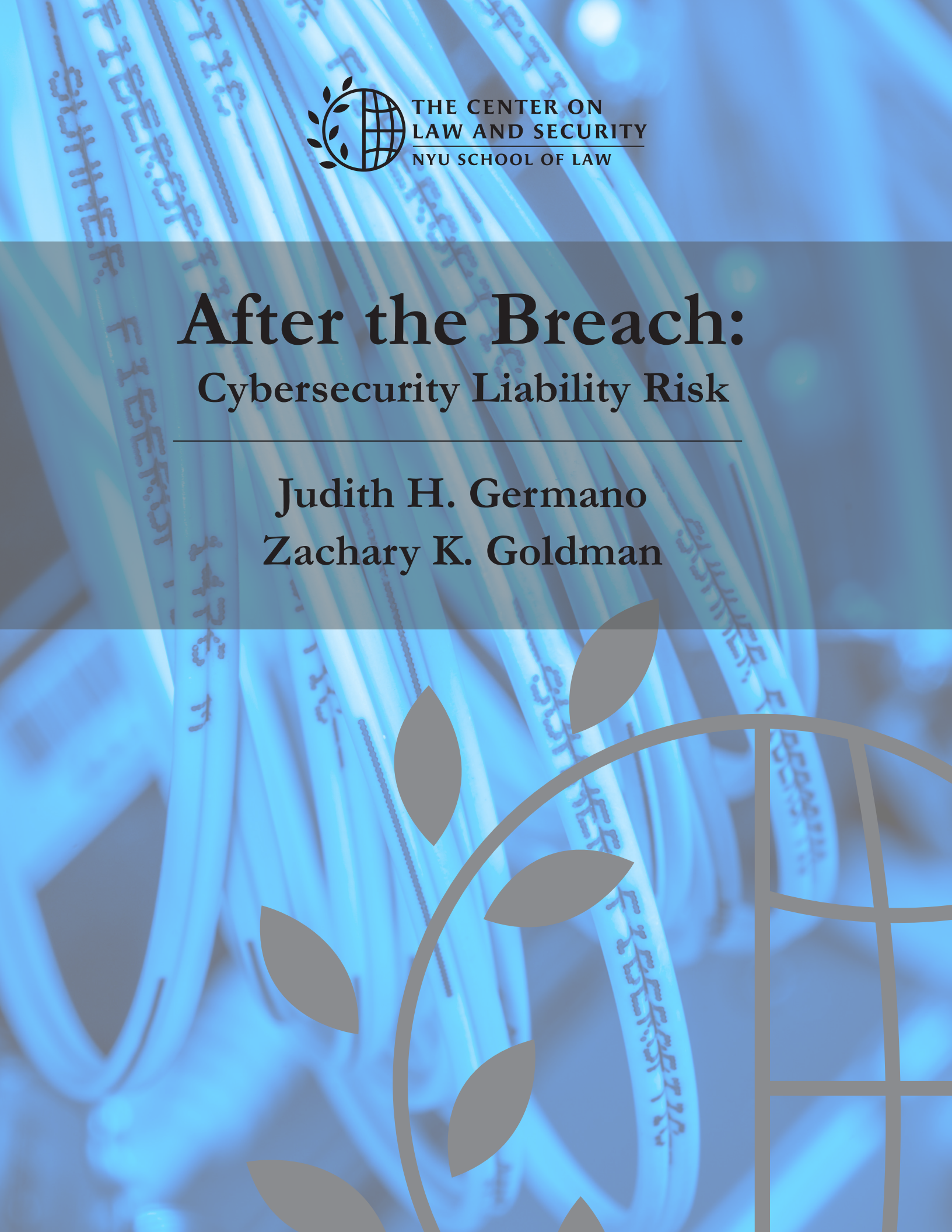

THE CENTER ON
LAW AND SECURITY
NYU SCHOOL OF LAW

After the Breach:
Cybersecurity Liability Risk

Judith H. Germano
Zachary K. Goldman

After the Breach:
Cybersecurity Liability Risk

Judith H. Germano
Zachary K. Goldman

The Center on Law and Security
New York University School of Law
139 MacDougal Street
New York, NY 10012
212.992.8854

CLS@exchange.law.nyu.edu
www.lawandsecurity.org

Cybersecurity's evolving regulatory and liability landscape compounds the challenges that companies face from cyber attacks, and further complicates the ability of corporate executives and their advisors to understand and effectively manage cyber risk. Companies must prepare for and respond to a potential cyberattack's direct damage, including financial and data loss, system and service interruptions, reputational harm and compromised security. Cyberattacks also expose companies to diverse and uncertain regulatory and civil liabilities. Although these risks generally become apparent post-breach, they must be contemplated and managed proactively, before a breach occurs.

The decision-making of companies that are facing systematic and strategic cyber threats is, therefore, fraught with legal uncertainty about the implications of how they prepare for and respond to the threat. With piecemeal statutes and regulations, and emerging technologies, companies must navigate myriad potential sources of civil and criminal liability related to cyber incidents whose doctrinal contours are unsettled. Concerns include, for example, how to: Institute and monitor security protections; implement cyber incident response policies and procedures; disclose threat, vulnerability and incident information; and determine when, whether and how best to inform, and potentially cooperate with, government. In addition to the inherent difficulties in determining how to address these concerns, companies also must evaluate how each of those decisions may impact litigation risk.

These concerns are particularly acute because many of the most serious cyber vulnerabilities reside in privately-owned networks and systems, those systems often contain some of the most valuable information available about the nature of the threat, and, ultimately, steps to prevent and mitigate harms must be implemented largely by the private sector. Unless we understand better the factors shaping the private sector's response to cyber harms, including the ways in which litigation risks shape strategic decisions about cybersecurity, it will be difficult to comprehensively address the threat. And while governments traditionally have been charged with protecting the national interest, that role, in a digital era, is increasingly also played by private companies. To the extent that an unsettled liability landscape shapes private sector decisions about investing in cybersecurity protections, disclosing cyber incidents to the public, and cooperating with government, the problem is no longer exclusively one of legal rights and remedies, but also one of strategic cyber preparedness.

Managing this shifting landscape requires executives, including at the board and senior leadership level, not only to confirm that adequate technological defenses are in place, but also to think strategically regarding how to create and implement corporate governance, and communication and response structures, to manage cyber risk. This means ensuring that the organization effectively can identify and address emerging regulatory and liability issues on both a proactive and responsive basis. Moreover, because systems can be compromised at any level, it also involves communicating (through training and protocols) the significance and means of properly managing cybersecurity risk.

PIECING TOGETHER A FRAGMENTED LANDSCAPE

The regulatory duties and liability risks that companies now face take many forms, and go far beyond requiring a determination of whether and when a breach is sufficiently material to trigger (where applicable) SEC and state disclosure obligations. Companies also might face potential enforcement and private civil actions brought by, for example:

- The FTC
- The SEC
- State attorneys general
- The U.S. Department of Justice
- Plaintiffs whose data is compromised (e.g., customers, clients, corporate partners, vendors, unrelated third-parties including affected banks, etc.)
- Shareholders

Congress also has conducted inquires of varying levels of formality in response to data breaches, and companies may be accountable to regulatory agencies, including the Consumer Financial Protection Bureau (CFPB), Federal Communications Commission (FCC) and Department of Health and Human Services (HHS), among others.

Litigation concerns are compounded by the piecemeal condition of state and federal laws governing cybersecurity obligations. The mixture includes fragmented statutes and regulations, and evolving common law standards that pose an obstacle to formulating stable expectations about cybersecurity behavior. Despite legislative efforts and extensive discussions, there is currently no U.S. federal data breach notification law. Instead, there exists a patchwork of sometimes contradictory state data breach notification laws. With the addition of Kentucky on April 10, 2014, forty-seven U.S. states, as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands, have enacted legislation requiring private or government entities to notify individuals of security breaches of personally identifiable information. (Kentucky's new law will be effective July 14, 2014; the only states still without data breach notification laws are Alabama, New Mexico and South Dakota.)

In the context of this uncertainty, government enforcement has become more aggressive, and the plaintiffs' bar increasingly more active, in this area. Recent legislation being discussed in the U.S. (and passed in the U.K.) focuses on making corporate victims more accountable for breaches. And the May 13, 2014 EU Court of Justice decision finding that Google Inc. is subject to Spanish data protection law[1] has far-reaching implications for international companies, who may now find themselves subject to the reach of different national data protection laws in the EU. Moreover, despite legislative efforts, current laws do not adequately protect companies who share information with government. Indeed, there have been concerns that the Electronic Communications Privacy Act (ECPA) and Antitrust laws in their current form could be applied to bring civil or criminal actions against companies for sharing such information.[2]

Given this environment, the extant legal regime does not provide clear guidance to companies that are looking to effectively manage not only cyber incidents themselves, but also attendant liabilities. Moreover, in light of the uncertainty and broad range of potential exposure, a victim-defendant understandably may be reluctant to disclose threat and incident information voluntarily to the government, or may delay disclosure because of concerns that statements might be used against it in subsequent legal proceedings.

In this context, where sources of liability are fragmented and expanding, the appropriate strategic relationship between industry and government remains, in many respects, unclear. For example, timely disclosure and information-sharing can help companies and government in many ways, including by exposing threats and vulnerabilities to enable a swift, coordinated and more effective response. Timely disclosure also facilitates effective cooperation about how best to prevent, detect and address potential harm. But that same cooperation could, potentially, harm companies in subsequent civil litigation, or may prematurely escalate an incident and cause a company to lose control of an investigation. Different government agencies also take different approaches to disclosure, with some encouraging enhanced cooperation, while others increasingly focus on holding companies accountable, civilly and possibly criminally, when their systems are breached.

What is the proper way to reconcile, or balance, the desire to assure companies that cooperation is beneficial and not an undue risk, while also holding them accountable for deficient security measures or for failing to provide timely and adequate disclosures of cyber vulnerabilities and attacks? The public and private sectors are struggling with that question, and legislative efforts thus far have fallen short of providing an adequate answer. In this milieu, it is important to understand the various types of regulatory and litigation risk that companies are facing.

Theories of liability revolve around both the actual breach, and the company's response to the breach, including regarding the content and timing of notice and disclosure. And exposure can be grounded in statutory, regulatory, and common law. Recent breaches have triggered a variety of claims based on inadequate security measures constituting unfair or deceptive practices, breach of contract, negligence, unjust enrichment, breach of fiduciary duty and duty of care, and negligent misrepresentation.

1 *Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez*, Case C-131/12, 13 May 2014, available at http://curia.europa.eu/juris/documents.jsf?num=C-131/12

2 The U.S. Department of Justice and Federal Trade Commission issued a joint statement on April 10, 2014, that "properly designed" cyber threat information sharing "is *not likely* to raise antitrust concerns." Available at http://www.justice.gov/opa/pr/2014/April/14-at-365.html

This article highlights below several noteworthy cases in order to demonstrate some of the various theories of liability (and diverse actors employing them) that are driving behavior with respect to cybersecurity, and shaping the ways in which government and the private sector interact in order to mitigate resulting harms.

New York Presbyterian/Columbia University Medical Center

On May 7, 2014, agreement was reached on the largest fine to date to settle allegations of patient privacy violations – $4.8 million – between New York Presbyterian Hospital and Columbia University Medical Center and the Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS). The case involved HIPAA violations pertaining to records of 6,800 patients (including patients' status, vital signs, medication and lab test results) that inadvertently were exposed to the Internet in 2010, when a Columbia University physician who had developed applications for the hospital and the university attempted to shut down a personally owned computer server on the network. The OCR reported that, due to the lack of technical safeguards, this deactivation resulted in ePHI (electronic protected health information) being accessible on Internet search engines. The breach was revealed when an individual discovered, via an Internet search, a deceased partner's hospital medical records; both entities then submitted a joint breach report disclosing the breach of their shared data network. This was one of approximately 985 breaches (accounting for 31.3 million compromised records) posted on OCR's website,[3] created pursuant to Section 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, Pub. L. 110-185, 122 Stat. 619. That law requires HHS to post a list of breaches of unsecured protected health information affecting 500 or more individuals.

3 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Target Breach

On Monday, May 5, 2014, Target CEO Gregg Steinhafel was ousted following a major cyberattack that compromised the personal data of millions of shoppers during the 2013 holiday season. Target's concern reportedly was that the CEO moved too slowly in increasing Target's defenses despite warnings regarding vulnerabilities in point-of-sale terminals, along with other problems in Target's pre-incident planning and post-incident response. This sequence of events sends a resounding message that senior executives and board members bear the risk of a cyber breach and need to understand and combat the threat. The Target attack, in which 40 million payment card records and 70 million other customer records were stolen, also illustrates the multiple (and multiplying) sources of liability to which companies can be subject after a cyber incident. Target now faces dozens of class actions (the number was reported at approximately 70 at one point, with seven filed the day Target disclosed the breach). Several of the lawsuits claim that the plaintiff-customers could have done more to protect themselves if Target had notified them of the breach immediately. And Target's Board and senior managers are facing a shareholder derivative suit for their "responsibility for, release of false and misleading statements concerning, and the bungling of the aftermath of the *worst data breach in retail history.*" Complaint at ¶4, *Collier v. Steinhafel*, No. 0:14cv00266, 2014 WL 321798 (D.Minn., filed Jan. 29, 2014). Target also faces potential action from banks seeking reimbursement for millions of dollars in losses due to fraud and the cost of replacing compromised debit and credit cards. In April 2014, the U.S. Judicial Panel on Multidistrict Litigation ordered that the lawsuits accusing Target of failing to protect customers from a data breach will be consolidated in Target's home state of Minnesota, before U.S. District Judge Paul Magnuson. This order encompassed 33 lawsuits across 18 districts, and potentially a large number of additional "tag-along" actions.

The DOJ stated it was looking into potential criminal charges, and state attorneys general have instituted actions under state security breach notification laws. On top of these sources of legal liability, Target also is subject to a congressional inquiry – Congress summoned Target's

CFO to appear before the Senate Judiciary Committee on February 4, 2014, and a House committee is seeking extensive documents from Target about its security program.

Despite calls by some that corporate victims of a breach should provide immediate notice to affected parties, the Target case also reveals the extent to which assessing the scope of the breach can take time. For days and weeks after the breach was announced, the public received increasing revelations regarding the extent and nature of the information compromised, thereby illustrating the tension that often exists between expediency and accuracy of breach notifications. In its 10-K annual report filed with the SEC months after the breach was discovered, on March 14, 2014, Target stated: "Our investigation of the matter is ongoing and it is possible that we will identify additional information that was accessed or stolen, which could materially worsen the losses and reputational damage we have experienced." That report was released just a day after Target admitted that it had declined to act on an early alert of a cyber breach detected by its FireEye security system, and that Target's security team had, at some point before the attack, disabled the function that automatically deletes malicious software (to avoid grappling with false positives that would halt email and legitimate web traffic).

Wyndham Hotel Group

As of February 2014, the Federal Trade Commission (FTC) had brought 50 civil actions against companies for data security issues, alleging violations of Section 5 of the FTC Act (prohibiting unfair or deceptive practices affecting commerce),[4] as well as violations of the Gramm-Leach-Bliley Act[5] and the Fair Credit Reporting Act.[6] *Stmt. of FTC Chairwoman Edith Ramirez to U.S. Senate Judiciary Committee, Hearing on Privacy in the Digital Age: Preventing Data Breaches and Combatting Cybercrime, February 4, 2014.* Among those actions is the FTC's $10.6 million civil suit alleging that Wyndham Hotels and Resorts violated Section 5 of the FTC Act related to breaches impacting approximately 619,000 credit card accounts of Wyndham guests.

The Wyndham case may be the most important of those actions, at least from the perspective of the legal community, because it implicates the scope of the FTC's statutory authority to regulate private companies' data security practices and (along with LabMD) may be the first fully-litigated privacy case under Section 5. (Wyndham also is facing actions from various state attorneys general.) The FTC charged that Wyndham engaged in "unfairness and deception" by: Failing to adequately secure hotel guests' personal information in light of three data breaches in two years; insufficiently clarifying the relationship between franchisees and Wyndham regarding data security; and misstating, in its privacy policy, the precautions that Wyndham took to secure customer data.

In a highly anticipated ruling, on April 7, 2014, U.S. District Judge Esther Salas, of the U.S. District Court in New Jersey, denied Wyndham's motion to dismiss the FTC case, finding that: (1) the FTC has authority under Section 5 to bring actions against companies that fail to provide reasonable security for personally identified information that they possess; (2) despite a lack of established data-security rules that would advise companies what constitutes "reasonable" data security, the FTC has provided sufficient fair notice via guidance, consent orders and draft complaints and therefore can proceed on a case-by-case basis against companies the FTC believes have not provided reasonable security; and (3) the FTC complaint set forth sufficient allegations of unfairness and deception to survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6).[7] Ten days later, Wyndham moved the court for permission to immediately appeal that decision, arguing the case presented "hotly contested and critically important" issues regarding the scope of the FTC's statutory authority. In a brief filed May 5, 2014, the FTC opposed that request, urging that the court allow the case to proceed in the trial court.

4 Section 5 of the FTC Act, Title 15, United States Code, Section 45, prohibits "unfair or deceptive acts or practices in or affecting commerce."
5 The Gramm-Leach-Bliley Act (GLBA), Pub. L. 106-102, 113 Stat. 1338 (enacted Nov. 12, 1999), requires financial institutions (companies offering financial products or services including loans, financial or investment advice, or insurance) to explain their information-sharing practices to their customers and to safeguard sensitive data.
6 The Fair Credit Reporting Act (FCRA), Title 15, United States Code, Section 1681, regulates how companies collect, use, disseminate and dispose of certain consumer information, including consumer credit information.

7 In assessing a Rule Fed. R. Civ. P. 12(b)(6) motion, the court must accept the facts alleged in the complaint as true. The FTC still must, as the litigation proceeds, provide sufficient evidence to support its claims of unfairness and deception against Wyndham to survive a motion for summary judgment and ultimately to prevail at trial.

Accretive Health

The line of cases against Accretive Health, a provider of medical billing and revenue management services to hospitals, illustrates the wide range of claims and lasting impact that can occur from a single event. In July 2011, an Accretive laptop containing over 600 files with information relating to 23,000 patients was stolen from an employee's car in Minnesota. The data on the laptop included sensitive personal and health information, such as patient names, billing information, diagnostic information, and Social Security numbers; information beyond what the employee needed to do his job. Consequently, Accretive faced a lawsuit brought by the Minnesota attorney general; investigations before two congressional committees, the FTC and state regulatory agencies; and securities and consumer lawsuits. The lawsuits and investigations alleged that the company's policies and practices violated HIPAA, the Fair Debt Collection Practices Act, Section 5 of the FTC Act, and other state privacy, debt collection and consumer protection laws. Accretive settled with the Minnesota attorney general and the FTC. As part of the December 31, 2013 FTC settlement, Accretive is required, for 20 years, to implement a comprehensive information security program and submit the program for evaluation every two years by a certified third party.

Kaiser Foundation Health Plan

The Kaiser action pertains to the potential negative consequences of delay in notifying consumers of a data loss. Kaiser ultimately settled unfair competition claims brought by California's attorney general alleging that Kaiser improperly waited four months to notify more than 20,000 current and former employees that their personally identifiable information ("PII") had been compromised when an unencrypted hard drive containing the PII was purchased at a thrift shop in 2011. The court found that Kaiser had gathered sufficient information to notify some of the individuals after the recovery of the hard drive in December 2011 and prior to the end of its investigation in February 2012.

TJX Companies

The TJX cases involve shareholder derivative and other civil actions by individuals and entities following a data breach. More than two-dozen civil class actions followed a major data breach and loss of customer credit card data, as did a derivative suit by a municipal pension fund shareholder in the Delaware Court of Chancery. Litigation theories included that the company failed to comply with Payment Card Industry Data Security Standards (PCI DSS), and breach of fiduciary duty for failing to ensure sufficient security. *La. Mun. Police Emp.'s Ret. Sys. v. Alvarez, et al.*, C.A. No. 5620-VCN, 2010 WL 2709960 (Del. Ch. Filed Jul. 2, 2010).

Patco Construction

The *Patco* case centers on the appropriateness of a victim-defendant's security measures. People's United Bank was found to have violated the UCC by having " commercially unreasonable" electronic transfer security features after six fraudulent electronic funds transfers were made from Patco's account. The bank's security system flagged the transactions as suspect but did not notify the customers of the information or block the transfers. *Patco Constr. Co., Inc. v. People's United Bank,* 684 F.3d 197, 213 (1st Cir. 2012).

Hannaford Brothers

Hannaford illustrates a breach of contract litigation arising from a massive payment card data breach. Hackers stole 4.2 million debit and credit card numbers from Hannaford, resulting in at least 1,800 incidents of fraud. Hannaford faced claims based on breach of an implied contract that Hannaford would take reasonable measures to protect the information from breaches. *Anderson v. Hannaford Bros. Co.,* 659 F.3d 151 (1st Cir. 2011).

Heartland Payment Systems

Liability in the Heartland case was grounded on a theory of negligence. The Fifth Circuit upheld plantiffs' negligence theory based on Heartland's failure to protect payment card processing information as evidenced by a massive data breach. *Lone Star Nat'l Bank, N.A. v. Heartland Payment Systs., Inc.,* 729 F.3d 421 (5th Cir. 2013).

Moreover, whether companies are insured, under commercial general liability (CGL) coverage policies, for litigation costs and other losses stemming from cyber attacks, is not always clear. For example, in *Zurich American Insurance Company v. Sony Corporation of America, et al.*, Index Number: 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014), the New York trial court ruled that, based on a CGL policy, Zurich had no duty to defend Sony in litigation stemming from the 2011 attack on Sony's PlayStation Network. That attack exposed account data on close to 100 million people and compromised more than 12 million credit and debit cards, resulting in more than 60 class actions nationwide against Sony. (Sony, however, also does have cyber-specific policies in addition to the CGL.) The *Zurich* decision is contrary to a November 2013 federal ruling that a CGL policy did, in fact, cover a data breach involving hospital records of approximately 20,000 patients. *Hartford Cas. Ins. Co. v. Corcino & Associates*, CV 13-3728 GAF JCX, 2013 WL 5687527 (C.D. Cal. 2013).

MANAGING THE RISK

Ultimately, the divergent theories of liability against which companies might need to defend derive from important differences in the goals and methods of different cyber actors, and the different institutions within the United States that have responsibility for cybersecurity. The SEC, FTC, and state attorneys general all have different mandates and focus on guarding against different kinds of harms. When the perpetrator is an organized crime group, whose objective is to steal and then sell payment card or other personal data for a quick profit, there is potentially a large number of people affected—some of whom subsequently turn into plaintiffs. DHS, FBI, the Secret Service, and other national security-focused government agencies, in turn, tend to seek different kinds of relationships with companies that have been the subject of a breach. They also address different kinds of threats, including state-sponsored advanced persistent threats seeking sensitive intellectual property and valuable trade secrets, which do not always lead to identifiable harms outside the company that will generate lawsuits.

Directors and senior corporate officers are challenged, therefore, to determine how to avoid (or at least reduce) liability risk related to cyber attacks. Indeed, as the *Target* case shows, their jobs can depend upon it. Successfully navigating this complex regulatory and enforcement environment requires collaboration within companies, among the legal, technical, information security and senior leadership teams. Moreover, companies also must determine whether, when, how and why to cooperate with the government on these issues.

This requires determining, implementing and testing effective governance structures for balancing those concerns while making and executing effective and timely decisions regarding cybersecurity cooperation and response. Much of this comes down to effective internal corporate communications, and requires getting the right people in the room speaking a common language, in a cybersecurity-focused discussion facilitated by internal, and sometimes external, experts. Some companies are doing that more effectively than others. Given the broad and serious nature of cyber-related liability risks that companies face, it is essential for senior leaders to address those governance and communication issues effectively before the next breach, to encourage and prepare a coherent, strategic approach to managing cybersecurity risk.

THE CENTER ON LAW AND SECURITY

The Center on Law and Security is a non-partisan multidisciplinary research institute at NYU School of Law focused on promoting informed dialogue and conducting groundbreaking research on the most important national security, legal, and strategic questions of the post-9/11 era. The Center is led by its Faculty Director, Professor Samuel Rascoff, and its Executive Director, Zachary Goldman.

Judith H. Germano is a Senior Fellow at the Center on Law and Security, and Adjunct Professor of Law at NYU School of Law. She is also the founding member of GermanoLawLLC. Judith specializes in cybersecurity, privacy, securities and other financial fraud, and regulatory compliance matters, and is the former Chief of Economic Crimes at the U.S. Attorney's Office, District of New Jersey.

Zachary K. Goldman is the Executive Director of the Center on Law and Security at NYU School of Law. Zachary served as a Policy Advisor in the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence, and as a Special Assistant to the Chairman of the Joint Chiefs of Staff.

Max E. Rodriguez, NYU School of Law Class of 2015, contributed to the research for this article.