GIBSON DUNN

August 8, 2017

CYBERSECURITY & DATA PRIVACY: AN OVERVIEW FOR HEALTH CARE, PHARMACEUTICAL, AND BIOTECH COMPANIES

To Our Clients and Friends:

Cyberthreats are ubiquitous, and significant cyberattacks on private and publicly traded companies occur on a near-daily basis. As a result of the ongoing barrage of increasingly advanced and evolving cyberattacks, even companies with sophisticated security systems are potentially susceptible to a cybersecurity breach. A breach may lead to unauthorized access to sensitive company and personal data and have far-ranging and costly consequences. Immediately following a cyberattack, a company must work to secure its systems from further damage and/or data loss, handle media inquiries, and confront often-complex legal issues concerning notification to consumers, business partners, and government agencies. Thereafter, there may be civil lawsuits (including litigation with business partners, consumer class actions, and, for publicly traded companies, actions by shareholders), regulatory enforcement actions, and investigations by federal and state agencies. As breaches have become more frequent, federal, state, and foreign government regulators have responded by strengthening and expanding laws, regulations, and enforcement concerning cybersecurity and data privacy.

This article provides an overview of the key issues health care, pharmaceutical, and biotech companies face with regard to cybersecurity and data privacy. The article begins with a discussion of federal regulations, guidance, and enforcement actions. With myriad federal regulators asserting jurisdiction to regulate data security, companies are subject to an increasingly complex regulatory framework. The article also reviews certain notable state regulations and guidance that address cybersecurity and data security issues, and briefly summarizes some of the key issues related to data privacy outside the United States. Finally, the article closes with a discussion of the private civil litigation that can result from a data breach.

Table of Contents

---

1. Federal Regulation, Enforcement, and Guidance

There is no single regulatory body tasked with enforcing a uniform set of cybersecurity standards. For many years, the Federal Trade Commission ("FTC" or the "Commission") and the Department of Health and Human Services ("HHS") have been the primary federal regulators in the cybersecurity area. Recently, however, a number of other federal regulators have also entered the arena and have issued guidance and/or taken legal action against companies that allegedly have failed to implement adequate cybersecurity measures. These regulators include the Securities and Exchange Commission ("SEC"), the Food and Drug Administration ("FDA"), the Federal Communications Commission ("FCC"), the Consumer Financial Protection Bureau ("CFPB"), the Department of Energy ("DOE"), the Federal Deposit Insurance Corporation ("FDIC"), and the Financial Industry Regulatory Authority ("FINRA"), among others.

Although there are many federal regulators asserting jurisdiction over cybersecurity issues, the primary cybersecurity and privacy regulators for health care, pharmaceutical, and biotech companies (and those covered in this article) are the FTC, HHS, SEC, and FDA. The recent trends in guidance and enforcement actions by these agencies are described below.

1.1 Federal Trade Commission

1.1.1 Authority to Regulate Privacy and Cybersecurity

The FTC derives its authority to regulate cybersecurity practices from Section 5 of the FTC Act, which states that "unfair or deceptive acts or practices in or affecting commerce, are . . . unlawful."[1] Because the FTC Act dates to 1914, it does not mention cybersecurity. However, the FTC has long taken the

position that Congress intended "unfair" practices to be defined broadly and flexibly to allow the agency to effectively protect consumers as the economy and technology develop.[2]

The FTC first asserted that its authority under Section 5 encompassed investigating and prosecuting companies for insufficient data security procedures in 2002.[3] Since that time, the FTC has brought more than 60 data security cases—with more than half of those initiated since 2010.

Although most FTC enforcement actions have settled with a company agreeing to a consent order (discussed further below), there have been several high-profile challenges to the FTC's authority to bring data security enforcement actions. For example, companies have argued that Congress did not intend for the FTC to have broad regulatory authority over corporate cybersecurity practices under the FTC Act.[4]

While courts have thus far accepted the FTC's assertions of jurisdiction, a case regarding that issue is currently pending before the Eleventh Circuit. The case involves LabMD, a now-defunct medical testing laboratory. In 2013, the FTC sued LabMD, alleging that the company had failed to "develop, implement, or maintain a comprehensive information security program" to protect consumers' sensitive personal and health information.[5] After an Administrative Law Judge ruled in favor of LabMD on the company's argument that the FTC lacked authority to bring the action, the Commission overturned that decision and entered an order against the company. LabMD sought relief from the Eleventh Circuit, challenging the FTC's broad regulatory authority over cybersecurity practices.[6] Oral argument was heard on June 21, 2017, but the case remains pending; a three-judge panel granted LabMD's request to stay enforcement of the FTC's decision pending appeal.[7]

1.1.2 Enforcement

As noted above, the FTC has used its regulatory authority to initiate a number of civil enforcement actions in recent years. When the FTC brings these actions, data security liability under Section 5 is governed by a "reasonableness" test. This test considers data security measures (and statements made about such measures) in light of factors such as the sensitivity and volume of consumer information being stored; the size and complexity of the data storage operations; and the costs and benefits of taking additional steps to improve security and reduce vulnerabilities within the system. The FTC has stressed that because a perfect data security system is neither expected nor required, the mere fact that a data breach occurred will not necessarily subject a company to liability—so long as the security system and all statements issued about it were reasonable under the circumstances.

The LabMD case described above is relatively unique because most enforcement actions brought by the FTC are not litigated but, rather, result in the FTC entering into a consent order with the targeted company. Consent orders often include civil penalties and require that companies establish comprehensive security programs subject to independent audits or monitoring for up to 20 years; agree to make no misrepresentations regarding their handling of consumer data; and agree to notify consumers about the data breach and about methods to safeguard their personal information.[8]

1.1.3 Guidance

The FTC also has issued cybersecurity guidance to companies falling within its purview. For example, in June 2015 the FTC launched the "Start with Security" business education initiative.[9] The initiative includes guidance for businesses drawing on lessons learned from the data security cases previously brought by the FTC. The guidance outlines ten steps to implement in order to achieve effective data security. The steps are high-level, consisting of general advice such as "control access to data sensibly"; "require secure passwords and authentication"; "secure remote access to your network"; and "make sure your service providers implement reasonable security measures."

In September 2016, the FTC published a guide specifically relating to data breaches, *Data Breach Response: A Guide for Business*.[10] The guide features steps for securing operations, preventing additional data loss, fixing vulnerabilities, and notifying the appropriate parties of a data breach—including law enforcement, regulators, affected businesses and individuals, and the media. In May 2017, the FTC also launched a new website, ftc.gov/SmallBusiness, that includes articles, videos, and other information aimed at helping small businesses protect their computers and networks from scams and cyberattacks.[11]

Notably, whether or not a company follows the FTC's cybersecurity guidance has been cited as a factor in determining liability in FTC enforcement actions. For example, in *FTC v. Wyndham Worldwide Corp.*, the Third Circuit held that the defendant was on sufficient notice that its cybersecurity practices fell short of the FTC's cybersecurity standards.[12] In reaching its decision, the court pointed to several FTC publications and enforcement actions regarding cybersecurity, and noted that the company should have been aware that its practices fell short of those the FTC had previously deemed necessary.[13]

The FTC seems determined to maintain its position as the primary federal regulator of cybersecurity issues, as evidenced by recent statements regarding the regulation of broadband providers. In March 2017, Acting FTC Chair Maureen K. Ohlhausen issued a statement, together with the Chair of the FCC, stating that "jurisdiction over broadband providers' privacy and data security practices should be returned [from the FCC] to the FTC, the nation's expert agency with respect to these important subjects."[14] Ohlhausen expressed that all online actors should be governed by the same rules, enforced by one agency, stating that the federal government shouldn't favor one set of companies over another—and certainly not when it comes to a marketplace as dynamic as the Internet. So going forward, we will work together to establish a technology-neutral privacy framework for the online world. Such a uniform approach is in the best interests of consumers and has a long track record of success.

1.2 Department of Health and Human Services

The United States Department of Health and Human Services Office for Civil Rights ("HHS OCR") has enforcement responsibility for the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA provides a comprehensive framework for the use and disclosure of certain protected health information ("PHI"). Its requirements govern how such data may be used (the "Privacy Rule"); physical, technical, and administrative security standards that companies must have in place (the

"Security Rule"); and notice obligations in the case of unauthorized use or disclosure (the "Breach Notification Rule").

Enacted in 1996, HIPAA is in many ways the oldest and most well-developed data security regime under federal law. Although most other government agencies have only begun to address cyber-related issues in recent years, HHS OCR has been addressing these issues for more than two decades.

There has been a recent increase in both attention and enforcement proceedings related to HIPAA. As data security gets more attention, HHS OCR has increased the aggressiveness and scope of its enforcement efforts. Moreover, as health care companies increasingly become the target of cyberattacks, HIPAA has emerged as a key backdrop for all sorts of data breach litigation, in cases brought by both the government and private plaintiffs.

1.2.1 Applicability to Health Care, Pharmaceutical, and Biotech Companies

HIPAA regulations are directly applicable to "covered entities," which include health plans (e.g. insurers), certain health care providers (e.g., hospitals), and health care clearinghouses. However, HIPAA also is applicable to "business associates" of those covered entities, including companies that perform functions or activities on behalf of, or provide certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.

By the very nature of their businesses, health care, pharmaceutical, and biotech companies are very likely to encounter some type of protected health information. Although not every such company will be covered by HIPAA, many will, at least in some capacity. Indeed, it is possible that certain aspects of a company's business will be covered, for example, in its role as a business associate, even while others may not.

1.2.2 The Privacy Rule

The HIPAA Privacy Rule[15] establishes a set of standards for the protection of certain health information, and requires that covered entities and business associates use or disclose PHI only as permitted by the rule.[16] Although the rule is meant to allow for ordinary business operations, the regulations are nonetheless complicated and demand significant attention. Uses generally permitted under the rule include those connected with the treatment of a patient, payment requests, and a company's own health care operations (e.g., quality assessment and improvement activities).[17] There is also a hierarchy of other permitted uses, which are organized according to the type of permission or authorization required: some uses are permitted only with express patient authorization (e.g., commercial sale of PHI);[18] other uses require an opportunity for the individual to agree or object (e.g., listing in facility directories or for disaster relief purposes);[19] and finally, some uses are permitted even without authorization, so long as certain protections are in place (e.g., in litigation when there is a HIPAA-qualified protective order in place).[20] The Privacy Rule also establishes standards that govern the use of PHI for marketing purposes (e.g., prescription refill reminders),[21] research purposes,[22] and reporting related to public health activities, including reporting to the FDA.[23] The Privacy Rule is directly applicable to both covered entities and business associates, and also requires that covered entities have agreements in place with their business associates that limit the use of PHI to the specific purposes

enumerated by the agreement and permitted by HIPAA.[24] Before using or disclosing PHI in any fashion, it is important to understand how HIPAA treats that type of use under the hierarchy just described, and what rules therefore might apply.

1.2.3 The Security Rule

Whereas the Privacy Rule establishes how and when protected information may be used and disclosed, the Security Rule establishes standards for how that information must be protected.[25] The Security Rule references a variety of administrative, technical, and physical safeguards, and it includes required standards and implementation specifications related exclusively to electronic PHI ("ePHI"). Those standards and specifications deal at a relatively granular level with system requirements where ePHI is kept or stored. For example, HIPAA includes implementation specifications that govern encryption, automatic logoff, password management, and other detailed issues. Like the Privacy Rule, the Security Rule is also directly applicable to business associates.

Importantly, the Security Rule also requires that companies "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to . . . electronic protected health information."[26] These mandatory HIPAA risk assessments can be complicated and time-consuming, and HHS OCR has demonstrated its willingness to take enforcement action where a comprehensive and up-to-date assessment is not in place, as discussed below. A risk analysis process includes: (1) evaluating the likelihood and impact of potential risks to ePHI; (2) implementing appropriate security measures to address the risks identified in the risk analysis; (3) documenting the chosen security measures and, where required, the rationale for adopting those measures; and (4) maintaining continuous, reasonable, and appropriate security protections. Every company that deals with ePHI should therefore carefully evaluate its obligation to conduct a risk analysis and ensure it has a current, well documented, and comprehensive assessment in place.

1.2.4 The Breach Notification Rule

The third major component of HIPAA is the Breach Notification Rule.[27] Under the Breach Notification Rule, a covered entity must report unauthorized uses or disclosures of PHI to the government, the media, and affected individuals, with certain exceptions for small breaches.[28] Business associates are required to report breaches to the covered entity.[29] Under HIPAA, a breach is (1) the acquisition, access, use, or disclosure (2) of PHI (3) in a manner not permitted under the HIPAA Privacy Rule (4) that compromises the security or privacy of the PHI.[30] Any disclosure of PHI in a manner not permitted under the Privacy Rule is presumed to be a breach unless the covered entity performs a required "Risk Assessment" under 45 C.F.R. § 164.402(2) and demonstrates that there is a "low probability that the [PHI] has been compromised." Generally speaking, breach notifications must be sent within 60 days of the discovery of the breach.[31] HIPAA's notification obligations are in addition to state law requirements, which may impose notice obligations of shorter than 60 days.

1.2.5 HHS OCR Enforcement

HHS OCR has increased its enforcement efforts related to HIPAA in recent years. Several recent enforcement actions illustrate the types of incidents that can draw scrutiny from HHS OCR and the types of failures under the Privacy and Security Rules that can lead to large settlements.[32]

In April 2017, HHS OCR announced the first ever settlement involving a wireless health service provider, CardioNet, which provides mobile monitoring and rapid response to patients with cardiac arrhythmias. CardioNet agreed to pay $2.5 million in a HIPAA settlement after an employee's laptop containing the ePHI of over 1,300 individuals was stolen from a parked vehicle.[33] OCR's investigation revealed that CardioNet's policies and procedures were in draft form and had not yet been implemented, and CardioNet had "insufficient risk analysis and risk management processes in place."

In February 2017, Memorial Healthcare System paid a $5.5 million HIPAA settlement with HHS.[34] Memorial Healthcare System reported to HHS OCR that the ePHI of more than 115,000 individuals had been impermissibly accessed by its employees and improperly disclosed to affiliated physician office staff when the login credentials of a former employee had been used to access ePHI on a daily basis without detection for a year. HHS noted that although Memorial Healthcare System had workforce access policies and procedures in place, it failed to implement the procedure with regard to reviewing, modifying, or terminating users' rights of access.

In January 2017, HHS OCR issued a notice of Final Determination and a $3.3 million civil monetary penalty against Children's Medical Center of Dallas ("Children's") following impermissible disclosure of ePHI and many years of alleged non-compliance with the Security Rule.[35] The penalty followed several separate incidents resulting in the loss of ePHI, including loss of an employee's BlackBerry and theft of an unencrypted laptop. OCR's investigation of these incidents revealed that Children's failed to implement risk management plans even after they received external recommendations to do so, and they failed to deploy encryption measures on their devices, despite knowledge of the risk of maintaining unencrypted devices containing ePHI. The OCR Acting Director stated that "[a]lthough OCR prefers to settle cases and assist entities in implementing corrective action plans, a lack of risk management not only costs individuals the security of their data, but it can also cost covered entities a sizable fine."

In November 2016, the University of Massachusetts – Amherst ("UMass") agreed to pay $650,000 and enter a corrective action plan to settle alleged HIPAA violations.[36] UMass reported to OCR that "a workstation . . . was infected with a malware program, which resulted in the impermissible disclosure of electronic protected health information (ePHI) of 1,670 individuals, including names, addresses, social security numbers, dates of birth, health insurance information, diagnoses and procedure codes."[37] According to OCR, UMass "determined that the malware was a generic remote access Trojan that infiltrated their system, providing impermissible access to ePHI, because UMass did not have a firewall in place."[38] OCR's investigation found that UMass had failed to categorize components of its operations appropriately under HIPAA, resulting in ePHI being present on systems that were not HIPAA compliant. OCR's investigation also faulted UMass for its failure to complete an accurate and thorough risk analysis and the lack of a firewall.

In August 2016, Advocate Health Care System ("Advocate") agreed to pay $5.55 million to settle a variety of HIPAA violations.[39] Among the violations was a data breach of Advocate's subcontractor billing company that exposed sensitive patient information. HHS found that Advocate failed to obtain written assurances from its business associate that electronic patient data would be appropriately protected.

Finally, in December 2015, the University of Washington ("UW") agreed to pay $750,000 and enter into a corrective action plan to resolve allegations that it violated the HIPAA Security Rule.[40] OCR initiated an investigation of UW after it received a breach report indicating that ePHI for more than 90,000 individuals was "accessed after an employee downloaded an email attachment that contained malicious malware."[41] According to OCR, the malware "compromised the organization's IT system," including patient data such as names, medical record numbers, dates of service, bill balances, social security numbers, and insurance identification or Medicare numbers.[42] OCR's investigation found that UW failed to ensure that its affiliates conducted risk assessments and responded to risks and vulnerabilities in their environments.

1.3 Securities and Exchange Commission

In the last few years, the SEC has increased its focus on cybersecurity, particularly in the areas of protecting client data, creating disclosure standards for cybersecurity risks and incidents, and ensuring the orderly functioning of the markets. In May 2016, then-SEC Chair Mary Jo White explained that cybersecurity is the biggest risk facing the financial system, stating that the "[SEC] can't do enough in this sector[.]"[43] The SEC's Office of Compliance Inspections and Examinations identified cybersecurity as one of its examination priorities in 2015, 2016 and 2017.[44] And most recently, Trump administration officials reiterated the SEC's dedication to cybersecurity issues and enforcement, with SEC Chairman Jay Clayton affirming that the SEC is working "to improve [its] ability to receive critical information and alerts and react to cyber threats."[45] In addition, as explained below, the SEC staff has issued disclosure guidance relating to cybersecurity that is applicable to all public companies, including those in the health care, pharmaceutical, and biotech industries.

1.3.1 Guidance

In 2011, the SEC staff released CF Disclosure Guidance: Topic No. 2, which relates to public company disclosures regarding cybersecurity risks and cyber incidents.[46] The guidance provides that registrants should disclose risks of cybersecurity incidents if "these issues are among the most significant factors that make an investment in the company speculative or risky."[47] The guidance provides recommendations on a number of topics. For example, the SEC instructs that companies should disclose the risk of cyber incidents and that disclosures should not be generic or boilerplate. However, companies are not required to disclose threats if doing so would compromise the companies' cybersecurity. The guidance also advises that companies should address cybersecurity risks in their Management's Discussion and Analysis of Financial Condition and Results of Operations ("MD&A") if the costs associated with the risks are likely to have a material effect on the company's operations, liquidity, or financial condition, or would cause reported financial information not to be necessarily indicative of future operating results or financial condition. The SEC staff further advises that companies should

disclose cyber incidents that materially affect their operations in their Description of Business and Legal Proceedings disclosures. Finally, the SEC staff provides guidance on how to account for cybersecurity risks and incidents in company financial statements.

Additionally, in a June 2014 speech, then-SEC Commissioner Luis A. Aguilar provided boards of directors with important, albeit informal, cybersecurity guidance.[48] He advised that boards of directors should ensure the adequacy of a company's cybersecurity measures and, as a guide, should look to the industry standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity, released by the National Institute of Standards and Technology ("NIST"). Commissioner Aguilar's other recommendations included cyber-risk education for directors, creating a separate enterprise risk committee on the board, ensuring that the company has cyber-risk management personnel who report regularly to the board, and developing a well-constructed, deliberate company cyber incident response plan.[49]

The SEC also issued a Ransomware Alert in response to the WannaCry ransomware attack of May 2017, which affected numerous organizations in over one hundred countries.[50] The alert explained how hackers gain access to servers, and encouraged organizations to review the alert published by the U.S. Department of Homeland Security's Computer Emergency Readiness Team and evaluate whether applicable operating system patches had been installed. The SEC alert also discussed the importance of conducting periodic cyber-risk assessments, conducting penetration tests and vulnerability scans, and updating system maintenance.

1.3.2 Enforcement

To date, the SEC has brought only a few cybersecurity enforcement actions, involving companies' failure to adequately safeguard their customers' personal information. The enforcement actions involved companies in the financial sector and alleged violations of Rule 30(a) of Regulation S-P, also know n as the "Safeguards Rule." This regulation requires brokers, dealers, investment companies, and registered investment advisers to "adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information."[51]

In 2015, investment adviser R.T. Jones Capital Equities Management agreed to pay a $75,000 penalty as a settlement for the firm's failure to establish cybersecurity policies and practices.[52] The penalty was levied in response to a June 2013 breach of the company's server, which exposed the personal information of 100,000 customers.

On April 12, 2016, Craig Scott Capital agreed to pay $100,000 to resolve allegations that it violated the Safeguards Rule by using email addresses other than those with the company's domain name to electronically receive more than 4,000 faxes from customers and other third parties.[53] The SEC found that this practice was evidence of a "failure to adopt written policies and procedures reasonably designed to insure the security and confidentiality of customer records and information."

On June 8, 2016, Morgan Stanley agreed to pay a $1 million penalty to settle charges "related to its failures to protect customer information, some of which was hacked and offered for sale online."[54] These alleged failures included the company's decision not to conduct auditing or testing

of its "portals" that allowed for access to customer data.[55] As a result of these failures, the company suffered a breach, which exposed customer data on the internet. Despite the fact that Morgan Stanley had acted quickly to respond to the breach, take the customer data offline, and alert the proper authorities, the SEC found that Morgan Stanley violated the "Safeguards Rule."[56]

In each of these matters, the SEC found against the companies even though there was no apparent financial harm to their customers. Thus, companies should be aware that lax cybersecurity standards could lead to an SEC enforcement action even if there is no appreciable harm to customers resulting from such practices. That said, it is important to note that these cases involved companies in the financial sector, which are subject to the SEC's Regulation S-P. It is not clear whether the SEC would treat companies outside the financial sector (and not subject to Regulation S-P) in a similar manner. In addition, while the SEC has now acted three times against companies for failure to protect investor data, it has yet to initiate an enforcement action against a company for the failure to disclose a cybersecurity incident or threat. However, in April 2016, the SEC warned that it expects to initiate more cybersecurity enforcement actions in the future.[57]

1.4 Food and Drug Administration

Thus far, the FDA has not been a leader in cybersecurity enforcement. In fact, a recent report analyzing the FDA's cybersecurity regulatory practices criticized the FDA as being "in a constant state of offering subtle suggestions where regulatory enforcement is needed."[58]

In the absence of clarity on the agency's cybersecurity priorities based on past enforcement actions, health care, pharmaceutical, and biotech companies should pay particular attention to recent cybersecurity guidance issued by the FDA. The guidance is most applicable to medical device companies, as medical devices have been the primary focus of those guidance efforts.

1.4.1 Guidance

In December 2016, the FDA released the *Postmarket Management of Cybersecurity in Medical Devices Guidance*, which outlines steps manufacturers should take to continually address cybersecurity risks associated with medical devices.[59] The "Internet of Things" (which refers to everyday objects, such as thermostats and refrigerators, with connectivity to the Internet) now includes medical devices, which are often connected to both the Internet and hospital intranets and are vulnerable to cyberattacks. The FDA's guidance is aimed at ensuring the security of such devices in light of these vulnerabilities. To that end, the FDA recommends that medical device manufacturers conduct routine post-market surveillance of their products and develop programs to assess the cyber risks that could potentially be associated with their products. In January 2017, the FDA held a webinar on the guidance.[60] The 2016 guidance follows guidance issued by the FDA in 2014 regarding pre-market steps medical device companies should take to implement security into the design and development of medical devices.[61]

1.4.2 Enforcement

In April 2017, the FDA sent a warning letter to Abbott (St. Jude Medical Inc.), marking its most public enforcement effort to date in the cybersecurity space.[62] Specifically, the letter addressed alleged

cybersecurity issues related to Abbott's at-home monitoring devices. It remains to be seen, however, whether this is the beginning of a trend of FDA enforcement actions related to cybersecurity, or an isolated foray into the field.

2. State Regulation, Enforcement, and Guidance

State attorneys general play a significant role in policing cybersecurity issues. Several states have enacted statutes or regulations that establish specific cybersecurity standards.[63] State attorneys general also use state consumer protection laws, including laws patterned after the FTC Act (known as "Little FTC Acts"), and the Uniform Deceptive Trade Practice Act to address data security issues using theories analogous to those applied by the FTC in enforcing Section 5 of the FTC Act. Companies may look to FTC guidance (*supra*, Section 1.1.3) to understand what these state analogues typically require with regard to data security practices.

In addition, nearly every state has adopted laws that impose notification requirements on entities that have suffered a data breach. These laws generally contain provisions describing who must comply with the law (e.g., businesses, data/information brokers, government entities); definitions of "personal information" (e.g., name combined with social security number, driver's license or state ID numbers, account numbers); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information). State attorneys general have brought enforcement actions pursuant to these provisions.[64] One such action revolves around Target's 2013 data breach that resulted in the theft of the names, credit card numbers, and email addresses of approximately forty million customers. In May 2017, Target reached a $18.5 million settlement agreement with forty-seven state attorneys general and the District of Columbia.[65] In addition to the monetary settlement, Target agreed to better maintain software encryption programs, separate cardholder data from its normal computer network, and pay for an independent assessment of its security efforts.

Some states also have issued specific guidance or regulations on data security. In 2014, the California Attorney General released "Cybersecurity in the Golden State," a framework for protecting against and responding to data breaches and other cyber incidents.[66] The California report, like other guidance, emphasizes risk assessment, involvement from a company's leadership, adherence to industry best practices, training and education, and incident response planning. Likewise, in New York, new regulations relating to data security standards in the financial industry have recently come into effect; these regulations may affect many health insurance providers, among others.[67] Companies should be aware of the regulations in those states in which they do business.

3. International Issues

3.1 Key Non-U.S. Regulators

In addition to the many U.S. government regulations, companies with operations overseas must also consider data protection regulations of foreign jurisdictions. Prominent foreign regulators include those in the European Union (European Data Protection Supervisor), the United Kingdom (Information Commissioners Office - ICO), Germany (the Federal Data Protection Commissioner, the states' Data

Protection Authority), and Canada (Office of the Privacy Commission of Canada, provincial Information and Privacy Commissioners). While a full discussion of cybersecurity requirements outside the United States is beyond the scope of this article, every company should evaluate the laws, regulations, and other requirements of each country in which it operates so that it complies with all applicable requirements and is prepared to interact quickly with regulators in the event of a breach.

3.2 EU-U.S. Safe Harbor and Data Transfer

One important international privacy law issue for many companies involves European data transfer law, which governs the protection of personal data in the European Union and limits how U.S.-based companies may use and transfer data originating in Europe.

The Charter of the Fundamental Rights of the European Union (the "Charter") creates a right to protection of personal data.[68] The European Union also issued Directive 95/46/EC ("EU Data Protection Directive") in 1995, governing the protection of individuals with regard to the processing of their personal data within the EU.[69] Article 28(1) of the EU Data Protection Directive requires Member States to establish public authorities responsible for independent monitoring of compliance with EU rules on the protection of individuals and processing of personal data. Article 25(1) of the EU Data Protection Directive also specifies a principle that transfers of personal data from the Member States to third countries may take place only if the third country ensures an "adequate level of protection."[70]

To facilitate international commerce between EU Member States and the United States, the U.S. Department of Commerce issued the Safe Harbor Privacy Principles (the "Safe Harbor") in 2000.[71] The Safe Harbor included a number of principles on protection of personal data to which U.S. companies could subscribe voluntarily. For years, the Safe Harbor was used by U.S. organizations receiving personal data from the EU. Companies pledged adherence to Safe Harbor principles through a process of self-certification. Despite European acceptance of the Safe Harbor for many years, the Safe Harbor became increasingly questioned, with EU policymakers calling for an overhaul of the system. Then, in 2015, the European Court of Justice ("ECJ") invalidated the EU-U.S. Safe Harbor.[72]

In mid-2016, the U.S. Department of Commerce announced the approval of the EU-U.S. Privacy Shield Framework ("Privacy Shield"), which replaces the Safe Harbor. The Privacy Shield allows U.S. businesses to develop a conforming privacy policy, identify an independent recourse mechanism, and self-certify through a Commerce Department website. Among other benefits, the Privacy Shield states that participating organizations will be deemed to provide "adequate" privacy protection for the transfer of personal data outside of the European Union under the EU Data Protection Directive.[73] However, legal challenges against the Privacy Shield already have been filed, asserting many of the same arguments used against the Safe Harbor. Given the potential that the Privacy Shield, like the Safe Harbor, may be disallowed by the ECJ, companies would be well-served to consider a "belt and suspenders" approach to data transfer, pairing Privacy Shield participation with the adoption of other measures—such as Binding Corporate Resolutions ("BCRs") regarding the manner in which the company will handle EU data that can facilitate such transfers in accordance with EU law.

3.3 New European Regulations: NIS and GDPR

In 2016, the European Union announced the adoption of the Network and Information Security ("NIS") Directive and General Data Protection Regulation ("GDPR"), which will go into effect in May 2018. The GDPR establishes security and notification provisions to protect personal data, while the NIS establishes security obligations for operators of essential services and digital service providers. The NIS and GDPR, taken together, amount to a comprehensive overhaul of EU data protection regulations, and impose steep penalties for non-compliance. These regulations deserve close scrutiny from any company performing business in Europe or processing data on EU residents.

The United Kingdom has repeatedly reaffirmed its commitment to data privacy in the wake of its decision to exit the European Union. For example, in a June 2017 speech, Queen Elizabeth II outlined the UK's proposed Data Protection Bill, which would replace the Data Protection Act of 1998.[74] Importantly, the UK will implement the EU's GDPR while the UK is still a member of the EU. Once the UK has left the European Union, the UK appears poised to enable members of the UK to have the same ability to share data with the EU as they did previously.

3.4 New Asia-Pacific Regulations

On June 1, 2017, a new Chinese law went into effect that "bans the collection and sale of users' personal information" and requires that firms store sensitive user data on servers in China.[75] Commentators have expressed concerns with the new law because it is unclear what information will be considered sensitive. Additionally, the scope of some of the key provisions of the law, such as the requirement that companies submit their products to the Chinese government for cybersecurity checks, remains unknown. It is unclear how often such checks will be required and how the Chinese government will determine what products need to be checked.[76] Failure to comply with the new law could result in fines up to one million yuan (about $150,000) and potential criminal charges.[77]

4. Civil Litigation

In addition to government regulatory action, in the wake of a data breach companies handling sensitive data also face the risk of private civil litigation. To date, pharmaceutical and biotech companies have not been frequent targets of such litigation. But because no company is immune in the wake of a cyberattack, any comprehensive data security assessment and plan should account for the specific risks posed by civil litigation.

This section (1) provides an overview of the types of information that create the greatest exposure to civil litigation, (2) reviews the most common theories of liability in civil litigation, and (3) discusses the key issue of a plaintiff's standing to bring data breach litigation.

4.1 Data that Creates Exposure to Civil Litigation

4.1.1 Consumer Data

Most data security litigation is premised on the loss or exposure of consumer data. Often, these cases involve retailers, health care providers, and technology companies that collect personal identifying information ("PII") from customers, including names, addresses, credit card numbers, and social security numbers.

Any amount of consumer data—if accessed in a data breach—can create exposure for a company. Indeed, while the greatest risks come from purported class actions involving compromises of hundreds of thousands of consumers' information, plaintiffs have shown a willingness to bring suits even when far fewer consumer records are exposed in a breach.[78] As such, health care, pharmaceutical and biotech companies should understand and identify what consumer data they collect and retain as part of their business operations, whether it is from clinical trials, customer lists, or other sources.

4.1.2 Employee Data

Data breach litigation also can be premised on the loss or exposure of employee data. Most companies have extensive information about their employees, including PII (e.g., name, address, social security number), financial information (e.g., bank account numbers, retirement account numbers), and even protected health information (e.g., medical insurance information, disability claims information). Large companies may maintain such information for tens- or even hundreds-of-thousands of individuals. To facilitate business functions related to human resources, benefits administration, and information technology systems, among other things, this information is often centrally managed and accessible.

It is no surprise then, that employee data can be a rich target for cyber criminals. The loss of such data inevitably gives rise to civil litigation. In one high-profile data breach, for example, employees at a media company sued their employer for allegedly failing to protect their personal data, claims that the company eventually settled for more than $8 million.[79]

4.1.3 Intellectual Property and Trade Secrets

Although the vast majority of data breach litigation is based on the loss of consumer or employee data, health care, pharmaceutical, and biotech companies also may face a risk of litigation related to the theft of intellectual property or trade secrets during any data breach. For companies that depend on research, development, and innovation to drive their business, loss of such information can be highly costly in its own right. Although it has not been the basis of many prominent cases to date, theft of that information could also give rise to private litigation, whether from business partners, shareholders, or other affected groups.

4.2 Theories of Liability

Data breach litigation is a relatively new area, with most cases having been filed within the last five years. As such, few cases have proceeded to adjudication on the merits—whether through summary

judgment or trial—and therefore substantive standards of liability are underdeveloped. There are, however, several common theories of liability that plaintiffs routinely advance. Under any of these claims, a company's liability will, of course, depend on the facts of the case. But in evaluating the risks associated with a data breach, companies should be mindful of how their actions could be viewed under different legal theories. Some of the common claims and legal theories that have been advanced by plaintiffs are discussed below.

4.2.1 Common Law Liability—Negligence and Related Theories

The most common claim in data breach litigation is common law negligence. Plaintiffs argue that companies have a duty to provide security for customer, employee, and other sensitive information, and that a company violates that duty by failing to protect against a data breach.[80] In negligence cases, the fundamental standard against which companies are judged is "reasonableness"—that is, did the company take reasonable precautions to understand risks, prepare for, and prevent a data breach. In the event of a breach, the reasonableness of a company's response, including adequate breach notification under relevant notice statutes (discussed below), is equally important. Until a body of case law develops to determine what is considered "reasonable," the touchstone for reasonableness is likely to be the government guidance discussed in Section 2 above, along with industry best practices. Even then, given the rapidly evolving nature of cyber threats and defenses, reasonableness is likely to be a moving target.

In addition to negligence, other common law theories of liability advanced by plaintiffs include invasion of privacy,[81] unjust enrichment,[82] negligent misrepresentation, and fraud.[83] Compared to negligence, which plaintiffs allege in almost every case, these are secondary theories of liability. But they present some unique risks. For example, to guard against the risk of negligent misrepresentation and fraud claims (in addition to securities actions and FTC enforcement actions, among others), companies must remain attuned to *what they say and represent* about their security practices, not only the objective reasonableness of those practices.

4.2.2 Statutory Liability

There are also several federal and state statutes that, in certain circumstances, provide for a private right of action for an individual plaintiff in cases of data breaches.

At the federal level, plaintiffs have attempted to bring suit under a variety of federal statutes in the wake of data breaches, including the Fair Credit Reporting Act,[84] the federal Privacy Act,[85] and the Stored Communications Act.[86] Thus far, plaintiffs have not been very successful under these statutes,[87] which tend to require intentional or knowing behavior that results in a disclosure of information, and therefore are inapplicable to most data breach situations (where a company, along with its consumers or employees, is a victim of a criminal third party). As such, these federal statutes, as interpreted and applied to date, have presented a relatively low risk in the civil litigation context—at least insofar as data breaches are concerned.[88]

At the state level, there are several different theories of liability that plaintiffs have pursued with more success. First, state consumer protection statutes often provide plaintiffs with private causes of action for unfair and deceptive trade practices, and plaintiffs have been able to use such statutes to pursue data

breach litigation premised on those allegedly unfair business practices.[89] Like FTC enforcement actions and claims premised on fraud and misrepresentation, these claims are most often based on statements a company makes about its data security practices, and are most successful when those statements are inconsistent with a company's actual practices. Second, some states have passed laws or regulations specific to data security or consumer records.[90] And third, nearly every state also has a data breach notification statute that requires companies to notify consumers in the event of a data breach.[91] Most data breach litigation includes at least some of these state law claims in addition to common law theories of liability discussed above.[92] And in nationwide breaches, companies can often face numerous state law claims from different jurisdictions.[93]

4.2.3 Contractual Liability

Health care, pharmaceutical, and biotech companies may also be subject to liability, based on an express or implied contract, for data security issues that affect their customers or business partners.[94] Although these theories are less common than negligence-based and statutory theories by customers, their existence counsels in favor of careful consideration of contractual approaches to limiting risk in the event of a data breach.[95]

There is also the potential for more novel theories of contractual liability. For example, an area of risk for biotech companies is the possibility that medical devices may be hacked to create a "back-door" into networks at health care companies. Indeed, some reports have warned against a threat of cyber criminals hacking devices such as X-ray machines, CT scanners, and MRI machines—which are connected to hospital networks—to gain broader access to patient records and other sensitive information at health care providers.[96] Contracts should address the risks of improper use and cyberattacks of such devices. Without contractual indemnification, this type of attack potentially could give rise to liability for manufacturers.

4.3 Standing in Data Breach Litigation

As noted, very few data breach cases have reached adjudication on the merits. Instead, much of the litigation by private plaintiffs has focused on the threshold issue of whether plaintiffs have standing to pursue their cases. Because of the importance of standing issues to data breach litigation, this issue is addressed in more detail below.

For many years, companies facing civil suits related to data breaches often succeeded at the motion to dismiss stage by arguing that plaintiffs could not show actual harm, and therefore did not have standing to pursue their claims. As one court observed, "despite generating little or no discussion in most other cases, the issue of injury-in-fact has become standard fare in cases involving data privacy[, and] the court is hard-pressed to find even one recent data privacy case . . . in which injury-in-fact has not been challenged."[97] Indeed, one of the first and most powerful defense tools in any data breach litigation is to challenge, with a motion to dismiss, whether a plaintiff or class of plaintiffs has sufficiently alleged actual harm. Reflecting the importance of this issue, the Supreme Court has weighed in with two decisions in recent years that set the framework for analyzing standing in data breach cases.

In *Clapper v. Amnesty International USA*[98] the Supreme Court established the test for the injury-in-fact element of Article III standing in data security cases. In *Clapper*, human rights organizations and media groups challenged the constitutionality of an amendment to the Foreign Intelligence Surveillance Act that made it easier for the government to obtain wiretaps on intelligence targets outside of the United States. The plaintiffs, all U.S. persons, alleged that they had standing because their work included privileged telephone and email communications with people who were likely foreign targets of surveillance and such communications could be intercepted in the future. The plaintiffs also alleged that they had suffered injury by undertaking costly steps to protect their communications from surveillance. The Supreme Court held that the allegations of potential interception of privileged communications were too speculative to sustain a claim, determining that "a highly attenuated chain of possibilities [] does not satisfy the requirement that threatened injury must be certainly impending"[99] and that plaintiffs cannot manufacture standing "merely by inflicting harm on themselves based on their fears of hypothetical future harm."[100]

Where plaintiffs might not otherwise be able to satisfy Article III standing requirements—in particular the element of actual injury—they have often tried to predicate their privacy claims on statutory rights of action, under the theory that a statutory violation is a sufficient harm to create Article III standing. That is the issue the Supreme Court took up in *Spokeo, Inc. v. Robins*.[101] In *Spokeo*, the plaintiff, Thomas Robins, filed a class action complaint claiming that Spokeo—which operates a "people search engine" that gathers and provides information about individuals —willfully failed to comply with the requirements of the Fair Credit Reporting Act, 15 U.S.C. § 1681e(b).[102] The Ninth Circuit ruled that Robins had satisfied the Article III injury-in-fact requirement because "Spokeo violated *his* statutory rights, not just the statutory rights of other people" and his "personal interests in the handling of his credit information are individualized rather than collective."[103]

The Supreme Court vacated and remanded, holding that the Ninth Circuit's Article III analysis was "incomplete"; although it considered whether the alleged injury was "particularized," it had "overlooked" whether Robins had also alleged a "concrete" injury.[104] The Court explained that it has "made it clear time and time again that an injury in fact must be both concrete *and* particularized."[105] An injury must be "particularized" in that it "must affect the plaintiff in a personal and individual way."[106] But while "[p]articularization is necessary to establish injury in fact, . . . it is not sufficient" because "[a]n injury in fact must also be 'concrete.'"[107]

While the Court did not resolve whether Robins had alleged a concrete injury, it provided guidance on the meaning of this requirement and the role that statutes play in assessing whether a plaintiff has standing under Article III. The Court first explained that "[a]lthough tangible injuries are perhaps easier to recognize, . . . intangible injuries can nevertheless be concrete."[108] The Court made clear that this "does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[109] Rather, "Article III standing requires a concrete injury even in the context of a statutory violation."[110] Thus, "Robins could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III."[111] The Court, however, noted that it is possible for a "risk of real harm" to "satisfy the requirement of concreteness," and

acknowledged that "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact."[112]

After the decisions in *Clapper* and *Spokeo*, plaintiffs have become more adept at pleading standing, and more and more suits are therefore surviving motions to dismiss. In the immediate wake of *Clapper*, the majority of courts deciding data breach cases held that absent allegations of actual identity theft or other fraud, increased risk of harm alone is insufficient to confer Article III standing.[113] But plaintiffs have succeeded in pleading the requisite "certainly impending" harm when they are able to point to alleged injuries such as unlawful charges, restricted or blocked access to bank accounts, inability to pay bills, or late payment charges or new card fees.[114] In the short time since the Supreme Court's decision in *Spokeo*, lower courts have continued to grapple with when, and how, a statutory violation can create standing. While several courts have held that plaintiffs fail to allege a concrete injury when their harm is based on a procedural violation of a statute,[115] others have found that plaintiffs can survive under *Spokeo*, especially where a statute creates substantive, not only procedural, rights.[116]

One issue that could arise for health care, pharmaceutical and biotech companies in this context relates to the nature of the information they possess. Whereas plaintiffs have had difficulty showing that mere disclosure of their identity—without more—creates standing, health-related information is more sensitive. Thus far, medical information has not necessarily been subject to any heightened standard absent a showing of actual harm. Indeed, several courts that have considered alleged breaches related to medical records and personal health information have declined to find standing.[117] But as plaintiffs become more adept at pleading around the standing requirement, precisely how courts analyze standing in the context of health-related information after *Clapper* and *Spokeo* remains to be seen.

4.4 Shareholder and Securities Litigation

4.4.1 Shareholder Derivative Litigation

Some corporate data breaches also may result in shareholder derivative litigation against a company's officers and directors, alleging breaches of fiduciary duties, mismanagement, abuse of control, and/or corporate waste relating to a company's policies and procedures concerning cybersecurity, disclosures, and response to cyberattacks. To date, plaintiffs have not had great success pursuing such claims. But the risk of shareholder derivative litigation remains alive in any data breach situation, so boards and officers should be proactive in addressing cybersecurity practices and disclosures both before and after any breach to protect themselves against liability.

In *Palkon v. Holmes*, one of the few cases to address claims against directors and officers after a cyberattack, plaintiff filed a derivative lawsuit in the District of New Jersey against directors and officers of Wyndham Hotels. After making a demand on the board that was refused, plaintiff brought an action asserting claims for breach of fiduciary duty, waste of corporate assets, and unjust enrichment, relating to three separate data breaches that took place between April 2008 and January 2010 and impacted more than 600,000 customers, alleging that the defendants failed to implement adequate data security mechanisms and failed to timely disclose the breaches after they occurred.[118] In October 2014, the district court dismissed the action, finding that the board's refusal of the shareholder demand constituted

a legitimate exercise of the business judgment rule. The court based this finding on a number of factors, including the fact that the board and audit committee had discussed the breaches and data security at numerous meetings, the company had hired technology security firms to investigate the breaches and make recommendations, and the company had begun to implement the recommendations.[119]

One of the most prominent derivative actions based on a cyberattack was brought against directors and officers of Target after a breach in 2013 compromised credit card and personal data of up to 110 million people. In *Davis v. Steinhafel*, plaintiffs filed derivative lawsuits against Target directors and officers, asserting claims of breach of fiduciary duty, gross mismanagement, waste of corporate assets, and abuse of control. Plaintiffs alleged that the defendants failed to take adequate steps to prevent a cyberattack, concealed facts from the public, and "bungled" the company's response to the attack. In response to the derivative lawsuits and a demand on the board, Target's board established a Special Litigation Committee, which conducted an extensive, two-year investigation into whether it was in the corporation's best interests to pursue any of the claims. The Special Litigation Committee ultimately concluded that it was not in Target's best interests to pursue such claims based on numerous factual and legal considerations, including the applicability of the business judgment rule protecting reasonably prudent good faith business decisions.[120] After issuing a report containing its conclusions, the Committee made a motion to dismiss the action, which was unopposed by plaintiffs, and was granted in July 2016.[121]

Plaintiffs brought similar claims against directors and officers of Home Depot following another high-profile data breach. In *In re the Home Depot, Inc. Shareholder Derivative Litigation*, Home Depot shareholders filed a derivative lawsuit in September 2015 in district court in Georgia. On November 30, 2016, the court dismissed the action on grounds that shareholders failed to either demand that the board take action or demonstrate that such a demand would have been futile.[122] Since the Home Depot plaintiffs made no demand prior to filing suit, the court turned to the issue of demand futility.[123] To demonstrate demand futility under Delaware law, a plaintiff must plead particularized facts that establish reasonable doubt regarding the ability and willingness of the board to evaluate a demand in a disinterested manner.[124] With regard to plaintiffs' primary claim for breach of the duty of loyalty, the court found that "[w]hen added to the general demand futility standard, the Plaintiffs essentially need to show with particularized facts beyond a reasonable doubt that a majority of the Board faced substantial liability because it consciously failed to act in the face of a known duty to act."[125] The court concluded that plaintiffs' allegations that the board violated this duty by disbanding Home Depot's infrastructure committee and moving too slowly in addressing the security breach were insufficient to overcome this "incredibly high hurdle."[126] After arriving at a similar conclusion for the claims for corporate waste[127] and violations of Section 14(a) of the Securities Exchange Act,[128] the court held that plaintiffs' failure to make a pre-suit demand was not excused, dismissed the case with prejudice, and permitted defendants to recover costs.[129]

Although the hurdles for success of such shareholder claims remain high, a company experiencing a major breach should be prepared for such litigation. As the decisions to date demonstrate, in such litigation, it will be important for any defense of directors and officers to be able to show that cybersecurity risks are routinely considered and addressed, even before a breach occurs.

4.4.2 Securities Class Action Litigation

In addition to shareholder derivative litigation, in the wake of a cyberattack, there is also a risk of securities class actions premised on a company's public disclosures about its cybersecurity practices and risks, particularly if a disclosure concerning a breach causes a significant stock price drop.

A good starting point for any company seeking to understand its obligations with regard to disclosures about data security is the SEC's 2011 guidance.[130] As discussed above in Section 2.3.1, the SEC has recommended that registrants make disclosures related to data security in certain circumstances, including where the risks associated with potential or actual cyber incidents represents a material event for the company or could have a material effect on the financial condition of the company.[131]

In the few securities cases that have been filed, plaintiffs have argued that companies committed securities fraud by making misleading statements about their data security practices or the risks posed by cybersecurity incidents or breaches. For example, in January 2017, Yahoo! Inc. (now Altaba Inc.) was sued after announcements in September and December 2016 that it had suffered significant cybersecurity breaches..[132] Thus far, however, these types of theories have been largely unsuccessful. Indeed, in one of the few cases to address such theories, a court rejected plaintiffs' claims and recognized that even a company's good-faith statements can be quickly outdated given the challenges of data security issues.[133] As one court has noted, "[t]he fact that a company has suffered a security breach does not demonstrate that the company did not place significant emphasis on maintaining a high level of security."[134] Nonetheless, the threat of securities fraud litigation is another reason that every company should carefully evaluate its public disclosures regarding its data security practices and risks.

5. Conclusion

Given the varied cybersecurity-related regulatory and litigation risks that health care, pharmaceutical, and biotech companies face, planning, assessment, and preparation are key. Among other things, such activities require close coordination between companies' legal, IT, and senior management teams with regard to setting strategy; auditing areas of cyber risk; and developing, implementing, and testing response plans. While no defense is perfect, making such preparations may help companies minimize the impact of any cybersecurity incidents when such incidents occur.

---

[1] 15 U.S.C. § 45(a)(1).

[2] *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 242 (3d Cir. 2015).

[3] *See* Fed. Trade Comm'n, "Commission Statement Marking the FTC's 50th Data Security Settlement" (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[4] *See Wyndham*, 799 F.3d at 247. The hotel chain Wyndham Worldwide Corp. raised this argument (among others) in response to an enforcement action brought by the FTC in the wake of three

data breaches suffered by the company. The FTC alleged that the hotelier's failure to use encryption, firewalls, and non-obvious passwords constituted an "unfair" practice under Section 5 of the FTC Act. After Wyndham challenged the FTC's ability to bring its case, in 2015 the Third Circuit unanimously upheld the FTC's jurisdiction over such issues. *Id*. at 240. Wyndham entered into a consent order with the FTC shortly thereafter. Press Release, Fed. Trade Comm'n, *Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk* (Dec. 9, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.

[5] Complaint, *In the Matter of LabMD, Inc*., No. 102-3099 (Aug. 28, 2013), No. 9357.

[6] Specifically, LabMD challenged the FTC's authority to bring an enforcement action on three bases, arguing: (1) only HHS is empowered to regulate patient-related or health care data-security practices, and the FTC is thus preempted from initiating enforcement actions in this area; (2) Congress intended for the FTC's Section 5 "unfairness" authority to be limited and very narrow in scope, demonstrated by the fact that Congress has enacted many other specific statutes governing data security; and (3) the FTC had failed to publish guidelines or standards for data security practices that LabMD could follow and, as a result, the company did not have fair notice as to what a violation of Section 5 would entail.[6] *See* Petition for Review from the Fed. Trade Comm'n, *In the Matter of LabMD Inc.*, No. 16-16270, 2016 WL 7474626 (11th Cir. Dec. 27, 2016).

[7] *See* Order, *In the Matter of LabMD Inc.*, No. 16-16270 (11th Cir. Nov. 10, 2016).

[8] For example, a recent settlement involving mobile advertising company inMobi required the company to pay $950,000 in civil penalties and implement a new privacy program that will be independently audited for the next 20 years. *See* Press Release, Fed. Trade Comm'n, *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission* (June 22, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked. *See also* Press Release, Fed. Trade Comm'n, *ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk* (Feb. 23, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put; Press Release, Fed. Trade Comm'n, *FTC Approves Final Order In TRUSTe Privacy Case* (Mar. 18, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/03/ftc-approves-final-order-truste-privacy-case.

[9] Fed. Trade Comm'n, *Start with Security: A Guide for Business*, *Lessons Learned from FTC Cases* (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[10] Fed. Trade Comm'n, *Data Breach Response: A Guide for Business* (Sept. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business.

[11] Press Release, Fed. Trade Comm'n, *New FTC Website Helps Small Businesses Avoid Scams and Cyber Attacks* (May 19, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/05/new-ftc-website-helps-small-businesses-avoid-scams-cyber-attacks.

[12] 799 F.3d at 259.

[13] *Id.* at 256–57.

[14] Press Release, Fed. Trade Comm'n, *Joint Statement of Acting FTC Chairman Maureen K. Ohlhausen and FCC Chairman Ajit Pai on Protecting Americans' Online Privacy* (Mar. 1, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/03/joint-statement-acting-ftc-chairman-maureen-k-ohlhausen-fcc.

[15] 45 C.F.R. § 164.500 *et seq.*

[16] *Id.* § 164.504.

[17] *Id.* § 164.506.

[18] *Id.* § 164.508.

[19] *Id.* § 164.510.

[20] *Id.* § 164.512.

[21] *Id.* § 164.508.

[22] *Id.* § 164.512(i).

[23] *Id.* § 164.512(b).

[24] *Id.* § 164.504.

[25] *Id.* §§ 164.302–164.318.

[26] *Id.* § 164.308.

[27] *Id.* § 164.400, *et seq.*

[28] *Id.* §§ 164.404, 406, 408.

[29] *Id.* § 164.410.

[30] *Id.* § 164.402.

[31] *E.g.*, *id.* § 164.404(b).

[32] The settlements detailed below are only a sample of recent HHS OCR settlements and fines. Nine settlements have been reached between HHS and various covered entities in the first half of

2017 alone. A list of settlements can be accessed at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.

[33] Press Release, U.S. Dep't of Health and Human Servs., Office for Civil Rights, *$2.5 million settlement shows that not understanding HIPAA requirements creates risk* (Apr. 24, 2017), *available at* https://www.hhs.gov/about/news/2017/04/24/2-5-million-settlement-shows-not-understanding-hipaa-requirements-creates-risk.html.

[34] Press Release, U.S. Dep't of Health and Human Servs., *$5.5 million HIPAA settlement shines light on the importance of audit controls* (Feb. 16, 2017), *available at* https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html.

[35] Press Release, U.S. Dep't of Health and Human Servs., Office for Civil Rights, *Lack of timely action risks security and costs money* (Feb. 1, 2017), *available at* https://www.hhs.gov/about/news/2017/02/01/lack-timely-action-risks-security-and-costs-money.html.

[36] Press Release, U.S. Dep't of Health and Human Servs., Office for Civil Rights, *UMass settles potential HIPAA violations following malware infection* (Nov. 22, 2016), *available at* https://www.hhs.gov/about/news/2016/11/22/umass-settles-potential-hipaa-violations-following-malware-infection.html.

[37] *Id*.

[38] *Id*.

[39] Press Release, U.S. Dep't of Health and Human Servs., *Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million*, *available at* http://www.hhs.gov/about/news/2016/08/04/advocate-health-care-settles-potential-hipaa-penalties-555-million.html.

[40] Press Release, U.S. Dep't of Health and Human Servs., Office for Civil Rights, *$750,000 HIPAA settlement underscores the need for organization-wide risk analysis* (Dec. 14, 2015), *available at* https://www.hhs.gov/about/news/2015/12/14/750000-hipaa-settlement-underscores-need-for-organization-wide-risk-analysis.html?language=en.

[41] *Id*.

[42] *Id*.

[43] Lisa Lambert & Suzanne Barlyn, *SEC says cyber security biggest risk to financial system*, Reuters (May 18, 2016), *available at* http://www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4.

[44] *See OCIE's 2015 Cybersecurity Examination Initiative*, Nat'l Exam Program Risk Alert, Vol. IV, Issue 8 (Sept. 15, 2015), *available at* https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf; Carmen Germain, *SEC Poised to Turn Cybersecurity Focus Into*

Enforcement, Law360.com, July 7, 2017, *available at* https://www.law360.com/cybersecurity-privacy/articles/937197/sec-poised-to-turn-cybersecurity-focus-into-enforcement?nl_pk=daebfb21-b47a-48aa-a4f0-e78841e97f3a&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy.

[45] Jay Clayton, Chairman, Sec. and Exch. Comm'n, Remarks at the Economic Club of New York (July 12, 2017), *available at* https://www.sec.gov/news/speech/remarks-economic-club-new-york.

[46] Sec. and Exch. Comm'n, *CF Disclosure Guidance: Topic No. 2, Cybersecurity* (Oct. 13, 2011), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[47] *Id.*

[48] Comm'r Luis Aguilar, Sec. and Exch. Comm'n, *Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus* (June 10, 2014), *available at* https://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

[49] *Id*.

[50] *OCIE's Cybersecurity: Ransomware Alert*, Nat'l Exam Program Risk Alert, Vol. VI, Issue 4 (May 17, 2017), *available at* https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf.

[51] 17 C.F.R. § 248.30; *see also* Sec. and Exch. Comm'n, *Regulation S-P*, *available at* https://www.sec.gov/spotlight/regulation-s-p.htm.

[52] Teri Robinson, "R.T. Jones reaches settlement with SEC in data breach case," SC Magazine (Sept. 23, 2015), *available at* http://www.scmagazine.com/sec-hits-security-adviser-with-75000-penalty-in-breach-settlement/article/440268/.

[53] *See In re Craig Scott Capital*, Sec. Exch. Act Release No. 77595, Admin. Proceeding File No. 3-17206 (Apr. 12, 2016) (Order), *available at* https://www.sec.gov/litigation/admin/2016/34-77595.pdf.

[54] Press Release, Sec. and Exch. Comm'n, *SEC: Morgan Stanley Failed to Safeguard Customer Data* (June 8, 2016), *available at* https://www.sec.gov/news/pressrelease/2016-112.html.

[55] *See In re Morgan Stanley Smith Barney LLC*, Sec. Exch. Act Release No. 78021, Inv. Advisers Act Release No. 4415, Admin. Proceeding File No. 3-17280 (June 8, 2016), *available at* https://www.sec.gov/litigation/admin/2016/34-78021.pdf.

[56] *Id*. at 6.

[57] Andrew Ceresney, Dir., Sec. and Exch. Comm'n, *Compliance Outreach Program – 2016 National Seminar for Inv. Adviser and Inv. Co. Senior Officers*, Webcast (Apr. 19, 2016), *available at* https://www.sec.gov/video/webcast-archive-player.shtml?document_id=041916ccoia.

[58] James Scott & Drew Spaniel, *Assessing the FDA's Cybersecurity Guidelines for Medical Device Manufacturers: Why Subtle 'Suggestions' May Not Be Enough* 1 (2016), *available at* http://icitech.org/wp-content/uploads/2016/02/ICIT-Blog-FDA-Cyber-Security-Guidelines2.pdf.

[59] Food and Drug Admin., *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff* (Dec. 2016), *available at* https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.

[60] Food and Drug Admin., *Webinar – Postmarket Management of Cybersecurity in Medical Devices Final Guidance* (Jan. 12, 2017), *available at* https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm534592.htm.

[61] Food and Drug Admin., Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Guidance for Industry and Food and Drug Administration Staff; Availability, 79 Fed. Reg. 59,493 (Oct. 2, 2014), *available at* https://www.federalregister.gov/documents/2014/10/02/2014-23457/content-of-premarket-submissions-for-management-of-cybersecurity-in-medical-devices-guidance-for.

[62] Food and Drug Admin., Warning Letter to Abbott (St. Jude Medical Inc.) (Apr. 12, 2017), *available at* https://www.fda.gov/iceci/enforcementactions/warningletters/2017/ucm552687.htm.

[63] *See, e.g.*, 201 CMR 17.00 (promulgated under Mass. Gen. Law 93H) (establishing minimum data security standards for storing consumers' personal information); Nev. Rev. Stat. 603A.210 (same).

[64] *See, e.g.*, *California v. Kaiser Foundation Health Plan, Inc.,* No. RG14711370 (Cal. Sup. Ct., Alameda Co., Feb. 10, 2014) (Kaiser paid $150,000 to settle claims by the California Attorney General that Kaiser's notification regarding a breach of personal information was unreasonably delayed; according to the California Attorney General, Kaiser should have provided notice as soon as it determined that particular individuals' information had been or was "reasonably believed to have been" breached.).

[65] Rachel Abrams, *Target to Pay $18.5 Million to 47 States in Security Breach Settlement* (May 23, 2017), *available at* https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.

[66] Atty. Gen. Kamala D. Harris, *Cybersecurity in the Golden State: How California Businesses Can Protect Against and Respond to Malware, Data Breaches and Other Cyberincidents* (Feb. 2014), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/2014_cybersecurity_guide.pdf.

[67] On March 1, 2017, new cybersecurity regulations enforced by the New York State Department of Financial Services ("DFS") became effective. *See* http://www.dfs.ny.gov/about/cybersecurity.htm.

[68] *See* Charter of Fundamental Rights of the European Union art. 8, 2000 O.J. C 364/01, *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[69] *See* Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, 1995 O.J. L 281/31, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

[70] *See id.* at 47–48.

[71] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666 (July 24, 2000).

[72] *See* Case C-362/14, *Maximillian Schrems v. Data Prot. Comm'r*, 2015 E.C.R. I-1-35, *available at* https://cdt.org/files/2015/10/schrems.pdf.

[73] A complete overview of the requirements and benefits of the Framework is maintained at www.privacyshield.gov.

[74] *Queen's Speech: new data protection law*, BBC (June 21, 2017), *available at* http://www.bbc.com/news/technology-40353424.

[75] *China data protection tightened in new laws*, BBC (May 31, 2017), *available at* http://www.bbc.com/news/technology-40106826.

[76] Mike Orcutt, *Unprecedented Cyber Law Signals Its Intent to Protect a Precious Commodity: Data*, MIT Technology Review (June 1, 2017), *available at* https://www.technologyreview.com/s/608010/chinas-unprecedented-cyber-law-signals-its-intent-to-protect-a-precious-commodity-data/.

[77] Sophia Yan, *China's new cybersecurity law takes effect today, and many are confused*, CNBC (June 1, 2017), *available at* http://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html.

[78] *E.g.*, *Smith v. Triad of Ala., LLC*, 2017 WL 1044692 (M.D. Ala. Mar. 17, 2017) (discussing data breach that allegedly involved a maximum of 1,208 affected individuals); *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524, 527 (D. Md. 2016) (allegations based on purported disclosure of 18,000 patient records).

[79] *See* Order re Motion for Preliminary Approval of Class Settlement, *Corona v. Sony Pictures Entm't, Inc.*, No. 14-cv-09600 (C.D. Cal. Nov. 24, 2015); *see also* Ben Fritz, *Sony Pictures Settles Emp. Class Action Over Hack*, Wall St. J., Oct. 20, 2015, *available at* http://www.wsj.com/articles/sony-pictures-settles-employee-class-action-over-hack-1445369345.

[80] *See, e.g.*, *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 16-CV-00014, 2016 WL 6523428, at *12 (S.D. Cal. Nov. 3, 2016) (discussing allegations that defendant "did not take adequate security measures to protect the information they obtained, [] and that Defendants owed a duty to Plaintiff and class members to exercise reasonable care in [] securing, safeguarding, and protecting [] personal information" (internal quotations and citations omitted)); *see also In re Sony Gaming Networks*

& Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 963 (S.D. Cal. 2014) (discussing allegations that "Sony had a duty to provide reasonable security consistent with industry standards, to ensure Sony Online Services were secure, and to protect Plaintiffs' Personal Information from theft or misuse . . . . [and that] Sony breached this duty by failing to adequately secure its network").

[81] *See, e.g.*, *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617, 2013 WL 4759588, at *4 (N.D. Ill. Sept. 3, 2013) (dismissing invasion of privacy claim for lack of standing).

[82] *See, e.g.*, *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177–78 (D. Minn. 2014) (discussing theory of unjust enrichment in data breach cases).

[83] *See, e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 976, 990 (S.D. Cal. 2014) (granting in part and denying in part a motion to dismiss claim for negligent and fraudulent misrepresentations).

[84] 15 U.S.C. § 1681.

[85] 5 U.S.C. § 552a.

[86] 18 U.S.C. § 2702(a)(1).

[87] *See, e.g.*, *Holmes v. Countrywide Fin. Corp.*, No. 08-CV-00205, 2012 WL 2873892, at *15–17 (W.D. Ky. July 12, 2012) (granting motion to dismiss under FCRA where claims were not against a "consumer credit reporting agency"); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 28–34 (D.D.C. 2014) (granting motion to dismiss claims under the Privacy Act); *Worix v. MedAssets, Inc.*, 857 F. Supp. 2d 699, 701 (N.D. Ill. 2012) (granting motion to dismiss under Stored Communications Act).

[88] There are also a handful of federal statutes that plaintiffs use to litigate data privacy issues—separate from instances of data breaches. These statutes (e.g., the Wiretap Act or the Telephone Consumer Protection Act) most often focus on the collection or disclosure of communications.

[89] *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011) (denying motion to dismiss under Illinois Consumer Fraud Act).

[90] *See, e.g.*, 201 CMR 17.00 (Massachusetts' "Standards for the Protection of Personal Information of Residents of the Commonwealth").

[91] *See, e.g.*, Cal. Civ. Code §§ 1798.29, 1798.80 *et seq.*; N.Y. Gen. Bus. Law § 899-aa; N.Y. State Tech. Law § 208.

[92] *See, e.g.*, *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 690–91 (7th Cir. 2015) (discussing claims for "negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of multiple state data breach laws").

[93] *See, e.g.*, *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617, 2016 WL 3029783, at *39 (N.D. Cal. May 27, 2016) (discussing claims under state laws in New Jersey, New York, California, and Georgia).

[94] *See, e.g.*, *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1176–77 (discussing claims for breach of a credit card contract and "an implied contract in which Plaintiffs agreed to use their credit or debit cards to purchase goods at Target and Target agreed to safeguard Plaintiffs' personal and financial information").

[95] For example, companies have been subject to lawsuits by business partners, including financial institutions and other entities which suffered financial losses associated with a cyberattack on a business partner. This type of litigation has arisen most frequently against retailers when credit and debit cards have been compromised. *See, e.g.*, Consolidated Class Action Complaint, *In re Target Corp. Customer Data Sec. Breach Litig.*, No. 14-md- 02522 (D. Minn. Aug. 1, 2014) ECF No. 163.

[96] *See, e.g.*, Darlene Storm, *MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks*, Computerworld (June 8, 2015), *available at* http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medicaldevices-to-create-backdoors-in-hospital-networks.html.

[97] *In re Google, Inc. Privacy Policy Litig.*, No. 12-CV-01382, 2013 WL 6248499, at *4 (N.D. Cal. Dec. 3, 2013).

[98] 133 S. Ct. 1138, 1147 (2013).

[99] *Id.* at 1148.

[100] *Id.* at 1151.

[101] 136 S. Ct. 1540 (2016), *as revised* (May 24, 2016).

[102] *Id*. at 1543

[103] *Robins v. Spokeo, Inc.*, 742 F.3d 409, 413–14 (9th Cir. 2014) (emphasis in original).

[104] *Spokeo, Inc.*, 136 S. Ct. at 1548–50.

[105] *Id.* at 1548 (emphasis in original).

[106] *Id.*

[107] *Id.*

[108] *Id.* at 1549.

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] *See, e.g.*, *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 368 (M.D. Pa. 2015) (finding no standing where plaintiffs did not allege that they actually suffered any form of identity theft as a result of the defendant's data breach); *Green v. eBay Inc.*, No. 14-1688, 2015 WL 2066531, *1, *5 (E.D. La. May 4, 2015) (citing *Clapper* and finding threat of future harm stemming from disclosure of names, passwords, birthdates, email and physical addresses "far too hypothetical or speculative"); *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847, 850, 854 (S.D. Tex. 2015) (finding alleged future harm "speculative" where disclosed information included social security numbers, addresses, medical records and bank account information, and where fraudulent credit card purchase was declined); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 958–59 (D. Nev. 2015) (distinguishing cases within the Ninth Circuit that conferred standing based on increased risk of harm alone, and holding that increased risk of future harm was insufficient to confer standing given no evidence of personal data misuse in three-year period).

[114] *See, e.g.*, *Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, 2016 WL 4728027, at *3 (6th Cir. Sept. 12, 2016) (finding standing based on "a substantial risk of harm, coupled with reasonably incurred mitigation costs"); *Remijas*, 794 F.3d at 692 (finding standing based on allegations of, among other things, "lost time and money resolving [] fraudulent charges" and "protecting [] against future identity theft").

[115] *See, e.g.*, *Smith v. Ohio State Univ.*, No. 15-CV-3030, 2016 WL 3182675, at *4 (S.D. Ohio June 8, 2016) (finding no Article III standing under FCRA); *Gubala v. Time Warner Cable, Inc.*, No. 15-cv-1078, 2016 WL 3390415, at *5 (E.D. Wis. June 17, 2016) (finding plaintiff failed to allege a concrete harm where his suit was based on the defendant's failure to comply with the Cable Communications Policy Act); *Khan*, 188 F. Supp. 3d at 534 (finding plaintiff failed to connect the alleged statutory and common law violations to a concrete harm).

[116] *Aranda v. Caribbean Cruise Line, Inc.*, No. 12 C 4069, 2016 WL 4439935, at *6 (N.D. Ill. Aug. 23, 2016) (finding plaintiff's allegations of harm under the Telephone Consumer Protection Act were "concrete and particularized, traceable to defendants' conduct, and judicially redressable").

[117] *See Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1087 (E.D. Cal. 2015) (holding plaintiff had not "shown he has standing to bring actual identity theft, identity fraud and/or medical fraud claims"); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d at 19 ("[T]he mere loss of data—without evidence that it has been either viewed or misused—does not constitute an injury sufficient to confer standing.").

[118] Verified Shareholder Derivative Complaint for Breach of Fiduciary Duty, Waste of Corporate Assets, and Unjust Enrichment, *Palkon v. Holmes*, No. 14-cv-01234, 2014 WL 11071195 (D.N.J. May 2, 2014).

[119] *Palkon v. Holmes*, No. 14-cv-01234, 2014 WL 5341880, at *5–7 (D.N.J. Oct. 20, 2014).

[120] Target Corp. Report of the Special Litig. Comm., *Davis v. Steinhafel*, No. 14-cv-00203 (D. Minn. May 5, 2016), ECF No. 62-2.

[121] *Davis v. Steinhafel*, No. 14-cv-00203 (D. Minn. July 7, 2016), ECF No. 88.

[122] Opinion and Order at 11, *In re The Home Depot, Inc. S'holder Derivative Litig.*, No. 1:15-cv-2999-TWT (N.D. Ga. Nov. 30, 2016), ECF No. 62.

[123] *Id.* at 11–12.

[124] *Id.* at 13–14.

[125] *Id.* at 14.

[126] *Id.* at 14–18.

[127] *Id.* at 22.

[128] *Id.* at 30.

[129] Judgment at 1, *In re The Home Depot, Inc. S'holder Derivative Litig.*, No. 1:15-cv-2999-TWT (N.D. Ga. Nov. 30, 2016), ECF No. 63. Before plaintiffs appealed, the parties reached a settlement including $1,125,000 in attorneys' fees to plaintiffs. *See In re The Home Depot, Inc. S'holder Derivative Litig.*, No. 1:15-CV-2999, 2017 WL 1830055 (N.D. Ga. Apr. 28, 2017) (stipulation of settlement and release agreement).

[130] *See* Sec. & Exch. Comm'n, Div. of Corp. Fin., *CF Disclosure Guidance: Topic No. 2 - Cybersecurity* (Oct. 13, 2011), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[131] *See id.*

[132] *See* Complaint, *Madrack v. Yahoo! Inc.*, No. 5:17-cv-00373 (N.D. Cal. Jan. 24, 2017).

[133] *See, e.g.*, *In re Heartland Payment Sys., Inc. Sec. Litig.*, No. 09-1043, 2009 WL 4798148, at *2, *7 (D.N.J. Dec. 7, 2009) (granting motion to dismiss where plaintiffs alleged that "statements concerning the general state of security [] [we]re fraudulent because [company officers] were aware that Heartland had poor data security and had not remedied the problem"); *Avila v. LifeLock Inc.*, No. 15-01398, 2016 WL 4157358, at *7 (D. Ariz. Aug. 3, 2016) (granting motion to dismiss claims of misrepresentations concerning effectiveness of identity theft protection services and compliance with applicable payment card industry standards because plaintiffs failed to show that public statements regarding the company's data security practices were made with scienter).

[134] *In re Heartland Payment Sys.*, 2009 WL 4798148, at *5 (internal quotations omitted).

The following Gibson Dunn lawyers prepared this client update: Jennifer L. Conn, Ryan T. Bergsieker, Reid F. Rector and Danielle Serbin.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding the above developments. Please contact the Gibson Dunn lawyer with whom you usually work, or the following authors:

Jennifer L. Conn - New York (+1 212-351-4086, jconn@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)

Please also feel free to contact the following practice group leaders:

Alexander H. Southwell - Chair, Privacy, Cybersecurity and Consumer Protection Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Caroline Krass - Chair, National Security Practice, Washington, D.C. (+1 202-887-3784, ckrass@gibsondunn.com)
Daniel J. Thomasch - Co-Chair, Life Sciences Practice, New York (+1 212-351-3800, dthomasch@gibsondunn.com)
Tracey B. Davies - Co-Chair, Life Sciences Practice, Dallas (+1 214-698-3335, tdavies@gibsondunn.com)
Ryan A. Murr - Co-Chair, Life Sciences Practice, San Francisco (+1 415-393-8373, rmurr@gibsondunn.com)
Stephen C. Payne - Chair, FDA and Health Care Practice, Washington, D.C. (+1 202-887-3693, spayne@gibsondunn.com)