliant entities that fail to provide adequate or timely notice. FLA. STAT. §501.171(9) (2015).

²⁵ Beyond Florida, a few state statutes also provide a private cause of action which may enable plaintiffs to recover damages flowing from a security breach. See, e.g., N.Y. GEN. BUS. LAW §380 (New York Fair Credit Reporting Act); CAL. BUS. PROF. CODE §17200 (California's Unfair Competition Law); 815 ILL. COMP. STAT. 505 (Illinois Consumer Fraud and Deceptive Business Practices Act); MASS. GEN. LAWS Ch. 93A §2 (Massachusetts Unfair and Deceptive Trade Practices Act).

²⁶ FLA. STAT. §§668.801-805 (2015).

²⁷ 15 U.S.C. §1681, *et seq.*

²⁸ *Holmes*, No. 5:08-CV-00205-R, 2012 WL 2873892 at *15 (W.D. Ky. Jul. 12, 2012).

²⁹ 18 U.S.C. §2702(a)(1); see, e.g., *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 523 (N.D. Ill. 2011).

³⁰ See *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d at 523.

³¹ See, e.g., *Stollenwerk v. Tri-West Healthcare Alliance*, No. Civ. 03-0185PHXSRB, 2005 WL 2465906 at *2-6 (D. Ariz. Sept. 6, 2005).

³² See *Resnick v. AvMed, Inc.*, 693 F.3d at 1323-24 (11th Cir. 2012).

³³ *Id.*

³⁴ *Id.*

³⁵ *Id.*

³⁶ In federal data breach litigation, the issues of causation and damages typically have been cast in terms of "standing" under U.S. CONST. art. III, and has resulted in an incurable defect for many plaintiffs. Compare *Burrows v. Purchasing Power, LLC*, No. 1:12-CV-22800-UU, 2012 WL 9391827 at *2 (S.D. Fla. Oct. 18, 2012) (finding that plaintiffs established proper standing under art. III where their alleged damages — mainly identity theft — were "fairly traceable" to the defendants' actions of losing plaintiffs' PII) with *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1092 (N.D. Cal. 2013) (granting defendant's motion to dismiss where plaintiffs failed to allege legally cognizable injuries). A federal suit brought by a plaintiff without art. III standing does not have a "case or controversy," which is a fundamental prerequisite for federal subject matter jurisdiction. *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d at 1092. See also *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013).

³⁷ Also, the difference between actual damages (such as identity theft) and inchoate damages (such as anticipated identity theft or financial harm) creates further complications for plaintiffs attempting to demonstrate commonality for purposes of class litigation. See *Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541 (2011).

³⁸ See, e.g., *Fanin v. U.S. Dep't of Veterans Affairs*, 572 F.3d 868, 874 (11th Cir. 2009) (affirming summary judgment against plaintiffs' claims for monetary damages under the Privacy Act because the plaintiffs, victims of data loss, failed to show any pecuniary loss from the data breach of their PII, and their allegations of increased stress and anxiety were legally insufficient to support their claimed damages).

³⁹ See *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 155 n.2 (1st Cir. 2011).

⁴⁰ See, e.g., *Pisciotta v. Old Nat. Bancorp.*, 499 F.3d 629, 635, 640 (7th Cir. 2007) (holding that allegations of increased risk of future harms is not a cognizable injury and will be insufficient to state a claim in tort or contract).

⁴¹ *Grigsby*, No. C12-0553JLR, 2012 WL 5993755 (W.D. Wash. Nov. 14, 2012).

⁴² See, e.g., *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 911 (N.D. Cal. 2009), *aff'd*, 380 F. Appx. 689 (9th Cir. 2010).

⁴³ See, e.g., *Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006) (holding that plaintiffs' expenditure of time and money was not the result of a present injury, but rather the anticipation of immaterialized future injury, which was not a cognizable injury).

⁴⁴ See, e.g., *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 131 (D. Me. 2009).

⁴⁵ See *id.*; see also *Ponder v. Pfizer, Inc.*, 522 F. Supp. 2d 793, 797 (M.D. La. 2007).

⁴⁶ *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 711 (D.C. 2009).

⁴⁷ National Institute of Standards & Technology, *NIST Releases Cybersecu-*

rity Framework Version 1.0 (Feb. 12, 2014), available at <http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm>.

⁴⁸ See 17 C.F.R. Part 248.

⁴⁹ U.S. Securities & Exchange Commission, *SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach* (Sept. 22, 2015), available at <http://www.sec.gov/news/press-release/2015-202.html>.

⁵⁰ See 15 U.S.C. §§41-58.

⁵¹ *F.T.C. v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015).

⁵² In December 2015, Wyndham agreed to settle the charges brought by the FTC. Wyndham was not fined or required to admit wrongdoing, but agreed to comply with multiple technology and data protection standards designed to protect cardholder data. See Federal Trade Commission, *Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk* (Dec. 9, 2015), available at <https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment>.

⁵³ Lawmakers have not been deaf to cybersecurity concerns, as various new federal statutes have been proposed to help unify cybersecurity standards and enforcement. Over the past few years, several pieces of legislation have been introduced in Congress, including the Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014), the Data Security Act of 2014, S. 1927, 113th Cong. (2014), and the National Cybersecurity and Critical Infrastructure Protection Act of 2013, H.R. 3696, 113th Cong. (2013). However, none of these legislative initiatives have been enacted into law as of this writing.

Michael Hooker is a partner in the commercial litigation practice group with Phelps Dunbar in Tampa. During his more than 30-year career, he has litigated a variety of complex commercial actions. Hooker is a past president of the Hillsborough County Bar Association, the Hillsborough County Bar Foundation, and the Federal Bar Association, Tampa Bay Chapter. He currently serves as a representative of the 13th Judicial Circuit on The Florida Bar Board of Governors.

Jason Pill is an associate in the labor and employment practice group with Phelps Dunbar in Tampa. He assists clients in handling unique issues that arise at the intersection of law and technology.

The authors thank Matthew Perez, an associate at Phelps Dunbar, for his assistance in researching this article.