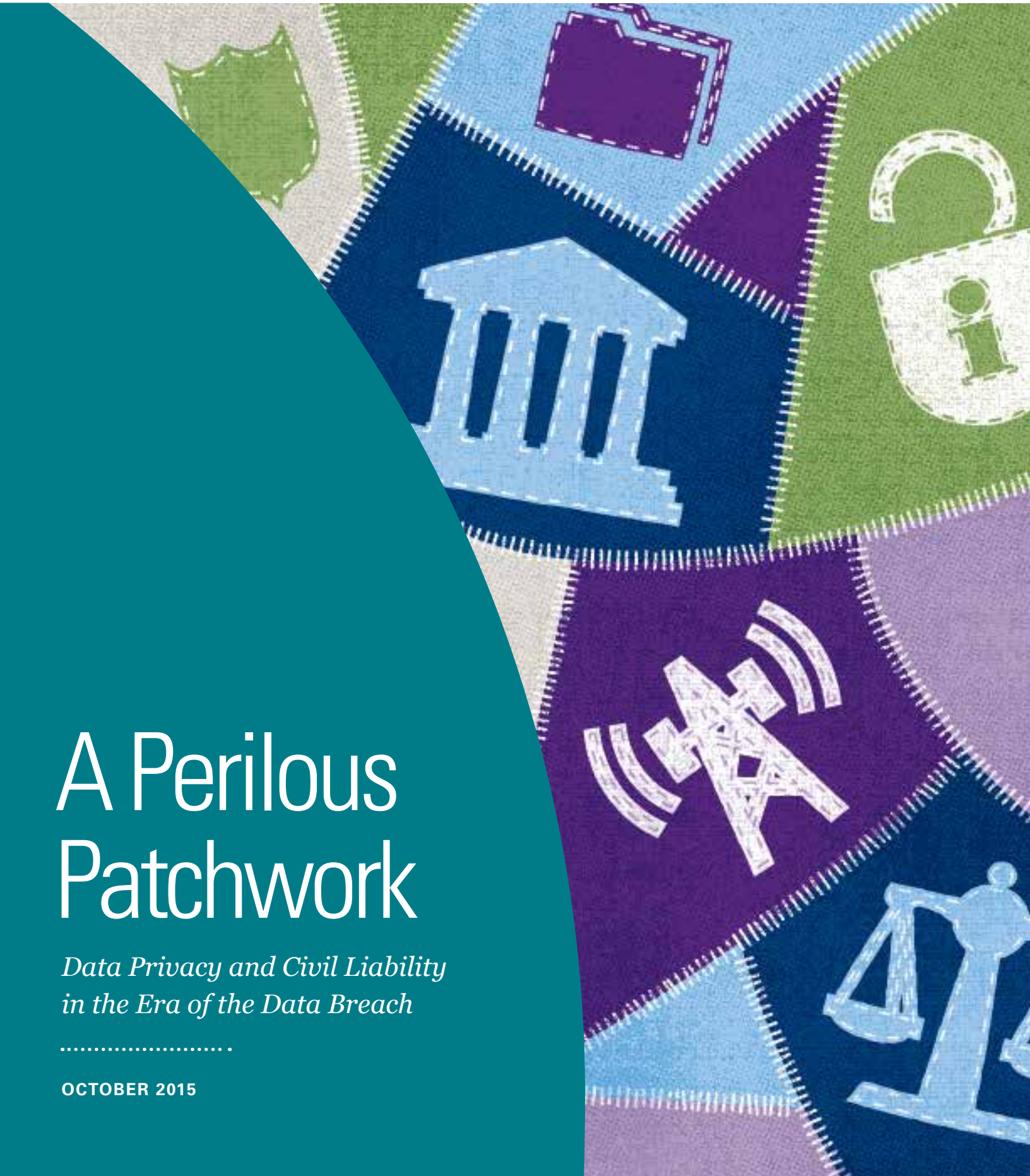
U.S. CHAMBER
Institute for Legal Reform



A Perilous Patchwork

Data Privacy and Civil Liability in the Era of the Data Breach

OCTOBER 2015

U.S. CHAMBER
Institute for Legal Reform

An Affiliate of the U.S. Chamber of Commerce

Table of Contents

Prepared for the U.S. Chamber Institute for Legal Reform by

Liisa M. Thomas, Robert H. Newman, and Alessandra Swanson, Winston & Strawn LLP[i]

Executive Summary

After a data breach, companies are often accused of having failed to adequately protect their customers' information, with that failure—so the argument goes—having led to the breach. Who brings these allegations? Many may think that they are brought by "the government." However, there is no single agency in the United States charged with enforcing data protection. Instead, there is a patchwork of regulatory agencies that handle these issues, depending on both the nature of the company's business and the activities in which it engages.

Historically, the Federal Trade Commission (FTC) has taken the lead in privacy law enforcement, largely bringing privacy violation actions under an unfair or deceptive trade practice theory. Now, however, with the rise of security breaches and an ever-increasing ability for companies to collect, store, and make use of consumer data, state attorneys general (AGs) and the class action bar are joining the brigade by bringing privacy-related actions under varied legal theories. This medley of enforcers and laws, coupled with the evolving nature of privacy concerns generally, means that companies in the United States face significant compliance challenges both when developing new products and technology and when establishing or refining programs to protect existing data and information systems.

On June 17, 2015, Medical Informatics Engineering (MIE), a software and IT company that focuses on the healthcare industry, began notifying people that it had suffered a breach earlier in the year and that individuals' personal information was potentially exposed to a hacker. Within two months, MIE was hit with three class action lawsuits, an inquiry from the Indiana Attorney General, and a federal investigation from the Department of Health and Human Services (HHS). Before MIE even had time to understand the circumstances surrounding the breach, they had to gear up to fight five—and counting—major legal battles.

We are living in an age where major data breaches are the norm, and class action lawsuits and regulatory inquiries have followed for many companies. In 2015 alone, four major breaches—affecting the federal

> *We are living in an age where major data breaches are the norm, and class action lawsuits and regulatory inquiries have followed for many companies.*

government,[1] Anthem,[2] Premera Blue Cross,[3] and UCLA[4]—together potentially exposed the information of 125 million people.[5] And while these are some of the largest breaches this year, there are many others, likely including some yet to be discovered.

Regulatory Enforcement

Regulators have been increasingly active in bringing and sustaining lawsuits against breached entities. The FTC, in particular, has been aggressive in pursuing enforcement actions in this area. The FTC has the authority to bring suit under Section 5 of the FTC Act, which prohibits companies from using unfair or deceptive practices.[6] The FTC is not the only federal regulator on the beat, as other agencies—like the Federal Communications Commission (FCC), the Securities and Exchange Commission (SEC), and HHS—are exercising their authority to bring enforcement actions under industry-specific laws such as the Communications Act of 1934 and the Health Insurance Portability and Accountability Act (HIPAA). Historically, these agencies would stake out their own territory. Now, however, with the increase of cybersecurity incidents, the agencies are starting to extend and stretch their jurisdiction to lead enforcement actions against entities that were not traditionally under their purview. For example, the FCC, an agency best known for its governance over television, telephone, and radio, recently attempted to expand its jurisdiction to oversee Internet carriers,[7] which is an area traditionally regulated by the FTC. At the same time, other agencies are getting into the privacy space, when they had not traditionally focused on these issues in the past. For example, the SEC, whose primary function is to regulate the securities industry and maintain market integrity, released cybersecurity guidance and strongly urged entities under its purview to review their data security protocols.[8] The FCC and SEC are two major players in the regulatory landscape that are departing from their traditional confines and signaling that they are interested in data privacy and security standards. This likely means that it will be more perilous for companies to navigate data breaches, as they will not know for sure to which agency—or agencies—they will be accountable in the aftermath.

In addition, many states have laws that closely mirror the FTC Act and enable both state AGs and individuals to bring an action if a company has engaged in an unfair or deceptive practice. On both the federal and state levels, data breach cases are generally based on allegations of a company's disregard for its own data security practices putting consumer's personal data at risk, and—in some cases—whether this constituted an unfair or deceptive practice.

Navigating Private Causes of Action

Despite the uptick in regulatory actions, plaintiffs have also been aggressive in seeking their day in court. Until recently, many classes of affected individuals have struggled to find an adequate cause of action to assert their claims. Because there is no federal law that specifically offers relief for data breaches, classes have been throwing a wide assortment of claims against the wall to see what sticks. Among them are federal laws such as the Fair Credit Reporting Act (FCRA), as well as common law principles such as negligence. Plaintiffs have also had difficulty establishing standing because they often do not have a concrete injury to demonstrate to the court.

What does all of this mean? As companies face the reality that they may be the next victim of a data breach, they must also understand and prepare themselves for the additional legal challenges that could follow. This is an area of the law that is constantly developing, and as explained below, courts have had different interpretations of what plaintiffs must show to maintain a suit. Given this, companies should carefully follow regulatory cases and settlements in order to better understand what the FTC and other agencies are looking for when they investigate and pursue enforcement actions related to data security.

> *"As companies face the reality that they may be the next victim of a data breach, they must also understand and prepare themselves for the additional legal challenges that could follow."*

To help companies understand the extent of the risk and identify effective mitigation techniques, this paper begins by examining the current landscape of private rights of action and consumer class actions in the data privacy space. The paper then turns to enforcement at the federal level, focusing most acutely on the FTC, as it has been—and will likely continue to be—at the helm of the government's enforcement efforts in this area. Finally, the paper examines the burgeoning enforcement activity at the state level, led by increasingly active state AGs. Taken together, it is clear that businesses are faced with a multifaceted enforcement landscape, which adds a significant layer of complexity to the existing collection of data-privacy-related laws that companies must juggle.

Who Are the Regulators?

When a company suffers a data breach, depending on the substance of the data at issue, it may be required to notify not only affected individuals but also regulatory agencies. This might include their industry regulator, if they are in a regulated industry, or a state authority, if the state law places such an obligation on companies that have suffered a breach. These notifications often turn into formal inquiries, where the regulators do not focus on the notification itself, but instead take the opportunity to investigate the company's security protocols and whether they resulted in the incident.

Often, this results in an inquiry of the totality of the company's security operations.[9] In some cases, this gives rise to formal enforcement actions with public-facing settlement documents.[10] In essence, companies are made to raise their hands, step in front of the proverbial class, and willingly have an example made out of themselves. Even companies that do not have an obligation to give notice may nevertheless find themselves facing the spotlight of regulatory scrutiny from the FTC or a state attorney general's office simply because someone at one of those entities read about the incident in the press or was impacted by the incident.[11]

Because there is no double-jeopardy-type prohibition for regulatory breach inquiries, companies may be forced to juggle investigations from multiple agencies.[12] The breadth of the investigations may depend on a number of variables, including the severity of the breach and the regulator's priorities and caseload at the time. However, regulators that have the resources and the interest in a certain breach can undertake years-long investigations, examining companies' data security practices under a microscope, and ultimately requiring hefty settlement amounts and constrictive corrective action plans.[13] These inquiries could also have other implications, as the regulators may come upon information unrelated to the breach that could ultimately affect the final outcome of the case.

> *"[R]egulators that have the resources and the interest in a certain breach can undertake years-long investigations, examining companies' data security practices under a microscope, and ultimately requiring hefty settlement amounts and constrictive corrective action plans. These inquiries could also have other implications, as the regulators may come upon information unrelated to the breach that could ultimately affect the final outcome of the case."*

For example, in 2011, Accretive Health, a company that provides finance-related services to the healthcare industry,[14] suffered a breach when an employee lost a laptop that contained the health information of approximately 23,000 individuals.[15] The breach triggered inquiries from both the Minnesota Attorney General's office and the FTC. During the state's investigation into the data breach, it uncovered information about what it ultimately deemed to be inappropriate debt-collection practices by Accretive.[16] This additional information was used against Accretive in its July 2012 settlement, which included a $2.5 million dollar fine and a two- to six-year ban from operating its business in Minnesota.[17] However, Accretive's regulatory woes were only beginning, as the FTC later settled with the company over its alleged failure to appropriately safeguard its data.[18] While the FTC opted not to include Accretive's debt collection actions in its enforcement action,[19] the settlement agreement includes specific corrective actions that Accretive must take to strengthen its data security program, as well as a 20-year period of monitoring by the FTC.[20]

As demonstrated by the Accretive example, regulators are confident in their ability to investigate breaches, even if other agencies are already involved, and will use information peripheral to the cause of the breach in their enforcement actions. The breach may bring the regulators to the door, but once companies let them inside—willingly or not—the regulators may use any of the information collected during an investigation to help determine the scope of their enforcement actions. It is therefore important for companies to know the major players in this arena, and to understand from where regulators derive their investigative authority and what their resulting enforcement actions look like.

Regulated Industries

The FTC might be the most recognizable name in the breach enforcement landscape, but it certainly isn't the only one with an interest in this area. Other regulatory agencies, such as those that are granted enforcement power under the Gramm-Leach-Bliley Act (GLBA) or HIPAA, may have purview depending on the industry involved in a beach. In addition, although the laws they enforce do not have breach notice obligations, both the FCC and the SEC have indicated their interest in becoming more involved in cybersecurity and related enforcement measures. As a result, where companies may have had to answer to only one, if any, federal regulator in the past, they may now face more than one inquiry with any future breaches.

GLBA AND FCRA

The GLBA and FCRA are two of the major rules that govern the safeguarding of consumer information by financial services entities. The GLBA requires financial institutions to keep private and appropriately safeguard the nonpublic personal information of their customers.[21] The FCRA governs the actions of entities that either furnish or use consumer reports, and comes into play in the data breach context because it requires consumer reporting agencies to have in place reasonable procedures—i.e., safeguards—to ensure that they only furnish consumer reports as permitted by the law.[22] Depending on an entity's activities in the financial space, different federal or state agencies enforce their compliance with these laws. The GLBA's requirement obliges regulatory agencies to create appropriate safeguards standards for the financial services institutions under their purview.[23] As such, the specific requirements vary, and so do the enforcing agencies. For example, the Board of the National Credit Union Administration has enforcement authority over federally insured credit unions and their subsidiaries.[24] The SEC, as explained in more detail below, can enforce its safeguards provisions against brokers, dealers, investment companies, and investment advisers.[25] The FTC's authority under the GLBA covers financial institutions not otherwise subject to the authority of another agency,[26] including loan brokers, some investment advisers and financial advisers, mortgage lenders not affiliated with banks, debt collectors, tax preparers, and those who provide real estate settlement services.[27]

In addition to complying with the GLBA-mandated rule requiring safeguards, some financial services entities are also required to provide notice to the agencies that regulate them in the event of a breach. This notification requirement applies to those that are governed by the Interagency Guidelines Establishing Information Security Standards (Security Standards).[28] The Security Standards were created by the Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision.[29] The Security Standards—and the notification obligations thereunder—thus apply to the financial services entities governed by those agencies as follows:

- The Comptroller of the Currency regulates national banking associations, any federal branch or agency of a foreign bank, and federal savings associations.[30]
- The FDIC oversees state nonmember insured banks, foreign banks with insured branches, and savings associations.[31]
- The Federal Reserve has purview over state member banks; some foreign banks, including those without insured branches; nonfederal agencies and commercial lending companies; bank holding companies and nondepository subsidiaries; and savings and loan holding companies and nondepository subsidiaries.[32]

Agencies that enforce the GLBA have not been particularly active in pursuing companies for failure to protect information. Ironically, the one exception is the FTC (described in more detail below), even though its GLBA regulations do not include an obligation to notify the agency in the event of a breach.

“Agencies that enforce the GLBA have not been particularly active in pursuing companies for failure to protect information. Ironically, the one exception is the FTC ... even though its GLBA regulations do not include an obligation to notify the agency in the event of a breach”

THE CONSUMER FINANCIAL PROTECTION BUREAU

While the enforcement of the GLBA's safeguard requirement is spread among several different agencies, the Consumer Financial Protection Bureau (CFPB) oversees the compliance by regulated entities with the GLBA's privacy provision.[33] This section of the law prohibits the sharing of nonpublic personal information with nonaffiliated entities, unless the entity has provided the consumer with appropriate disclosures and, in some cases, the ability to opt out.[34] In the past, the Federal Reserve, the Commodity Futures Trading Commission, the Department of Treasury, the FDIC, and the National Credit Union Administration shared enforcement authority for those entities under their jurisdiction.[35] The CFPB was created in 2011 in part to consolidate this jurisdiction under one federal agency.[36] While it has yet to settle any formal privacy enforcement actions, the CFPB now has the authority to enforce the GLBA's privacy provision over a wide variety of financial services entities, including banks, credit unions, mortgage brokers, and brokerage services.[37]

THE OFFICE FOR CIVIL RIGHTS

The Office for Civil Rights (OCR), a small agency under the umbrella of HHS, has enforcement authority over HIPAA on behalf of HHS.[38] HIPAA is divided into three sections—the Privacy Rule,[39] the Security Rule,[40] and the Breach Notification Rule.[41] The Privacy Rule outlines federal requirements related to how covered entities such as hospitals, health plans, and doctor's offices can use and disclose patient health information.[42] The Security Rule contains the minimum security standards that covered entities should employ to protect the health information they store, transmit, and maintain.[43] These are not specific technical standards, but rather types of safeguards that covered entities are required to implement or consider implementing in their data security infrastructure.[44] Finally, the Breach Notification Rule addresses when a covered entity must notify OCR, affected individuals, and the media regarding breaches of unsecured health information.[45] OCR uses its authority under HIPAA to both investigate and bring formal settlement actions against covered entities that violate the rules.

THE FCC

The FCC, best known for its regulation of the television, radio, and telephone industries, is gaining traction in privacy enforcement. The FCC derives its breach enforcement authority from Sections 222 and 201(b) of the Communications Act. These two sections work in tandem to require telecommunications carriers to take "just and reasonable"[46] measures to protect customers' private information.[47] The FCC used this statutory power recently to investigate and punish an entity that had suffered a data breach.[48] The FCC has also promulgated regulations to require telecommunications carriers to report breaches of customer information to the customer and law enforcement, including the United States Secret Service and the Federal Bureau of Investigation.[49]

THE SEC

The SEC has also begun venturing into data breach enforcement. The SEC enforces Rule 30 of Regulation S-P—referred to as the Safeguard Rule—which requires entities under its purview to create written procedures to safeguard the customer records and information they hold, to protect against any anticipated threats or attacks to the security of that information, and to protect against unauthorized use or disclosure of information that could result in substantial harm or an inconvenience to the customer.[50]

The SEC hosted a Cybersecurity Roundtable in March 2014, during which its Commissioners, its staff, and industry stakeholders discussed the importance of protecting consumer data from cyberthreats in order to keep the market secure.[51] The following month, the agency announced that its Office of Compliance Inspections and Examinations (OCIE) was going to proactively audit some of the broker-dealers and investment advisers under its purview to examine their cybersecurity protections.[52] OCIE reconfirmed its intention to focus on cybersecurity when it included cybersecurity compliance in its list of Examination Priorities for 2015.[53] In February 2015, OCIE released its summary of its examinations thus far

> *In February 2015, OCIE released its summary of its examinations thus far and noted, among other items, that 88% of the 57 broker-dealers and 74% of the 49 investment advisers involved in the audits had been targeted by cyberattacks, either directly or through one of their vendors.*

and noted, among other items, that 88% of the 57 broker-dealers and 74% of the 49 investment advisers involved in the audits had been targeted by cyberattacks, either directly or through one of their vendors.[54] Following this, in April 2015, the agency released cybersecurity guidance through its Investment Management Division, emphasizing the need for investment companies and advisers to evaluate where sensitive information is held within an entity, how it is protected, and what risks are associated with it.[55] The SEC also outlined the importance of considering how effective the current security measures are and determining whether they need to be enhanced.[56] In addition, the SEC noted the need for a security incident response plan and security-related policies, procedures, and training for staff in order to round out an effective cybersecurity program.[57] OCIE released additional guidance in September 2015, stating that its forthcoming cybersecurity examinations will focus on the areas of governance, risk assessment, access rights and controls, data loss prevention, vendor management, staff training, and incident response.[58] The SEC's guidance documents and publicly proclaimed focus on cybersecurity are a strong indication that it intends to become another major data breach enforcement agency.

Everyone Else

There is often a misperception that if an entity is not in a regulated industry, it has no regulators that will be looking closely at its activities. This is untrue. At a federal level, the FTC has been quite active in the breach space, as have individual state AGs.

THE FTC

While the FTC is the federal leader in bringing data security enforcement actions, it is interesting to note that there is only one law—the Health Breach Notification Rule—that requires certain companies to directly notify the FTC of a data breach.[59] The rule requires vendors of personal health records, personal health record-related entities not covered by HIPAA's breach rule, and third-party service providers (those offering services to vendors of personal health records in certain specific circumstances) to report breaches to the FTC.[60] This rule applies to a relatively small subset of companies. How, then, does the FTC get involved in so many breach cases? While the FTC may not be the recipient of many breach notifications directly from companies, it can pursue a case based on almost anything, from consumer complaints to news reports. The FTC enjoys broad authority under Section 5 of the FTC Act

to pursue breached companies on the theory that a company's failure to protect consumer information constituted either "unfair or deceptive acts or practices in or affecting commerce."[61]

The law describes unfair acts as those that cause or are likely to cause substantial injury to consumers, are not reasonably avoidable by consumers, and are not outweighed by countervailing benefits to consumers.[62] For the FTC, this includes situations where a company fails to adequately protect information. While "deceptive acts or practices" are not specifically defined within the statute, the FTC has elaborated on their meaning in guidance documents and in the many privacy cases it has brought. Specifically, the FTC has stated that deception is a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[63] In the privacy realm, this could be promising to protect personal information and then failing to do so. While the FTC does not have jurisdiction over certain entities, such as common carriers[64] and financial services entities regulated by other federal agencies, it still has the ability to cast an incredibly wide net in its enforcement activities.

STATE AGS

Following in the footsteps of the FTC are state AGs, who have been quick to file lawsuits against companies that suffer data breaches. It is rather easy for the AGs to find potential cases, given the plethora of state law requirements that impacted organizations notify the state. And even if the appropriate agency isn't notified, state AGs' constituents (impacted individuals residing in their states) may have been notified, as 47 states also have data breach notification laws that require companies to notify consumers if their personal information is breached.[65] State AGs typically have complaint portals on their websites as well, which aid in intelligence gathering regarding data breaches because they allow affected consumers to notify the state government.[66]

> *"While the FTC may not be the recipient of many breach notifications directly from companies, it can pursue a case based on almost anything, from consumer complaints to news reports."*

The legal authority for a state AG to bring a lawsuit following a breach is broad and mirrors the theories used by the FTC. Forty-three states have their own deceptive trade practices statutes that operate like mini-FTC Acts. Like the FTC, state authorities are aggressively investigating data breaches and filing lawsuits against companies for the lax or lack of security practices that led to the breach. State AGs also have authority to bring actions under state laws that require the protection of personal data, such as California's Online Privacy Protection Act[67] and Illinois's Personal Information Protection Act.

Enforcement Actions Brought by Government Agencies

With no shortage of enforcement authority, federal and state regulators have been very active over the past few years. In fact, over the past 13 years, the FTC has used its authority under Section 5 to bring over 50 enforcement cases against companies for their data security practices.[69]

The FCC, HHS, SEC, and state AGs have also ramped up their enforcement efforts in recent years. These cases not only drag companies into the national spotlight, but generally end with lofty compliance plans that require companies to implement the measures the regulator feels are appropriate in order to address the perceived security failures. These settlements can also include a monitoring element, where the company periodically has to send detailed reports to the agency for a certain number of years as specified by the regulator. The following cases include some of the most notable enforcement actions from the past few years, and illustrate not only the interest that agencies have in investigating data breach cases, but also the significant penalties and corrective actions they require in their settlement agreements.

Federal Regulatory Enforcement Actions

FTC PURSUES SNAPCHAT

The FTC's reputation as the leader in federal enforcement precedes it for good reason. For example, in December 2014, the FTC settled with Snapchat after it had accused the company of deceiving users into believing that the messages sent through the company's platform would disappear. The FTC further alleged that Snapchat had failed to secure one of its features, called "Find Friends,"[70] a feature that allowed users to find their friends on Snapchat. Not only, the FTC alleged, was the feature's functionality deceptive, it was not designed securely. Users were prompted to enter the phone numbers to find friends, implying that this was the only information Snapchat needed to find them. In fact, Snapchat then collected information directly from the users' contact lists on their phones.[71] In addition, the FTC contended, because

Snapchat failed to verify that the user was entering the phone number associated with his or her device, a user could create an account associated with someone else's phone number, and could send and receive someone else's messages.[72] In fact, the FTC stated in its complaint that people had done just this: consumers thought they were communicating with their own friends, when in fact they were sending snaps and photos to a stranger. Others complained that their numbers were used to send inappropriate content. The FTC argued that the failure to secure information was a deceptive practice, made in violation of the company's representations in the privacy policy.[73]

Snapchat settled with the FTC, and while no civil penalty was assessed, the company did submit to a lengthy and detailed corrective action plan. Under the agreement, the FTC will monitor Snapchat's compliance with the plan for 20 years. In addition to promising not to misrepresent its data privacy and security measures, Snapchat also agreed to maintain a "comprehensive security program"[74] that would be designed to manage privacy risks in the development of new programs and products and to protect the privacy and confidentiality of the information held by Snapchat.[75] The FTC included a lengthy set of requirements for this program, such as: designating employees to run the program; identifying risks that could result in the company's unauthorized collection, use, or disclosure of user information; implementing employee training; designing and implementing privacy controls; developing security standards for service providers; and evaluating and adjusting the privacy program to stay current with the company's practices.[76]

"Given the costly and long-term requirements of an FTC settlement agreement, and the broad authority granted to the FTC under Section 5, it is not surprising that one company challenged the FTC's ability to take action in this area."

In addition, Snapchat agreed to have a third party conduct biennial security assessments and send a corresponding report to the FTC. The assessments must analyze the privacy controls that Snapchat has implemented, explain why these controls and any related safeguards are appropriate for the company, and certify that the company was adequately protecting user information.[77]

The burdensome nature of the FTC's settlement with Snapchat was in line with many of its other data security settlements, such as its agreements with GMR Transcription Services[78] and Fandango.[79] Given the costly and long-term requirements of an FTC settlement agreement, and the broad authority granted to the FTC under Section 5, it is not surprising that one company challenged the FTC's ability to take action in this area.

WYNDHAM WORLDWIDE CORPORATION CHALLENGES THE FTC

Between 2008 and 2009, Wyndham Worldwide Corporation—the holding company for such brands as Wyndham Hotels and Resorts, Ramada Worldwide, Howard Johnson, Days Inn, and Knights Inn, among others[80]—suffered three data breach incidents.[81] Wyndham had granted brand licenses to approximately 90 independently run hotels.[82] Each hotel had a property management system that processed and stored customer information including names; home and email addresses; telephone numbers; and credit card account numbers, expiration dates, and security codes.[83] The FTC alleged that Wyndham had engaged in unfair practices under Section 5 related to its data security measures. In particular, the FTC contended that Wyndham allowed these hotels to store credit card information in a readable format and that it failed to implement common measures—such as using firewalls, changing default passwords, and updating security software—to protect data, which led to the three data breaches.[84] The FTC further alleged that Wyndham did not have the appropriate procedures in place to detect intrusions to its system, and, beyond that, it did not have proper incident response procedures in place to address the intrusions once they were detected.[85] The FTC pointed out that all three of the incidents were similar, and Wyndham failed to monitor its system for similar intrusions after the first was detected.[86]

Wyndham resisted the FTC's enforcement efforts, and instead claimed that the FTC had exceeded its authority by using the unfairness prong to bring a data security action and that it had failed to give appropriate notice to Wyndham of its expectations related to data security practices.[87] In August 2015, the U.S. Court of Appeals for the Third Circuit reaffirmed the finding of the district court, and held that the FTC does, in fact, have the authority to bring data security suits under the unfairness prong. In part, Wyndham had claimed that its data security practices were not "unfair," under the FTC Act.[88] Wyndham noted that the dictionary meaning of "unfair" was "not equitable" or "marked by injustice, partiality, or deception,"[89] and that it did not intend to deceive or cause injury to its customers. The court found that this argument fell flat and stated that Wyndham did not act equitably with regard to the data breaches because, while the company had a privacy policy in place that promised to secure customer data, it failed to invest the appropriate resources for cybersecurity.[90] This failure exposed its customers, who thought that they were doing business with a company that had suitable data security practices, to financial injury because the information was easily accessible to hackers.[91] All the while, Wyndham was collecting money from these customers.[92]

The court further noted that Wyndham was not "entitled to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices are required by § 45(a)."[93] Instead, the court found that Wyndham was only entitled to have fair notice about the meaning of the statute.[94] The court continued that Wyndham did receive fair notice in this case, because

it could "reasonably foresee that a court could construe its conduct as falling within the meaning of the statute."[95] In coming to this conclusion, the court noted that the FTC's complaint did not allege that the data security measures Wyndham had in place prior to the breach were insufficient, but rather that several security measures were simply missing. In particular, the failure to encrypt consumer information, implement firewalls, or require the change of default passwords.[96] The court also pointed out that Wyndham had suffered not one, but three data breaches in relatively rapid succession.[97] According to the court, after the second data breach, Wyndham at least should have expected that a court would take issue with its data security practices.[98] The FTC's previous data security settlements with other entities, which are published and available to the public, also provided notice to Wyndham of the agency's expectations, the court held.[99]

"In April 2015, the FCC made a splash on the federal regulatory scene when it used its authority under the Communications Act to punish AT&T following three breaches that affected the information of 280,000 customers."

OTHER AGENCY ACTIVITY

In April 2015, the FCC made a splash on the federal regulatory scene when it used its authority under the Communications Act to punish AT&T following three breaches that affected the information of 280,000 customers.[100] The FCC required a $25 million dollar settlement and a corresponding corrective action plan, alleging that AT&T failed to take "every reasonable precaution" to secure customer data, constituting a violation of the act.[101] The FCC also found that this failure constituted an unjust and unreasonable practice under the act.[102]

The FCC also recently expanded its privacy enforcement authority with its Open Internet rules.[103] The Open Internet rules reclassify fixed and mobile broadband Internet services as "common carriers,"[104] so that they are now under the purview of the FCC, and subject to the FCC's privacy requirements[105] and prohibition against unjust and unreasonable practices.[106] Interestingly enough, this move may effectively gut the FTC's authority to bring privacy enforcement actions against Internet services—such as Google for example—because there is a provision in the FTC Act that exempts common carriers from the FTC's jurisdiction.[107] While this exception previously delineated the regulatory authority of the two agencies, it will be interesting to see where the FCC goes with this new authority, and whether it has the effect of curtailing the FTC's enforcement measures. The move has been controversial, as the FCC has faced litigation from Internet services providers that are reticent to submit to the more stringent FCC rules.[108]

In recent years, OCR has increased its enforcement efforts, punishing entities that suffer data breaches and other privacy-related disclosures with fines that can run into the millions of dollars and detailed corrective action plans that subject entities to OCR's monitoring for up to three years. Of note was OCR's May 2014 settlement with Columbia University and New York Presbyterian Hospital, which resulted in a $4.8 million dollar settlement, in addition to monitoring and HHS input on the entities' privacy policies and risk management processes.[109]

The SEC is also ramping up its breach enforcement actions. On September 22, 2015, the SEC announced a $75,000 settlement with R.T. Jones Capital Equities Management following a breach that affected 100,000 individuals.[110] The SEC found that R.T. Jones failed to comply with the Safeguards Rule, as it did not have in place prior to the breach written policies and procedures related to the safeguarding of the customer information it held, and it had additionally failed to conduct risk assessments as appropriate, utilize safeguards such as firewalls or encryption to protect its data, and implement a cybersecurity incident response plan.[111] In addition to the monetary settlement, the company was censured and agreed to refrain from violating the Safeguards Rule again in the future.[112]

"The ability of state AGs to file lawsuits for data breaches adds yet another layer of potential liability for breached companies."

State Regulatory Enforcement Actions

The ability of state AGs to file lawsuits for data breaches adds yet another layer of potential liability for breached companies. An AG action is separate from any FTC or other federal inquiry and from private class action lawsuits. For example, Advocate Health, which suffered a breach in 2013 and is discussed in more detail below, faced not only an investigation spearheaded by the Illinois Attorney General, but a federal inquiry from HHS-OCR[113] and several class action lawsuits.[114]

State regulatory actions can be quite costly. For example, in May 2012, the Massachusetts Attorney General settled with South Shore Hospital for $750,000 following a breach involving 473 unencrypted computer backup tapes that contained the personal information of over 800,000 patients. The hospital had contracted with a vendor to erase the backup tapes and resell them, but it had neither notified the vendor that the tapes contained personal and health information, nor taken efforts to determine whether the vendor had sufficient safeguards

to appropriately protect the information while it is was in the vendor's control. In addition, only one of the 43 boxes arrived at the vendor's office. The rest of the boxes were lost and were not recovered. South Shore Hospital also agreed to monitoring by the AG's office and to take steps to come into compliance with state and federal data security rules, which included putting a data security requirement in its contracts with information disposal vendors.[115]

State AGs may also investigate and address data breaches that affect residents of several states. For example, in September 2014 the Illinois Attorney General announced that she was leading an investigation into a potential data breach involving Jimmy John's restaurants that potentially impacted 216 restaurants in 37 states.[116]

State AGs are protective of preserving their authority to investigate data breaches that affect residents of their respective states. On July 7, 2015, 47 AGs together sent a letter to Congress to provide their perspective on a potential federal data breach notification law.[117] The letter focused on the notion that any federal data breach law should not preempt state law, and emphasized the role that state AGs play in protecting consumer rights. According to the state AGs, their ability to conduct investigations and bring enforcement actions against companies that have suffered data breaches is paramount to ensuring the adequate protection of consumer information within their states.[118]

The letter provides valuable insight into the potential tensions that could come into play between the states and the federal government if there were a federal data breach notification and security law. The state AGs noted that any federal law should defer to the existing state laws, as there are different concerns in each state and an overarching law would not capture the appropriate nuances. In other words, state AGs want the states to be able to amend their own data breach laws to reflect the technological and business concerns in their respective states. Further, there is the concern that there are too many data breaches for any one federal agency to handle. The state AGs are also worried that smaller breaches could be overlooked by a federal agency because they are not national in scope. AGs have pointed out, however, that these small breaches could have a major impact on the residents of a certain state, but there would be no one to investigate them or help provide redress to affected consumers.[119]

"State AGs are protective of preserving their authority to investigate data breaches that affect residents of their respective states."

Lawsuits Filed by Private Individuals: The Class Action Cases

Despite the increase in or prevalence of regulatory enforcement cases, consumer class actions and other attempts to seek redress for perceived privacy-related harms have seemingly proliferated in the past decade.

There is no clear explanation for this trend. In part, it appears that plaintiffs are unsatisfied with regulatory redress and desire personal recourse against the companies that unwillingly disclose their personal information. That stated, to date, many of these actions have failed to bear fruit for the plaintiffs, despite the creative legal arguments that the class action bar has used in arguing these cases. This likely owes—at least in part—to the fact that many of the laws that plaintiffs' attorneys have sought to invoke were not initially drafted to address the type of perceived wrong that plaintiffs allege after a data breach.

The Harm Hurdle

Perhaps the most critical issue in examining civil liability is determining who has the legal right to sue a company subsequent to a data breach or other perceived data privacy violation. Potential plaintiffs need to establish standing to sue in order to maintain a cause of action. This means that a plaintiff must "prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision."[120] In other words, a plaintiff in a data breach case needs to show three things:

- The plaintiff suffered some sort of harm that can be measured or quantified.
- The harm can be connected to the specific data breach at issue.
- The lawsuit will be able to redress the plaintiff for the harm suffered.

Each of these points comes with its own set of challenges, but the first—establishing a concrete injury—has proved particularly difficult for data breach plaintiffs. Often, when these class actions are filed, the individuals affected by the breach cannot point to something definitive to show the court that they have suffered harm. These cases are unique because, while it is usually certain that a breach has led to

the access or acquisition of the plaintiffs' information, there is generally no proof—at least at the time that the suit is filed—that this has caused any damage, injury, or harm. Sometimes, plaintiffs are able to demonstrate that their information has been used to open fraudulent credit card accounts or their payment card numbers have been used by unauthorized third parties to make purchases. Beyond that, most plaintiffs have very little to show in terms of the fallout from the data breach, besides the idea that one day, maybe, they will suffer some sort of harm because their information was misappropriated or stolen.

FUTURE HARM

Currently, the single biggest hurdle in a plaintiff's path to establishing standing is the *Clapper v. Amnesty International* case, a 2013 Supreme Court decision holding, in relevant part, that an allegation of future harm will only constitute standing if the harm is "certainly impending" or there is a "substantial risk" that the harm will occur.[121] While the *Clapper* case does not arise as a result of a data breach, it has had important implications on whether or not breach plaintiffs can establish standing to sue. *Clapper* analyzed the ability of a group of people—including "attorneys and human rights, labor, legal, and media organizations"—to satisfy the standing requirements in order to challenge the constitutionality of the Foreign Intelligence Surveillance Act of 2008.[122] The law at issue authorized government officials to put suspected foreign agents under surveillance without first having to demonstrate probable cause.[123]

The plaintiffs argued that they had standing to challenge the law because there was an "objectively reasonable likelihood"[124] that their communications would be collected because their jobs regularly required them to converse with people who might be subject to surveillance under the law.[125] In plain terms, the people who were challenging the law had not yet been affected by it (i.e., they were not under surveillance), but they argued that they had the right to challenge the law because there was a chance that, in the future, they would be targeted under it. The challengers also noted that they had suffered an injury because they had to take costly measures to protect themselves from suffering this future harm.[126]

> *"Currently, the single biggest hurdle in a plaintiff's path to establishing standing is the* Clapper v. Amnesty International *case ... holding ... that an allegation of future harm will only constitute standing if the harm is 'certainly impending' or there is a 'substantial risk' that the harm will occur."*

The court disagreed.[127] In rejecting that argument, the court made two points that have proved key in data breach litigation cases: (1) the claim of future injury is not enough to fulfill the standing requirement that threatened injury be "certainly impending;"[128] and (2) standing cannot be manufactured by making expenditures to prevent harm that is not presently occurring.[129]

These points are significant because they effectively eliminate two of the only things that data breach plaintiffs can demonstrate as harm: (1) their increased future risk of identity theft; and (2) the costs associated with proactively preventing identity theft (canceling credit cards, obtaining credit monitoring services, etc.). While *Clapper* is a relatively recent case, it echoed—at the Supreme Court level—the district and appellate court cases that have previously found the increased risk of future harm[130] and expenditures related to mitigating future harm to be insufficient to support standing.[131]

OTHER WAYS TO ESTABLISH HARM

Data breach plaintiffs have also used a variety of other concepts in an attempt to establish harm, including loss of privacy,[132] loss of value of information,[133] and benefit of the bargain.[134] These theories have all generally been unsuccessful. Plaintiffs have also attempted to use unreimbursed losses to establish injury, but this often relates to credit card changes that are later reimbursed or forgiven by banks, and, therefore, courts have found that this is not an actual injury.[135]

However, in July 2015, the Seventh Circuit reversed the dismissal of a lawsuit brought against Neiman Marcus, finding that the risk of harm to the 350,000 people whose credit card numbers were exposed following a data breach was enough to suffice for standing purposes.[136] The court held that the plaintiffs "should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing," and, citing *Clapper*, stated that this was a case where there was an "objectively reasonable likelihood" that the plaintiffs would suffer an injury. [137]

> *"[T]he court made two points that have proved key in data breach litigation cases: (1) the claim of future injury is not enough to fulfill the standing requirement that threatened injury be 'certainly impending;' and (2) standing cannot be manufactured by making expenditures to prevent harm that is not presently occurring."*

> *"The court held that the plaintiffs 'should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing,' and, citing* Clapper, *stated that this was a case where there was an 'objectively reasonable likelihood' that the plaintiffs would suffer an injury."*

The case stems from a breach that occurred from July through October 2013, during which time a malware intrusion allowed an unauthorized third party access to customer credit card numbers.[138] The court noted that 9,200 cards had already been used to make fraudulent charges.[139] The court further stated that making the plaintiffs wait until the "threatened harm" materialized in order to grant standing created a separate causation problem.[140] The court found that, "the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach."[141]

The Seventh Circuit generally distinguished data breach cases from the circumstances examined in *Clapper*.[142] According to the court, whereas *Clapper* involved the speculative risk that government agencies were spying on the plaintiffs, in data breach cases, the only reason a hacker would have attacked the retailer's system was to engage in fraud.[143]

The court also provided plaintiffs with a victory on the causation front, as it rejected Neiman Marcus's argument that the plaintiffs could not prove that this particular breach led to fraudulent credit transactions because there were several other major data breaches that occurred in the same time period.[144] The court stated that, to survive a motion to dismiss, the plaintiffs are required only to show that this particular breach *might* have caused them injury.[145] Neiman Marcus also claimed that the plaintiffs' claims were moot because they were reimbursed by their credit card companies for the fraudulent activities.[146] The court rejected this argument, and stated that the practice of reimbursing fraudulent charges "defeats neither injury-in-fact nor redressability."[147] The court noted that this was a business practice that varied among credit and debit card companies, and that there were some instances when a consumer would not be reimbursed for the full amount of the fraudulent charge.[148] Therefore, according to the court, a favorable court judgment could help redress the outstanding injury.[149] Neiman Marcus asked the Seventh Circuit to reconsider its decision in a Petition for Rehearing En Banc, but the court officially refused to do so on September 17, 2015. The case is now back in the hands of the United States District Court for the Northern District of Illinois, Eastern Division, where it could potentially change the landscape for data breach plaintiffs.

In the same vein, another case could soon impact the ability of data breach plaintiffs to bring class actions. *Robins v. Spokeo, Inc.*, is scheduled to be argued in front of the Supreme Court on November 2, 2015. The question before the Court will be whether Congress can confer standing to a plaintiff simply by authorizing a private right of action based on the violation of a federal law.[150] In other words, the Court will determine whether a violation of a federal right constitutes a concrete injury.[151]

Robins is a class action case against Spokeo, a company that aggregates on its website data including contact information, age, marital status, economic and wealth levels, and occupation.[152] The plaintiff sued Spokeo, claiming that the information the website had gathered about him was false, and that this was a willful violation of the FCRA.[153] Spokeo moved to dismiss the case, stating that the plaintiff had not suffered an injury, and therefore did not have standing to sue.[154] The Ninth Circuit found that Robins did satisfy the requirements for standing: namely, that the violation of his statutory rights constitutes an injury, that Spokeo caused the injury by allegedly violating the FCRA, and that the FCRA's monetary damages provision allows the court to redress the injury.[155] The Supreme Court, then, has the opportunity to determine whether the mere violation of a federal law that allows for a private right of action will suffice for standing.

> *"Plaintiffs have gone through the book of common law in their attempts to find legal relief after a breach that affects their information."*

Specific Causes of Action Examined

Unfortunately for plaintiffs, many of the issues that affect their ability to establish standing also create difficulties in successfully maintaining a cause of action. Plaintiffs have gone through the book of common law in their attempts to find legal relief after a breach that affects their information. In addition, plaintiffs have used laws such as state unfair and deceptive trade practice statutes and the FCRA to pursue their claims. For the most part, these efforts have been creative, but largely unsuccessful.

UNFAIR AND DECEPTIVE TRADE PRACTICES

Most states have mini-FTC Act laws that focus on consumer protection and prohibit unfair trade practices, and most afford a private of right action, paving the way for data breach plaintiffs to pursue cases. Several states have adopted their own version of the Uniform Deceptive Trade Practices Act to account for the fact that these lawsuits may affect the residents of more than one state.[156] In practical terms, when states have the same deceptive trade practices act in place, it is easier for the class to proceed with the lawsuit because

they all have to plead the same components of the law. Of course, state AGs are also able to bring lawsuits under these statutes, potentially doubling the liability for companies on the state level.

However, while breach plaintiffs are granted a right of action under these state statutes, they still face significant challenges in adequately pleading their cause of action. Recently, a Pennsylvania court declined to approve class certification[157] for a case filed under the Pennsylvania Unfair Trade Practices and Consumer Protection Law (UTPCPL).[158] The case was brought against Keystone Mercy Health Plan and AmeriHealth Mercy Health Plan after their employees lost a flash drive containing the health information of over 283,000 individuals.[159] The lost health information in this case included the Social Security numbers of seven individuals, the partial Social Security numbers of 801 individuals, and various types of data—including member identification numbers, clinical health screening information, names, and addresses—for the rest of the affected individuals.[160] However, the lead plaintiff, who filed suit on behalf of his minor daughter and others similarly situated,[161] suffered only the loss of his daughter's member identification number and health screening information.[162]

In denying the class certification, the court found, in part, that the plaintiff could not show that the class satisfied the "commonality" requirement.[163] While the plaintiff claimed that commonality was satisfied because everyone in the class shared an equal increased risk of identity theft because all of their information was on the same flash drive, the court disagreed.[164] The court noted that, in its opinion, the lost information pertaining to the plaintiff's daughter could not be linked back to her, given that it was a member identification number and not her name.[165] Therefore, per the court, she was not at the same increased risk of identity theft as everyone else whose information was on the flash drive because their information could have included Social Security numbers, which would clearly identify them.[166] The court also rejected the plaintiff's argument under the UTPCPL.[167] The plaintiff attempted to bring the case under the statute's provision that prohibited engaging in "any other fraudulent or deceptive conduct which creates a likelihood of confusion or of

"[W]hen states have the same deceptive trade practices act in place, it is easier for the class to proceed with the lawsuit because they all have to plead the same components of the law. Of course, state AGs are also able to bring lawsuits under these statutes, potentially doubling the liability for companies on the state level."

> *"The cause of action for intentional misrepresentation differs only in that the plaintiff must show that the defendant acted with the intent to make the plaintiff believe that the misrepresentation was true."*

misunderstanding."[168] The court held that the plaintiff could not move forward with this claim because he could not establish that he relied on any promises made by the defendant concerning the protection of health information.[169]

NEGLIGENCE

In bringing negligence cases related to data breaches, plaintiffs must assert that the defendant had a duty to exercise reasonable care to protect personal information, and this duty was breached when the defendant failed to establish safeguards or provide timely notice of the breach. To succeed on a negligence claim, plaintiffs must show the following:

- The defendant owed the plaintiff a legal duty.
- The defendant breached the duty.
- The plaintiff suffered injuries.
- The defendant's breach was the legal or proximate cause of the plaintiff's injuries.[170]

Similarly, some plaintiffs attempt to use negligent or intentional misrepresentation as a cause of action in data breach cases. Here, plaintiffs must show that the defendant represented that it would take reasonable measures to safeguard their information, generally through representations made in a privacy policy. To sustain this cause of action, plaintiffs must demonstrate the following:

- The defendant made a misrepresentation.
- The defendant had no reason to believe the misrepresentation was true.
- The defendant acted with the intent to induce the plaintiff to rely on the misrepresentation.
- The plaintiff justifiably relied on the misrepresentation.
- The plaintiff suffered damages as a result.[171]

The cause of action for intentional misrepresentation differs only in that the plaintiff must show that the defendant acted with the intent to make the plaintiff believe that the misrepresentation was true.[172] In all of these cases, plaintiffs run into the same issues as discussed above in establishing standing. Namely, plaintiffs must establish that they suffered an injury and that they have tangible and redressable damages. For negligence actions, plaintiffs must also demonstrate that breached companies owed them a duty of care, which gets complicated in cases where the breached

entity is not a company that has a direct relationship with the consumer whose information was subject to the breach, but instead is a third party that offers services for the company.

A recent case highlights the difficulties that data breach plaintiffs may have in sustaining negligence-based causes of actions. *Lovell v. P.F. Chang's China Bistro, LLC*, was decided in March 2015, and the court found that the plaintiff failed to establish that he had suffered an injury due to the restaurant chain's data breach.[173] The plaintiff claimed that he suffered an injury from overpaying for the food (as he would not have done so if he had known of the company's lax security practices); from the resulting actions he had to take to protect himself from cybercriminals, including replacing credit cards; and from the possible stalking and harassment that he could be subjected to by the cybercriminals.[174] The court rejected the plaintiff's claims about the overpayment for the food because he did not clarify how the company's negligence lowered the value of the food he consumed.[175] The court further found that, much like in other data breach cases, the plaintiff did not articulate how the risk of future harm, or the actions he proactively took to prevent future harm, constituted an injury.[176] The court was similarly dismissive of the plaintiff's allegations related to P.F. Chang's negligent misrepresentations.[177] The plaintiff argued that the company's data security practices were below standard, but he did not offer any evidence to support this.[178] As such, the court found that the mere happening of a data breach was not enough to support that the company negligently misrepresented its practices to the plaintiff.[179]

BREACH OF CONTRACT

In many data breach class action cases, negligence claims are coupled with breach of contract claims. The plaintiff must show that that there was some sort of binding agreement between the parties prior to the breach, and that the company broke that agreement when the data breach occurred. Again, the failure of this cause of action often occurs when the plaintiff must demonstrate that the breach caused damages. To support this cause of action, a plaintiff must demonstrate the following:

- A binding contract existed between the plaintiff and defendant.
- The plaintiff satisfied its obligations under the contract.
- The defendant failed to satisfy its obligations under the contract.
- The plaintiff suffered damages because of the breach.[180]

The plaintiff in the *Lovell* case asserted a variation of the breach of contract claim, in that he alleged that there was a breach of an *implied* contract that was violated when P.F. Chang's suffered a data breach. This differs slightly from the traditional claim in that the plaintiff is asserting, in lieu of a binding contract in writing or in words,

> *"In many data breach class action cases, negligence claims are coupled with breach of contract claims."*

that the actions of the two parties gave rise to a contract.[181] In *Lovell*, the plaintiff contended that when he used his credit card to purchase his meal at P.F. Chang's, the restaurant impliedly promised to protect his credit card information.[182] The restaurant successfully rebutted this argument by stating that if there were an implied contract between the two parties, it was limited to the payment for and delivery of food.[183] The court agreed, holding that the plaintiff tendered his credit card because he chose to use that form of payment to satisfy the debt he owed to the restaurant for the food.[184] This, therefore, did not give rise to an enforceable contractual agreement for P.F. Chang's to protect the plaintiff's credit card information.[185]

THE FCRA

The FCRA has also been used as a cause of action in data breach cases. Traditionally, entities that fell under the purview of the FCRA were the big credit reporting agencies—such as Experian, Transunion, and Equifax—that collected large amounts of information in order to evaluate an individual's suitability for credit cards and employment decisions. These days, more and more entities are getting into the information business. The by-products of everyday life—mobile phones, social media, emails, and online shopping—produce huge amounts of data that are very valuable to companies that want to better understand and market to their customers. However, the accumulation and transfer of all of this information could trigger obligations under the FCRA, including, as some classes of plaintiffs have claimed, liability for a data breach.

"These days, more and more entities are getting into the information business ... However, the accumulation and transfer of all of this information could trigger obligations under the FCRA, including, as some classes of plaintiffs have claimed, liability for a data breach."

The FCRA includes a dense set of requirements, and proving liability for a data breach under the law is fairly complex. Plaintiffs must sufficiently plead four key points:

- The breached entity is a consumer reporting agency.
- The breached information was a consumer report.
- The breached entity did not have sufficient procedures in place to make sure that the consumer reports went to the correct third party.
- The breached entity "furnished" the consumer report to an unauthorized third party.

First, plaintiffs must show that the entity that suffered the breach is a consumer reporting agency. The FCRA defines an entity as a consumer reporting agency if, on a nonprofit basis or for monetary fees, it compiles information about consumers for the purpose of furnishing consumer reports

to third parties.[186] Second, plaintiffs must show that the breached data constituted a "consumer report." The FCRA definition for "consumer report" is incredibly broad and includes almost all of the information collected by consumer reporting agencies related to an individual's credit—such as general reputation and personal characteristics—which is used to make decisions about the individual's eligibility for employment, personal credit, and insurance underwriting.[187] This definition generally covers most of the information held by the consumer reporting agency, but there are also several express exclusions, including information that relates only to experiences and transactions between the consumer reporting agency and the individual.[188]

Assuming plaintiffs can clear the first two hurdles, they must prove the last two elements: that the entity failed to establish reasonable procedures to ensure that the consumer reports went to the correct place; and that the entity was, indeed, "furnishing" the report to the unauthorized third party.[189] In general, courts have yet to accept plaintiffs' assertions that a theft constitutes "furnishing" a consumer report for the purposes of a claim under the FCRA.[190]

The Seventh Circuit recently evaluated whether a healthcare system qualified as a consumer reporting agency under the FCRA. The court ultimately rejected the argument presented by a class of data breach plaintiffs who claimed that Advocate Health and Hospitals Corporation had willfully and negligently violated the FCRA provisions that require consumer reporting agencies to maintain reasonable procedures to ensure that consumer reports are disclosed only to individuals who are entitled to see them.[191] The case stems from a July 2013 breach in which four unencrypted desktop computers that contained the protected health information of over 4 million individuals were stolen from one of Advocate's administrative offices.[192]

In affirming the district court's decision to dismiss the FCRA claims, the court found that the plaintiffs failed to satisfactorily plead that Advocate was a consumer reporting agency and that it was distributing consumer reports.[193] The court noted that the plaintiffs sufficiently pled that Advocate compiles information about consumers because it assembles a variety of patient information, including names, addresses, dates of birth, Social Security numbers, and medical treatment information.[194] However, the court determined that the plaintiffs did not demonstrate that Advocate was compensated for the purpose of compiling the patient information and distributing it as a consumer report,[195] or that Advocate did so on a nonprofit basis.[196] Instead, the court distinguished the actions of the healthcare provider, stating that it collects and transmits patient information to insurance companies and government agencies for the purpose of obtaining payment for its providers who have rendered healthcare services.[197]

The court further found that the information compiled by Advocate did not qualify as a consumer report under the FCRA, citing the law's exclusion of reports that solely contain information about a consumer's experience or transaction with the entity. The court followed that the information that Advocate sent to third parties, such as medical diagnoses, was limited to its

experiences with the consumer, so it fell under the exception and was not considered a consumer report.[198] Interestingly enough, while the court could have affirmed the dismissal of the FCRA claims with its brief analysis of whether the information held by Advocate constituted consumer reports, it opted to provide an in-depth discussion of whether Advocate was a consumer reporting agency, based on its general actions as a healthcare provider. The court did note, however, that while it did not find the healthcare provider to be a consumer reporting agency in this instance, there are entities besides traditional credit reporting agencies that could be consumer reporting agencies under the FCRA.[199]

THE ELECTRONIC COMMUNICATION PRIVACY ACT AND THE STORED COMMUNICATION ACT

While the FCRA has been cited in breach class actions with great frequency, there are a few other federal statutes that also get a fair amount of play, such as the Electronic Communication Privacy Act (ECPA) and the Stored Communication Act (SCA). These causes of action have generally been unsuccessful, mostly because the statutes were never meant to provide relief for data breach victims. The ECPA, in part, is meant to prohibit the intentional interception of communications, including telephones and computer transmissions, as well as the disclosure of the intercepted information. The SCA is a subpart of the ECPA that prohibits the unauthorized access of data that is in an electronic form of storage.[200] In the privacy data breach context, these causes of action are seemingly more fitting for the bad actor that caused the breach rather than the company that was the victim of the breach. The courts have generally agreed, and, with SCA claims, have stated that an entity must be in the business of providing electronic communications in order to be under the purview of the act.[201] Therefore, showing that the entity merely sends and receives electronic communications is not enough to support a claim under the SCA.[202]

THE KITCHEN SINK—CONVERSION, UNJUST ENRICHMENT, AND BAILMENT

As noted above, there has been no shortage of creativity in the types of actions brought in the data privacy context. In addition to the theories described above, plaintiffs have looked to other common law causes of action in an attempt to recover for perceived wrongs in the data privacy space. Among these are conversion, unjust enrichment,[203] and bailment.[204] Most of these claims have been dismissed for procedural and jurisdictional deficiencies.

“The court did note, however, that while it did not find the healthcare provider to be a consumer reporting agency in this instance, there are entities besides traditional credit reporting agencies that could be consumer reporting agencies under the FCRA.”

Conclusion

Companies are in a difficult position. Cyberattacks are rapidly becoming more sophisticated and difficult to anticipate and prevent. At the same time, regulatory inquiries and private lawsuits come at companies from all directions, sometimes immediately after news of a breach becomes public. Regulators at the federal and state levels have demonstrated that they are becoming more aggressive about pursuing post-data-breach enforcement actions.

Regulators have easy access to news about breach notifications via the various state and federal reporting requirements, and they use these as an invitation to investigate breached companies. After completing their investigations, regulators derive legal authority from other sources in order to bring enforcement actions against the companies. In addition to the regulators are the individuals affected by these breaches, who have proved themselves eager to have their own day in court and are increasingly unforgiving in bringing class action lawsuits following breaches. For companies that suffer a data breach, it may seem that there is an endless road of inquiries, and it is no small task to navigate through the patchwork of liability that exists at the state and federal levels. However, there are a number of things companies can do to limit the fallout from a data breach.

BE AWARE OF THE RISKS

To the extent possible, the best defense is a good offense. Companies should conduct enterprise-wide risk assessments on a regular basis, and certainly when there are any major changes to the company's operations (e.g., acquiring a new subsidiary or entering a new field). This will assist in identifying any areas of weakness in the company's data security plan, and will help the company prioritize where to funnel its resources to ensure that consumer data stays safe. It is important for companies to follow up with the appropriate mitigation strategies to address the high- and medium-level risks that were uncovered during the assessment.

ENSURE DATA SECURITY PRACTICES ARE UP TO INDUSTRY STANDARD

It is vital that a company's data security practices are on par with what is considered standard for the industry. This way, even if the company falls victim to a data breach—and the chances are high that it will—the company will be able to demonstrate to a regulatory authority or court that it consistently evaluated its standards and placed a high priority on securing consumer data. This may lower or eliminate the company's liability in any post-breach lawsuits.

EXPECT AND PREPARE FOR REGULATORY SCRUTINY OF BREACH INVESTIGATIONS

If a company suffers a data breach, those who conduct the company's internal investigation should keep in mind that a regulator—be it the FTC, a state AG, or another agency with specialized enforcement authority—may want to review the investigation report. The regulators may also scrutinize what actions (if any) the company took to examine the underlying issues that enabled the breach and how the company addressed them to prevent a similar situation from occurring in the future. Thus, companies should work closely with their legal departments and external counsel not only to preserve privilege, but also to ensure that the investigation will withstand the scrutiny of a state or federal regulator.

KEEP TABS ON NEW AND EXISTING REGULATORY CASES AND CLASS ACTION LAWSUITS

Given the relative frequency of data breaches, and the likelihood that class actions and regulatory inquiries will follow, there are new developments in this area of the law on a monthly, and sometimes weekly, basis. Companies should stay informed about the most up-to-date cases, as they can offer clues about why courts and regulators are coming to certain decisions or settlements. With this information, companies may be able to proactively address certain data security issues within their systems, so they can better position themselves if they do fall victim to a data breach.

Endnotes

i This article was written for informational purposes only, and should not be used as a substitute for legal advice, which is based on specific facts. For more information about the information discussed herein, please contact Liisa M. Thomas, the chair of Winston & Strawn LLP's Privacy and Data Security Practice. She can be reached at lmthomas@winston.com.

1 *See* https://www.opm.gov/cybersecurity.

2 *See* https://www.anthemfacts.com/.

3 *See* http://www.premeraupdate.com/.

4 *See* https://www.uclahealth.org/news/ucla-health-victim-of-a-criminal-cyber-attack.

5 *See* http://www.hipaajournal.com/the-age-of-the-healthcare-data-breach-40-of-americans-now-victims-8083.

6 15 U.S.C. § 45(a).

7 *See* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf.

8 *See* SEC, IM Guidance Update, No. 2015-02 (April 2015), *available at* http://www.sec.gov/investment/im-guidance-2015-02.pdf; and OCIE, National Exam Program Risk Alert, [title], Volume IV, Issue 8 (September 15, 2015), *available at* https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

9 *See, e.g.,* Press Release, U.S. Department of Health and Human Services–Office for Civil Rights, Stolen Laptops Lead to Important HIPAA Settlements (April 22, 2014), *available at* http://www.hhs.gov/news/press/2014pres/04/20140422b.html.

10 *See, e.g., In the Matter of Credit Karma, Inc.,* Fed. Trade Comm'n, File No 1323091 (August 13, 2014).

11 *See* Steven Levy, *Grand Theft Identity*, Newsweek (July 3, 2005), *available at* http://www.newsweek.com/grand-theft-identity-121351.

12 For example, the Minnesota Attorney General and the FTC separately investigated Accretive Health's 2011 data breach, and Accretive ultimately entered into settlement agreements with each entity.

13 *See, e.g.,* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

14 *See* http://accretivehealth.com/services.

15 Tony Kennedy and Maura Lerner, *Accretive Is Banned from Minnesota*, Star Tribune (July 21, 2012), *available at* http://www.startribune.com/accretive-banned-from-minnesota-for-at-least-2-years-to-pay-2-5m/164313776/.

16 *Id.*

17 *Id.*

18 *See In the Matter of Accretive Health, Inc.*, Fed. Trade Comm'n, File No. 1223077 (February 5, 2014).

19 *See* https://www.ftc.gov/sites/default/files/documents/closing_letters/fair-debt-collection-practices-act/131231fairdebtclubokletter.pdf.

20 *Id.*

21 *See* 15 U.S.C. § 6801.

22 *See* 15 U.S.C. § 1681(e).

23 15 U.S.C. § 6801(b).

24 15 U.S.C. § 6805(a)(2).

25 *See* 15 U.S.C. §§ 6805(a)(3)-6805(a)(5).

26 *See* 15 U.S.C. § 6805(a)(7).

27 *See* https://www.ftc.gov/tips-advice/business-center/guidance/brief-financial-privacy-requirements-gramm-leach-bliley-act.

28 *See* 12 U.S.C. § 1831P-1.

29 The Office of Thrift Supervision was dissolved in October 2011, and its functions were divided among the FDIC, the Federal Reserve, and the Consumer Financial Protection Bureau.

30 12 U.S.C. § 1803(q)(1).

31 12 U.S.C. § 1803(q)(2).

32 *Id.*

33 *See* 15 U.S.C. § 6802.

34 *Id.*

35 15 U.S.C. §§ 1681(s)-6805.

36 *See* 12 U.S.C. §§ 5514-5517.

37 *Id.*

38 The FTC also has enforcement authority over HIPAA for certain types of companies.

39 *See* 45 C.F.R. § 164(e).

40 *See* 45 C.F.R. § 164(c).

41 *See* 45 C.F.R. § 164(d).

42 *See* 45 C.F.R. §§ 164.500, *et seq.*

43 *See* 45 C.F.R. § 164(c).

44 *Id.*

45 *See* 45 C.F.R. § 164(d).

46 47 U.S.C. § 201(b).

47 *See* 47 U.S.C. § 222.

48 Press Release, Federal Communications Commission, AT&T To Pay $25M To Settle Investigation Into Three Data Breaches (April 8, 2015), *available at* https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches.

49 *See* 47 C.F.R § 64.2011.

50 *See* 17 C.F.R. § 248.30(a).

51 *See* SEC Cybersecurity Roundtable (March 26, 2014), *available at* http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml.

52 *See* OCIE, National Exam Program Risk Alert, OCIE Cybersecurity Initiative, Vol. IV, Issue 2 (April 15, 2014), *available at* https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.

53 *See* Examination Priorities for 2015 (January 13, 2015), *available at* http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2015.pdf.

54 OCIE, National Exam Program Risk Alert, OCIE Cybersecurity Initiative, Vol. IV, Issue 4 (Feb. 3, 2015), at 2-3, *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

55 *See* SEC, IM Guidance Update, No. 2015-02 (April 2015), *available at* http://www.sec.gov/investment/im-guidance-2015-02.pdf.

56 *Id.* at 1-2.

57 *Id.* at 2.

58 OCIE, National Exam Program Risk Alert, Volume IV, Issue 8 (September 15, 2015), at 1-3, *available at* https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

59 *See* 16 C.F.R. § 318.

60 *See* 16 C.F.R. §§ 318.2-318.3.

61 15 U.S.C. § 45(a).

62 15 U.S.C. § 45(n).

63 Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

64 *See* 15 U.S. Code § 45(a)(2).

65 *See, e.g.,* MGL 93(h) § 3.

66 *See, e.g.,* http://illinoisattorneygeneral.gov/consumers/filecomplaint.html.

67 *See* Cal. Bus. & Prof. Code §§ 22575-79 (2004).

68 *See* 815 ILCS 530.

69 *See* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

70 *In the Matter of Snapchat, Inc.*, Fed. Trade Comm'n, File No. 1323078 (May 8, 2014), Complaint at 7.

71 *Id.*

72 *Id.*

73 *Id.* at 8.

74 *In the Matter of Snapchat, Inc.*, Fed. Trade Comm'n, File No. 1323078 (December 23, 2014), Decision and Order at 3.

75 *Id.*

76 *Id.*

77 *Id.* at 4.

78 *In the Matter of GMR Transcription Services, Inc.*, Fed. Trade Comm'n, File No. 1223095 (January 31, 2014).

79 *In the Matter of Fandango, LLC,* Fed. Trade Comm'n, File No 1323089 (August 19, 2014).

80 *See* http://www.wyndhamworldwide.com/category/our-brands.

81 *FTC v. Wyndham Worldwide Corp.*, 3d Cir., No. 14-3514 (August 24, 2015), at 6.

82 *Id.*

83 *Id.*

84 *Id.* at 8-9.

85 *Id.* at 9.

86 *Id.*

87 *Id.* at 7.

88 *Id.* at 16.

89 *Id.* at 17.

90 *Id.*

91 *Id.*

92 *Id.*

93 *Id.* at 38.

94 *Id.*

95 *Id.* at 40.

96 *Id.*

97 *Id.* at 41.

98 *Id.*

99 *Id.* at 42.

100 Press Release, Federal Communications Commission, AT&T to Pay $25M to Settle Investigation into Three Data Breaches (April 8, 2015), *available at* https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches.

101 *See* 47 U.S.C. § 222.

102 *See* 47 U.S.C. § 201(b).

103 *See* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf.

104 *Id.*

105 *See* 47 U.S.C. § 222.

106 *See* 47 U.S.C. § 201(b).

107 *See* 15 U.S. Code § 45(a)(2).

108 Rebecca R. Ruiz, *First Lawsuits Filed Against the F.C.C.'s 'Net Neutrality' Rules*, N.Y. Times (March 23, 2015), *available at* http://bits.blogs.nytimes.com/2015/03/23/first-lawsuits-filed-against-the-f-c-c-s-net-neutrality-rules/?_r=0.

109 Press Release, U.S. Department of Health and Human Services–Office for Civil Rights, Data Breach Results in $4.8 Million HIPAA Settlements (May 7, 2014), *available at* http://www.hhs.gov/news/press/2014pres/05/20140507b.html.

110 Press Release, U.S. Securities and Exchange Commission, SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach (September 22, 2015), *available at* https://www.sec.gov/news/pressrelease/2015-202.html.

111 *Id.*

112 *Id.*

113 Peter Frost, *Data Breach at Advocate Medical Group to be Investigated by Federal Government, Illinois Attorney General*, Chicago Tribune (August 29, 2013), *available at* http://articles.chicagotribune.com/2013-08-29/business/ct-biz-0829-advocate-20130829_1_data-breach-health-information-attorney-general.

114 Ian Fullerton, *Court Clears Advocate Medical Group in Data-Breach Lawsuit*, Chicago Tribune (August 13, 2015), *available at* http://www.chicagotribune.com/suburbs/park-ridge/news/ct-prh-advocate-lawsuit-tl-0820-20150813-story.html.

115 *See* Press Release, Office of the Attorney General of the State of Massachusetts, South Shore Hospital to Pay $750,000 to Settle Data Breach Allegations (May 24, 2012), a*vailable at* http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-05-24-south-shore-hospital-data-breach-settlement.html.

116 *See* Press Release, Office of the Illinois Attorney General, Madigan Urges Jimmy John's Customers to Take Action, Report Unauthorized Charges (September 25, 2014), *available at* http://www.illinoisattorneygeneral.gov/pressroom/2014_09/20140925.html.

117 *See* http://ag.virginia.gov/files/Final_NAAG_Data_Breach_Notification_Letter.pdf.

118 *Id.*

119 *Id.*

120 *Hollingsworth v. Perry*, 133 S. Ct. 2652, 2661 (2013) (citing *Lujan*, 504 U.S. at 560-561).

121 *See Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013).

122 *Id.* at 1145.

123 *Id.* at 1143.

124 *Id.*

125 *Id.* at 1145.

126 *Id.* at 1143.

127 *Id.*

128 *Id.* at 1143.

129 *Id.*

130 There have been many cases in which courts have found an increased risk of future identity theft insufficient to support standing. *See, e.g., Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 640 (7th Cir. 2007).

131 Again, there are quite a few cases in which courts have found the time and finances expended to mitigate the chance of future harm are insufficient to support standing. *See, e.g., Grigsby v. Valve Corp.*, C12-0553JLR, 2012 WL 5993755 (W.D. Washington. November 14, 2012), at 5.

132 *See, e.g., Ruiz v. Gap, Inc*, 540 F. Supp. 2d 1121 (N.D. Cal. 2008).

133 *See, e.g., In re Barnes & Noble Pin Pad Litig.*, 12-CV-8617, 2013 WL 4759588 (N.D. Ill. September 3, 2013).

134 The benefit of the bargain theory turns on the idea that part of the purchase cost of whatever the plaintiffs purchased from the company included a cost for securing the plaintiffs' information. *See, e.g., In re LinkedIn User Privacy Litig.*, 932 F. Supp 2d 1089 (N.D. Cal. 2013).

135 *See, e.g., In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518 (N.D. Ill. 2011).

136 *Remijas v. Neiman Marcus Group, LLC*, 7th Cir., No. 14 C 1735 (July 20, 2015).

137 *Id.* at 9, citing *Clapper*, 133 S. Ct. at 1147.

138 *Id.* at 2-3.

139 *Id.* at 3.

140 *Id.* at 9.

141 *Id.*

142 *Id.* at 8.

143 *Id.*

144 *Id.* at 15.

145 *Id.*

146 *Id.* at 15-16.

147 *Id.* at 16.

148 *Id.* at 16.

149 *Id.*

150 *Robins v. Spokeo, Inc.*, 742 F.3d 409, 410 (9th Cir. 2014), *cert. granted,* 82 U.S.L.W. 3689 (U.S. April 27, 2015) (No. 13-1339).

151 *Id.* at 413.

152 *Id.* at 410.

153 *Id.*

154 *Id.* at 411.

155 *Id.* at 413-14.

156 *See, e.g.,* 815 ILCS 510.

157 *See Baum v. Keystone Mercy Health Plan,* No. 3876, 1250 EDA 2015 (Phila. C.P. March 25, 2015).

158 73 Pa.C.S. § 201-1, *et seq.*

159 *Id.* at 6.

160 *Id.* at 5-6.

161 *Id.* at 2.

162 *Id.* at 6.

163 *Id.* at 16-18.

164 *Id.* at 15-17.

165 *Id.* at 16-17.

166 *Id.* at 17.

167 *Id.* at 19.

168 73 Pa.C.S. § 201-2(4)(xxi).

169 *Id.* at 18-19.

170 *Ann M. v. Pac. Plaza Shopping Ctr.*, 6 Cal. 4th 666, 673 (1993).

171 *Small v. Fritz Companies, Inc.,* 30 Cal. 4th 167, 173 (2003).

172 *Id.*

173 *Lovell v. P.F. Chang's China Bistro, LLC*, W.D. Wash., No. C14-1152RSL (March 27, 2015).

174 *Id.* at 3.

175 *Id.*

176 *Id.* at 4-5.

177 *Id.* at 13.

178 *Id.*

179 *Id.*

180 *Textron Fin. Corp. v. Nationwide Mut. Ins. Co.*,115 Ohio App.3d 137, 684 N.E.2d 1261, 1266 (Ohio Ct. App. 1996).

181 *Lovell v. P.F. Chang's China Bistro, LLC*, W.D. Wash., No. C14-1152RSL (March 27, 2015), at 6.

182 *Id.* at 5.

183 *Id.*

184 *Id.* at 6.

185 *Id.* at 6-7.

186 15 U.S.C. § 1681(a).

187 15 U.S.C. § 1681(a).

188 *Id.*

189 15 U.S.C. § 1681(e).

190 *Holmes v. Countrywide Fin. Corp.*, 5:08-CV-00205-R, 2012 WL 2873892, at 16.

191 *See Tierney v. Advocate Health and Hospitals Corporation,* 14-3168, 2015 WL 4718875 (August 10, 2015).

192 *Id.* at 2.

193 *Id.* at 8.

194 *Id.* at 4.

195 *Id.* at 7.

196 *Id.* at 8.

197 *Id.* at 5.

198 *Id.* at 6.

199 *Id.* at 8-9.

200 *See* 18 U.S.C. § 2701.

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

202 *See, e.g., In re Michaels Stores Pin Pad Litig., supra*.

203 *See, e.g., Bell v. Blizzard Entertainment Inc.*, No. 2:12-cv-09475 (C.D. Cal. July 11, 2013).

204 *Id.* at 15-16.

U.S. CHAMBER
Institute for Legal Reform

202.463.5724 main
202.463.5302 fax

1615 H Street, NW
Washington, DC 20062

instituteforlegalreform.com