International Franchise Association
51st Annual Legal Symposium
May 6-8, 2018
Washington, DC

Data Security and Addressing the Risks in the Franchise System

JoAnn Carlton
Bank of America Merchant Services
Charlotte, North Carolina

Heather Enlow-Novitsky
Bank of America Merchant Services
Charlotte, North Carolina

Matthew Fore
Alexandria, Virginia

TABLE OF CONTENTS

Page

I. Introduction[1] [2]

The law and risk landscape regarding data security continues to rapidly evolve. The continued high-profile attention on cyber-attacks attracts intense media and public interest, as well as from a variety of government regulators. For all the attention, however, the legal landscape in the U.S. remains a mixture of federal, and state laws as well as industry expectations and contractual commitments. There is no national law regulating data security and breach notification for all sectors. Rather, the U.S. has a sectoral approach based on industry (such as specific laws targeting financial institutions or healthcare institutions), and a patchwork of federal and state laws that regulate data security. The following provides an overview of the federal, state and industry laws and frameworks that likely apply in the majority of industries involving franchised businesses.[3]

II. Laws, Regulations and Standards Governing Data Security

A. Federal - Section 5 of the FTC Act

The data security landscape at the federal level has been largely defined by the actions of the Federal Trade Commission ("FTC"). The FTC has been the most active agency in investigating data security incidents and bringing enforcement actions against companies as a result of those incidents. The FTC does not have a specific data security mandate or regulation pursuant to which it brings these actions; rather, the FTC brings actions under its general authority under Section 5 of the Federal Trade Commission Act ("FTC Act") to regulate unfair or deceptive trade practices.[4] Since 2005, the FTC has brought over 60 complaints and orders related to data security practices. The FTC has stated it expects companies to implement "reasonable" security, not "perfect security", and has offered guidance on what is reasonable.[5] The FTC complaints primarily allege that a data security incident occurred as a result of

---

[1] The views and opinions expressed in this paper do not necessarily reflect the position of all of the authors, contributors, or any company or law firm where any of the authors or contributors work.

[2] The authors want to recognize the contributions of Chris LaRocco, Esq., Vorys, Sater, Seymour and Pease LLP, whose significant time and efforts made this paper possible.

[3] This paper does not address data security requirements that primarily apply to financial institutions under the Gramm-Leach-Bliley Act ("GLBA"), or those that apply to healthcare institutions under the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH").

[4] 10 U.S.C. § 45 *et seq.*

[5] *See, e.g.,* Federal Trade Commission, "State With Security: A Guide for Businesses" (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

unreasonable security practices and, as a result, constituted an unfair or deceptive practice.

1) Unfairness

The FTC frequently brings data security actions under the unfairness prong of Section 5 of the FTC Act, charging that the lack of reasonable security measures constitutes an unfair trade practice. The FTC has a three factor test to determine whether a practice is unfair:

> [t]o justify a finding of unfairness the injury must satisfy three tests. [1] It must be substantial; [2] it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and [3] it must be an injury that consumers themselves could not reasonably have avoided.[6]

Examples of "unfair" data security practices that have resulted in FTC enforcement actions include: failing to encrypt data, failing to manage and secure vendor access to systems where data is maintained, and failing to change default vendor-supplied passwords.

2) Deception

The FTC may also bring actions under the deception prong of Section 5 of the FTC Act. An act or practice may be considered "deceptive" under Section 5 if there is a representation or omission of information that is likely to mislead the consumer acting reasonably under the circumstances, and if that representation or omission is "material." Something is "material" where that act or practice is "likely to affect the consumer's conduct or decision with regard to a product or service."[7] In order to bring an enforcement action charging deceptive practices, the FTC must first establish that the company has represented that they will adequately secure data or keep it confidential. The FTC can then allege that poor data security practices conflict with those representations, resulting in a deceptive practice in violation of Section 5.[8] Multiple enforcement actions by the FTC demonstrate that it will charge a company with deceptive practices where the company (1) fails to implement safeguards against commonly known hacking strategies; (2) publishes a website with clear security flaws

---

[6] 15 U.S.C. § 45(n).

[7] FTC Policy Statement on Deception, *appended* to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

[8] *See* Guess? Inc., No. 022-3260 (FTC Aug. 5, 2003); Life is Good, Inc., No. 072-3046 (FTC Apr. 18, 2008).

permitting unauthorized access to other users' information; or (3) makes statements to consumers with false information regarding nonexistent security measures.[9]

3) Data Security Guidance

In June of 2015, the FTC released "Start With Security: A Guide for Business" (the "Guide").[10] The Guide is intended to provide businesses with data security guidance, and summarizes lessons learned regarding data security from the FTC's enforcement actions up to that point. The Guide notes that "companies that consider security from the start assess their options and make reasonable choices based on the nature of their business and sensitivity of the information involved" and that while threats may evolve and change over time, "the fundamentals of sound security remain constant." The Guide breaks its security recommendations into 10 key areas:

1. Start with security, including not collecting personal information that isn't needed and retaining such information for only as long as there is a legitimate business need;
2. Control access to data sensibly, including restricting access to sensitive data and limiting administrative access;
3. Require secure passwords and authentication, including guarding against brute force attacks and protecting against authentication bypass;
4. Store sensitive personal information securely and protect it during transmission, such as using Transport Layer Security/Secure Sockets Layer (TLS/SSL), encryption, data-at-rest encryption, or an iterative cryptographic hash;
5. Segment your network and monitor who's trying to get in and out;
6. Secure remote access to your network, including ensuring endpoint security;
7. Apply sound security practices when developing new products, including verifying privacy and security features work properly and testing for common vulnerabilities;

[9] *See, e.g.,* Guess?, Inc., No. 022-3260 (FTC Aug. 5, 2003); Life is Good, Inc., No. 072-3046 (FTC Apr. 18, 2008); MTS Inc., No. 032-3209 (FTC June 2, 2004); Petco Animal Supplies, No. 032-3221 (FTC May 5, 2005).

[10] Federal Trade Commission, "Start With Security: A Guide for Businesses" (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

8. Ensuring your service providers implement reasonable security measures;

9. Implementing procedures to keep your security current and address vulnerabilities that may arise, including patching third-party software and moving quickly to fix credible security warnings; and

10. Securing paper, physical media, and devices.

While the Guide does not explicitly require companies to implement each recommendation, it does set forth the FTC's minimum security expectations. The FTC will likely evaluate whether a company's security was "reasonable" in part by reviewing whether these steps were evaluated and implemented in some form, and thus the Guide provides a good starting point for companies in evaluating whether their data security practices are "reasonable."

In the summer and fall of 2017, the FTC provided further guidance on what specific security measures it expects as part of a reasonable security program in its "Stick with Security" blog post series (the "Series"). Each post focuses on one of the Guide's security principles, and provides examples both from more recent FTC enforcement actions since the Guide was published, as well as day to day challenges the FTC has seen companies face.[11] The Series provides additional data security recommendations not present in the Guide, such as training staff on your company's data security standards and ensuring they are following through, and offering consumers more secure choices.[12] The Series is another useful tool in assisting companies in determining whether their data security practices are reasonable and therefore have a better chance of avoiding an enforcement action from the FTC in the event of a data security incident or breach.

4) Challenges to FTC Authority and Enforcement Actions

Although the FTC has long asserted its authority in the data security space, in recent years its jurisdiction under Section 5 of the FTC Act has been challenged. Between 2008-2009, several Wyndham branded hotels experienced three separate data breaches. After an investigation by the FTC and failing to resolve or settle the FTC's investigation, the FTC sued the hospitality company and three subsidiaries in 2012, alleging that data security failures led to the three data breaches at Wyndham hotels.[13] According to the FTC's complaint, hackers infiltrated the network of a Wyndham franchisee and then exploited lax security on Wyndham's corporate network

[11] FTC, "Stick With Security" (July 21, 2017), *available at*: https://www.ftc.gov/news-events/blogs/business-blog/2017/07/stick-security-insights-ftc-investigations.
[12] FTC, "Start with security – and stick with it," (July 28, 2017), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2017/07/start-security-stick-it.
[13] FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (11th Cir. 2015).

to grab sensitive consumer data from dozens of other Wyndham franchisees. Those breaches resulted in the transfer of account data about hundreds of thousands of consumers to a website registered in Russia and $10.6 million in fraudulent charges on consumers' credit and debit cards. In 2014, a federal District Court in New Jersey denied Wyndham's motion to dismiss the FTC action.[14] The Third Circuit agreed to hear an immediate appeal on two issues: "whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision."[15] The Third Circuit upheld the District Court's ruling that the FTC could use the prohibition on unfair practices in Section 5 of the FTC Act to challenge the alleged data security lapses outlined in the complaint. The Court also rejected Wyndham's fair notice argument.[16] After the Third Circuit's decision, the parties agreed to settle the case.[17]

Despite the FTC's victory in the Third Circuit, its authority was again challenged by LabMD. The parties' long-running dispute dates to 2013, when LabMD became the second company, after Wyndham Worldwide Corp., to push back rather than settle the Commission's data security allegations.[18] LabMD appealed the FTC's decision to the Eleventh Circuit following a July 2016 opinion by the FTC commissioners that overturned their own administrative law judge's dismissal of the case. In the July 2016 decision, the FTC concluded that the lab's failure to employ "basic" security precautions led to the unauthorized disclosure of personal data belonging to approximately 9,300 patients that constituted the type of "substantial" injury necessary to support a Section 5 claim. The FTC also ordered LabMD to take steps to notify affected consumers and establish a comprehensive information security program. LabMD has argued that no actual harm to consumers occurred from the alleged lax data security practices, and that the 2016 FTC opinion was unduly burdensome as LabMD had ceased operating as a business. In June 2017, oral arguments were presented to the Eleventh Circuit. The appeals court questioned the FTC on numerous issues, including its view on how far the FTC's enforcement authority might extend. The FTC responded that it can proceed on a case-by-case basis and that companies have a duty to act reasonably under the circumstances. However, the court criticized this approach, stating that an unclear standard of "reasonableness," determined by the Commissioners, isn't "good public policy."[19] Despite this exchange, no decision has been issued.[20]

---

[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] FTC v. Wyndham Worldwide Corp., Stipulated Order for Injunction, a*vailable at* https://www.ftc.gov/system/files/documents/cases/151211wyndhamstip.pdf.
[18] LabMD Inc. v. Federal Trade Commission, case number 16-16270, in the U.S. Court of Appeals for the Eleventh Circuit.
[19] Oral Argument Recordings, LabMD, Inc., Petitioner v. Federal Trade Commission, June 21, 2017, *available at http://www.ca11.uscourts.gov/oral-argument-recordings?title=&field_oar_case_name_value=labmd&field_oral_argument_date_value*

Finally, in a third case against the FTC, while the defendant did not challenge the FTC's jurisdiction generally, it did successfully challenge the FTC's enforcement action in determining whether the data security practices at issue were unfair. In September 2017, a California court found that the FTC did not adequately plead that the defendant, D-Link, engaged in unfair practices.[21] The complaint alleged that D-Link failed to take reasonable steps to secure its routers and internet protocol cameras despite promoting its products as "easy to secure" and having "advanced network security," or supporting "the latest wireless security features to help prevent unauthorized access, be it from a wireless network or from the Internet."[22]

In contrast to Wyndham and other enforcement actions, the FTC in the matter against D-Link failed to identify "a single incident where a consumer's financial, medical or other sensitive personal information has been accessed, exposed or misused in any way, or whose IP camera has been compromised by unauthorized parties, or who has suffered any harm or even simple annoyance and inconvenience from the alleged security flaws in the [D-Link's] devices," Judge Donato wrote.[23]

In dismissing the FTC's unfairness claim in this case, the D-Link court held "[t]he absence of any concrete facts makes it just as possible that [D-Link's] devices are not likely to substantially harm consumers, and the FTC cannot rely on wholly conclusory allegations about potential injury to tilt the balance in its favor," adding that the "lack of facts indicating a likelihood of harm is all the more striking in that the FTC says that it undertook a thorough investigation before filing the complaint, and that the DLS devices have had the challenged security flaws since 2011."[24] Despite the successful challenge to the FTC's unfairness claims, the FTC's deception claims survived, and the litigation is ongoing.

Despite these challenges to the FTC and its authority, or particular claims brought by the FTC, at this point the FTC is the primary federal regulator in the data security space and has not signaled any intention to cede that position to other regulators. Companies should consider FTC data security guidance in evaluating their information security programs and practices and be prepared for an inquiry from the FTC in the event of a large data breach.

%5Bvalue%5D%5Byear%5D=&field_oral_argument_date_value%5Bvalue%5D%5Bmonth%5D=.

[20] No decision has been issued by the Eleventh Circuit as of April 16, 2018.

[21] Federal Trade Commission v. D-Link Systems, Inc., No. 3:17-cv-00039-JD (N.D. Cal. Sept. 19, 2017).

[22] *Id.*

[23] *Id.*

[24] *Id.*

B. Other Federal Regulators Cybersecurity Initiatives and Enforcement

While the FTC remains the primary federal regulator in the cyber security space for non-regulated entities, both the Securities and Exchange Commission ("SEC") and the Consumer Financial Protection Bureau ("CFPB") have signaled increasing interest and authority in this space. In 2011, the SEC issued cybersecurity disclosure guidance to publicly-traded companies,[25] and recently updated this guidance in February of 2018.[26] Stating that "in light of the increasing significance of cybersecurity incidents" additional guidance has become necessary, the SEC emphasizes the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents, noting that "[c]ompanies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity."[27]

The SEC guidance highlights the need for cybersecurity disclosures based on current reporting obligations and the materiality standard, identifies specific cybersecurity risk factors, and emphasizes the adoption by public companies of appropriate policies and procedures to address cybersecurity matters and to enforce insider trading prohibitions. The guidance also makes clear that companies "have a duty to correct" disclosures that are determined later to have been untrue when originally made and may have "a duty to update" disclosures that were correct when made based on later material information, such as when reasonable investors are still relying on such disclosure. In particular, "[c]ompanies should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident."[28]

The SEC also highlighted the need for companies to abide by insider trading prohibitions as it related to cyber security risk. The SEC expects companies to take steps to prevent directors and officers and other corporate insiders who were aware of these cyber incident or risk matters from trading its securities until investors have been appropriately informed about the incident or risk. The SEC emphasizes the role of "well designed policies and procedures to prevent trading on the basis of all types of material nonpublic information, including information related to cybersecurity risks and incidents." Within a few weeks of announcing the guidance in February 2018, the SEC brought its first insider action charges in connection with a data breach against the Equifax Chief Information Officer.

---

[25] Div. of Corp. Fin., SEC, CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[26] Div. of Corp. Fin., SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[27] *Id.*

[28] *Id.*

In addition to disclosure guidance, the SEC has ramped up activity in connection with cybersecurity incidents in recent years. The SEC has announced investigations into Target and Home Depot as a result of their large breaches in recent years, but there been no official action taken. Last fall, the SEC announced the creation of the Cyber Unit in its Enforcement Division, which will target cyber-related misconduct, which brought its first case in December, 2017.

The CFPB has also made moves to regulate covered entities[29] regarding their cybersecurity. In March of 2016, the Consumer Financial Protection Bureau (CFPB) announced a $100,000 penalty and settlement with online payment processor Dwolla, Inc. (Dwolla) for weak data security practices.[30] Although Dwolla had not suffered a data breach, the CFPB found that Dwolla falsely advertised that customers' personal information was "safe" and "secure."[31] This was the CFPB's first action against a company for data security practices.

The action by the CFPB is consistent with and indicative of the overall regulatory focus on cybersecurity controls for many institutions. However, given the recent changes to the leadership of the CFPB under the Trump administration, which has indicated its disfavor for active regulatory and enforcement actions by the CFPB, it is uncertain whether this is a line of enforcement that the CFPB will continue to pursue.

C. State Laws

1) Data Security Laws

Unlike at the federal level, at least 17 states have explicit data security laws that generally require businesses that have access to, or store, personal information to have "reasonable security procedures and practices appropriate to the nature of the information."[32] In addition to general data security laws, many states have laws that impose certain restrictions on the use or requirement of certain data elements such as

---

[29] The CFPB regulates banks, thrifts and credit unions with assets over $10 billion and their affiliates. They also regulate nonbank mortgage originators and servicers, payday lenders, and private student lenders. Finally, the CFPB regulates "larger participants of other consumer financial markets" as defined by CFPB rules; this currently includes larger participants in the consumer reporting, consumer debt collection, student loan servicing, international money transfer and automobile financing markets. CFPB, "Institutions subject to CFPB supervisory authority," https://www.consumerfinance.gov/policy-compliance/guidance/supervision-examinations/institutions/ (last visited Apr. 21, 2018).

[30] *In the Matter of Dwolla, Inc.* CFPB, No. 2016-CFPB-0007, Consent Order (Mar. 2, 2016), *available at* https://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf.

[31] *Id.*

[32] R.I. Gen. Laws § 11-49.3-2; *see, e.g.,* Ark. Code §§ 4-110-104(b), Cal Civ. Code § 1798.81.5, Ind. Code § 24-4.9-3-3.5.

social security numbers,[33] or prohibit the collection of certain personal data in connection with a payment card transaction.[34] The most specific of these are the Massachusetts Data Security regulations,[35] which require businesses that own or license personal information of a Massachusetts resident to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information."[36] The regulation further requires designation of one or more employees to maintain the information security program; identifying and assessing foreseeable risks to personal information and evaluating and improving safeguards in place to limit such risks; and preventing terminated employees from accessing records containing personal information.[37]

2) Breach Notification Laws

In addition to state data security laws, all states, the District of Columbia, and Puerto Rico have enacted data breach notification laws that require notification to affected individuals or entities in certain circumstances relating to a data breach.[38] These laws are primarily designed to help prevent identity theft and protect Personally Identifiable Information (PII). PII typically is defined as an individual's name plus an additional data element, such as social security number, driver's license number, or financial account number. Many states also include a username and password, health information, and biometrics information in the definition of PII.

In addition to varying definitions of "PII" among the state laws, the state laws vary as to whether all data breaches involving PII must be disclosed or only those where there is a material risk of harm or identity theft to individuals; how quickly notification must occur, such as soon as reasonably practicable or within a specified time period such as 30 days; whether other entities must be notified such as consumer reporting agencies, state attorneys general or Divisions of Taxation, and how many residents must be impacted to trigger such notification; content requirements for notification

[33] *See. e.g.*, Alaska Stat. § 45.48.410; Kan. Stat. Ann. § 75-3520; Me. Rev. Stat. tit. 10, § 1272-B.
[34] *See, e.g.,* Cal. Civ. Code § 1747, *et seq.,* Del. Code Ann., tit. 11, § 914; M.G.L. ch.93, § 105.
[35] 201 CMR 17.00, *et seq.*
[36] 201 CMR 17.03(1).
[37] 201 CMR 17.03(2).
[38] Alabama's law goes into effect on May 1, 2018 and South Dakota's is effective July 2, 2018.

letters; and penalties, such as statutory damages and penalties.[39] These laws continue to be amended frequently as large scale breaches continue to occur, and require careful review during incident response planning and in the event of notification.

3) State AG enforcement - Individual and Multi-State

The data breach notification laws, as well as the state "mini-FTC" acts, have allowed state attorneys general to investigate and bring enforcement actions after cybersecurity incidents or data breaches. The state attorneys general have brought these actions both on an individual basis pursuant to their respective state's laws and, more recently, state attorneys general have acted together to investigate cybersecurity incidents and breaches as a joint action. In the past two years, attorney general offices have entered into multistate data breach settlements ("assurances of voluntary compliance") with Ashley Madison, Nationwide Insurance, Target Corporation, and Adobe.[40] In the largest of these, Target agreed to pay $18.5 million to 47 state attorneys general for failure to safeguard customer data.[41] Multistate enforcement trends continue, and in September of 2017, 34 attorneys general initiated an inquiry into Equifax as a result of its large data breach announced in August.[42]

---

[39] *See e.g.*, Mass. Gen Law 93H § 1 et seq. (Massachusetts); Ariz. Rev. State. § 18-545 (Arizona); 815 ILCS §§ 5301/1 to 530/25 (Illinois); La. Rev. State. §§ 51:3071 et seq. (Louisiana).

[40] *See* "A.G. Schneiderman Announces $17.5 Million Settlement with Owner of Ashleymadison.com In Joint Multi-State And FTC Agreement," (Dec. 14, 2016), *available at* https://ag.ny.gov/press-release/ag-schneiderman-announces-175-million-settlement-owner-ashleymadisoncom-joint-multi; "Attorney General Fox Announces Settlement with Nationwide Mutual Insurance Company Over Data Breach." (Aug. 10, 2017), *available at* https://dojmt.gov/attorney-general-fox-announces-settlement-nationwide-mutual-insurance-company-data-breach/; "Target Settles with Iowa and 46 States Over Massive 2013 Data Breach," (May 23, 2017), *available at* https://www.iowaattorneygeneral.gov/newsroom/target-settles-with-iowa-and-46-states-over-massive-2013-data-breach/; "Adobe to Pay $1 Million, Update Security Policies to Resolve Multistate Investigation Into Data Breach," (Nov. 15, 2016), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2016/adobe-to-pay-1-million-update-security.html.

[41] http://www.ag.state.il.us/pressroom/2017_05/17-AVC-0008TargetCorporation.pdf.

[42] https://law.georgia.gov/sites/law.georgia.gov/files/related_files/press_release/Equifax.Letter%20to%20Counsel.9-15-17.pdf. In addition, Massachusetts has already sued Equifax in connection with its breach, alleging violations of the Massachusetts Consumer Protection Act (G.L. c. 93A) and the Massachusetts Data Security Law (G.L. c. 93H). *See Commonwealth of Massachusetts v. Equifax Inc.*, Complaint, (Super. Ct. Mass. Sept. 19, 2017), available here: http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-09-19-equifax-lawsuit.html. On April 4, 2018, the court denied Equifax's motion to dismiss the action and the lawsuit could proceed.

A review of the recent assurances of voluntary compliance sheds some light onto the data security measures and controls that state attorneys general expect. Each settlement requires implementation of a comprehensive security program, and the program must assess risks, mitigate risks, and update the program based on the identified risks and mitigation controls. Vendor management is also a key part of the required information security programs, as the assurances of voluntary compliance also require contracts with vendors to require implementation and maintenance of appropriate safeguards, and policies and procedures to audit such service providers' compliance with the contractual safeguards. The assurances of voluntary compliance also require specific security measures such as: compliance with the Payment Card Industry Data Security Standard; annual employee training on the information security program; assigning priority levels and schedules for updates and patches; regularly reviewing and updating incident response policies; checking for common vulnerabilities or exposures; segmenting the cardholder data environment from other parts of the networks; develop and implement a risk-based penetration testing program; integration of two-factor authentication; logging and monitoring; encryption of payment card information throughout the course of the transaction and adoption of industry-accepted payment card technology like chip and PIN.[43]

In addition to FTC guidance, data security settlements with state attorneys general provide helpful guidance in determining what regulators expect from information security programs and specific security measures and controls. The state attorneys general have increased their activity in investigating and bringing enforcement actions against companies that have suffered data breaches, and have even had more success in leveraging fines than the FTC. Thus, companies should expect state attorneys general to remain active in this space. [44]

---

[43] *See* "A.G. Schneiderman Announces $17.5 Million Settlement with Owner of Ashleymadison.com In Joint Multi-State And FTC Agreement," (Dec. 14, 2016), *available at* https://ag.ny.gov/press-release/ag-schneiderman-announces-175-million-settlement-owner-ashleymadisoncom-joint-multi; "Attorney General Fox Announces Settlement with Nationwide Mutual Insurance Company Over Data Breach." (Aug. 10, 2017), *available at* https://dojmt.gov/attorney-general-fox-announces-settlement-nationwide-mutual-insurance-company-data-breach/; "Target Settles with Iowa and 46 States Over Massive 2013 Data Breach," (May 23, 2017), *available at* https://www.iowaattorneygeneral.gov/newsroom/target-settles-with-iowa-and-46-states-over-massive-2013-data-breach/; "Adobe to Pay $1 Million, Update Security Policies to Resolve Multistate Investigation Into Data Breach," (Nov. 15, 2016), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2016/adobe-to-pay-1-million-update-security.html.

[44] Companies who have international exposure also will need to consider emerging international standards affecting data security, including the General Data Protection Regulation ("GDPR").

D. Industry Standards

In addition to federal and state obligations, companies accepting payment cards for payment are contractually required to comply with the Payment Card Industry Data Security Standard ("PCI-DSS").[45] Companies may also choose or be contractually bound to comply with other cyber security frameworks, such as the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework, or those promulgated by the International Organization for Standardization ("ISO").

1) PCI-DSS

The PCI-DSS is a cybersecurity framework consisting of twelve primary components promulgated by the Payment Card Industry Security Standards Council ("PCI SSC"). Formed in 2006, PCI SSC was founded by American Express, Discover, JCB International, MasterCard and Visa Inc. to help protect payment card data and transactions. While the PCI SSC has no direct method of enforcing PCI-DSS, the card brands have incorporated compliance with PCI-DSS (including other standards like the Payment Application Data Security Standard ("PA-DSS")) into their operating regulations. PCI-DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational practices for system components included in or connected to environments with cardholder data. Ongoing compliance with PCI-DSS consists of three primary steps: (1) assess, which included identifying all locations of cardholder data and analyzing the payment card processing environment for vulnerabilities; (2) repair, which includes fixing identified vulnerabilities and implementing secure business processes; and (3) report, including documenting assessment and remediation details and submitting compliance reports to the applicable acquiring bank. The twelve requirements of PCI-DSS are:

Install and maintain a firewall configuration to protect cardholder data;

1. Do not use vendor supplied defaults for system passwords and other security parameters;
2. Protect stored cardholder data;
3. Encrypt transmission of cardholder data across open, public networks;
4. Protect all systems against malware and regularly update anti-virus software or programs;
5. Develop and maintain secure systems and applications;
6. Restrict access to cardholder data by business need to know;
7. Identify and authenticate access to system components;
8. Restrict physical access to cardholder data;

[45] Note that a few states have incorporated compliance with PCI DSS as evidence of proper data security or an affirmative defense to claims. *See, e.g.,* Minn. St. § 325E.64; Nev. Rev. Stat. Ch. 603A.

9. Track and monitor all access to network resources and cardholder data;
10. Regularly test security systems and processes; and
11. Maintain a policy that addresses information security for all personnel.[46]

2) NIST Framework and ISO Standards

Although not legally required for a majority of companies,[47] compliance with the National Institute of Standards and Technology's Cybersecurity Framework ("Framework") is encouraged and frequently viewed as a helpful standard by information security professionals. This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security. Compliance with the Framework may be one standard that vendors will agree to in lieu of your company's information security program.

The Framework focuses on five concurrent and independent functions that are characteristic of an effective cybersecurity program. These functions are:

1. Identify – the capacity to identify and understand organizational cyber risks;
2. Protect – the development and implementation of appropriate safeguards;
3. Detect – the activities and capabilities to detect cybersecurity intrusions and attempted intrusions;
4. Respond – the capability to react and respond to a detected cybersecurity incident; and
5. Recover – the activity of planning for resiliency and the capability to maintain or restore services that are impaired by a cybersecurity incident.[48]

A final industry framework that is helpful, although again not necessarily legally required, is the ISO/IEC 27000 standards. ISO is an international standard-setting body composed of representatives from various national standards organizations. The

---

[46] PCI DSS v. 3.2 (Apr. 2016), *available at* https://www.pcisecuritystandards.org/document_library.

[47] "Critical Infrastructure" must follow the Framework. *See* Exec. Order No. 13,636, 78 Fed. Red. 11,739 (Feb. 12, 2013), https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. "Critical infrastructure" includes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

[48] *Id.*

ISO/International Electrotechnical Commission (IEC) 27000 family of standards helps organizations keep information assets secure. Using this family of standards seeks to help organizations manage the security of assets and data. This may be another framework that vendors and other organizations use to measure and audit their information security program compliance, in lieu of an organization's information security program.

III. Data Breach Litigation Overview

This section provides a general overview of the landscape of data breach litigation, including the hurdles which potential private party plaintiffs face in bringing data breach lawsuits and the most common types of lawsuits surrounding data breaches.

Data breach lawsuits come in a wide variety of forms in both federal and state courts. The most prevalent data breach lawsuits filed by consumer breach victims allege breach of contract, negligence, and breach of fiduciary duty. These cases are frequently brought as class actions. The viability of any of these causes of action in the data breach context often hinges on whether an individual has standing (i.e. whether a plaintiff can bring a lawsuit as a result of a data breach). Standing in the data breach context is currently an evolving topic as the federal circuit courts are split on whether a plaintiff has suffered an injury merely by having his or her data accessed, or potentially accessed, by unknown parties. The U.S. Supreme Court has yet to resolve this split among the circuit courts and has thus far rejected the opportunity to do so.[49] In general, common law causes of action by consumers against companies that have suffered data breaches have not had significant success.

A. When Can a Consumer Plaintiff Bring a Private Cause of Action ?

The initial hurdle in any data breach lawsuit so far has been the issue of standing. "Standing" is defined as a party's right to make a legal claim or seek judicial enforcement of a duty or right. Standing is a preliminary inquiry in all legal claims.[50] The question of standing depends upon whether the party has alleged such a personal stake in the outcome of the controversy as to ensure that the dispute sought to be adjudicated will be presented in an adversary context and in a form historically viewed as capable of judicial resolution.

---

[49] *See CareFirst, Inc. v. Attias*, No. 17-641, 2017 WL 5041488 (U.S. Oct. 30, 2017). In February, 2018, the U.S. Supreme Court denied a petition for writ to resolve this issue permitting a data breach class action to proceed against a medical insurer.

[50] *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990); *Allen v. Wright*, 468 U.S. 737, 751 (1984). The standing requirement is not only federal, but is also required in all states. *See e.g.*, *State ex rel. Jones v. Suster*, 84 Ohio St.3d 70, 77 (1998) ("Standing is a threshold question for the court to decide in order for it to proceed to adjudicate the action.").

For a case to be heard in federal court, the lawsuit must comply with Article III of the United States Constitution. Article III requires that there be an actual "case or controversy" between the parties. A "case or controversy" requires that there be an injury-in-fact that is actual or imminent, not conjectural or hypothetical.[51] Further, "[t]o satisfy the case or controversy requirement a plaintiff must establish three elements: '(1) an injury-in-fact that is concrete and particularized; (2) a connection between the injury and the conduct at issue; (3) the injury must be fairly traceable to the defendant's action; and (4) [a] likelihood that the injury would be redressed by a favorable decision by the Court.'"[52]

1) "Injury In Fact"

The first prong of the Article III test for standing is that a plaintiff must suffer an injury that is concrete, particularized, and actual or imminent - an injury in fact. The injury in fact prong has proved a difficult hurdle in data breach lawsuits and the Supreme Court has yet to directly address what constitutes an injury in fact in the data breach context, particularly where only an increased risk of future risk of harm is alleged. However, until recently, lower courts have largely relied upon *Clapper v. Amnesty International USA* for guidance.[53] In *Clapper*, a group of international human rights organizations argued that there was a significant likelihood that the Foreign Intelligence Surveillance Act would cause some of their confidential communications to be monitored at some future date.[54] Based on the fact that there was no evidence that their communications had been targeted, or that they were going to be targeted, the Court found that plaintiffs' theory of future injury was too speculative and not actual or impending.[55] Further, plaintiffs' alleged injury of having "to take costly measures to protect their confidentiality of their . . . communications" did not constitute standing because plaintiffs should not be able to "manufacture standing by incurring costs in anticipation of non-imminent harm."[56]

Courts have used *Clapper* to dismiss data breach actions for failing to show a recognizable injury.[57] Typically, courts addressing data breach cases post-*Clapper*

---

[51] *See, e.g*., *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1544 (2016); *Friends of the Earth, Inc. v. Laidlaw Envtl Servs., Inc.*, 528 U.S. 167, 180-81 (2000).

[52] *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010); *Key v. DSW, Inc.*, 454 F. Supp.2d 684 (S.D. Ohio 2006). The test for federal constitutional standing (Article III standing) is, in all relevant respects, the same as the various states' test for standing. "By now, it is axiomatic that a litigant demonstrates Article III standing by tracing a concrete and particularized injury to the defendant--whether actual or imminent--and establishing that a favorable judgment would provide redress." *Morrison v. Bd. of Educ.*, 521 F.3d 602, 608 (6th Cir. 2008).

[53] 133 S. Ct. 1138, 1143-45 (2013).

[54] *Id.*

[55] *Id.* at 1147.

[56] *Id.* at 1155.

[57] *See e.g., Whalen v. Michael Stores*, 2015 U.S. Dist. LEXIS 172152 (E.D.N.Y. 2015).

have required allegations of actual identity theft or fraud to establish an injury.[58] To this end, plaintiffs seeking standing in data breach lawsuits typically allege that increased risk of identity theft or fraud and costs protecting against the same, constitute injury. In 2016, the Supreme Court further expanded on the *Clapper* test, stating that a plaintiff must allege an "injury-in-fact" that is both "concrete" and "particularized".[59]

With respect to the increased risk of future identity theft serving as an injury in fact, courts are split.[60] The D.C., Sixth, Seventh, and Ninth Circuits have all recognized that a plaintiff can establish injury in fact based on the threatened injury of identity theft.[61] Other circuit courts, however, have held that plaintiffs, in order to have standing to sue, must demonstrate that their personal information was not only accessed in a data breach, but was actually misused as a result (e.g., a fraudulent line of credit being taken out in the victim's name).[62] The First, Second, Third, Fourth and Eighth Circuits sit

---

[58] *See e.g., In re Zappos.com, Inc.*, 108 F. Supp.3d 949, 955 (D. Nev. 2015).

[59] *Spokeo Inc. v. Robins,* 136 S. Ct. 1540 (2016).

[60] *See Beck v. McDonald*, 848 F.3d 262, 273 (4th Cir. 2017) (identifying the deep current circuit split).

[61] *See Attias v. CareFirst, Inc*., 865 F.3d 620, 629 (D.C. Cir. 2017) (concluding that "simply by virtue of the hack and the nature of the data" alleged to be taken, substantial risk of injury to plaintiffs existed, even though no proof of actual misuse had yet been shown); *Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed. Appx. 384 (6th Cir. 2016) ("[T]here is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals"); *Remijas v. Neiman Marcus Grp., LLC*, 794 F. 3d 688, 692-95 (7th Cir. 2015) (finding injury in fact where hackers attacked Neiman Marcus with malware to steal credit card numbers because "presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."); *Lewert v. P.F. Chang's China Bistro, Inc*., 819 F.3d 963, 967 (7th Cir. 2016) (holding that standing existed where credit card information was stolen and plaintiffs incurred charges to mitigate potential effects of breach); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 632-34 (7th Cir. 2007) (banking services applicants' increased risk of harm theory satisfied Article III injury-in-fact requirement after "sophisticated, intentional and malicious" security breach of bank website compromised their information); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142-43 (9th Cir. 2010) (finding injury in fact where laptop containing unencrypted employee information was stolen which court found to be a "credible threat of harm.")

[62] *See Katz v. Pershing*, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (plaintiff's increased risk of unauthorized access and identity theft theory insufficient to constitute "actual or impending injury" after defendant failed to properly maintain an electronic platform containing her account information, because plaintiff failed to "identify any incident in which her data has ever been accessed by an unauthorized person"); *Whalen v. Michaels Stores, Inc*., 689 Fed. App'x 89, 90 (2d Cir. 2017) (rejecting standing where stolen credit card was promptly cancelled after the breach and no other personally identifying information was alleged to be stolen); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40, 44 (3d Cir. 2011) (plaintiffs' increased risk of identity theft theory too hypothetical and speculative to establish "certainly impending" injury-in-fact after unknown hacker

on this side of the split. In February of 2018, the U.S. Supreme Court had an opportunity to resolve this split in *CareFirst, Inc. v. Attias,* No. 17-641, 2017 WL 5041488 (U.S. Oct. 30, 2017). However, the Court denied a petition for certiorari and as a result ensured that lower courts will continue to struggle with the *Clapper* decision in the data breach context.

Until further intervention, plaintiffs in the D.C., Sixth, Seventh, and Ninth Circuits will likely establish the injury in fact prong of a standing analysis merely by having their personal information breached, while plaintiffs in at least the First, Second, Third, Fourth and Eighth Circuits will not and must allege additional, concrete injuries such as fraudulent charges, bank fees or payment of identity theft monitoring services.

2) Another Avenue to Establish Standing – Statutory Standing

As referenced above in Section II.C.2. above, all states, D.C., and Puerto Rico have data breach notification laws. Some of these state-specific laws provide affected individuals with a private right of action and, thus, the plaintiffs have "statutory standing" to sue.[63] Additionally, where there has been an alleged violation of federal law, data breach plaintiffs often attempt to satisfy Article III standing by alleging statutory standing (e.g., alleged Fair Credit Reporting Act ("FCRA") violations). Statutory standing means that a violation of the statute itself grants the plaintiff an independent cause of action pursuant to that statute.

In *Spokeo Inc. v. Robins*, the Supreme Court held that evidence of a statutory violation alone will not automatically satisfy Article III's injury requirement.[64] Despite the Court's ruling in *Spokeo*, federal appeals courts have since found statutory violations

---

infiltrated payroll system, because it was "not known whether the hacker read, copied, or understood" the system's information.); *Whalen,* 689 Fed. App'x at 90 (2d Cir. 2017) (rejecting standing where stolen credit card was promptly cancelled after the breach and no other personally identifying information was alleged to be stolen); *In re SuperValu, Inc.*, 870 F.3d 763, 769-72 (8th Cir. 2017) (holding that the existence of a data breach—by itself—was insufficient to establish standing, even though payment card information was accessed and one plaintiff faced a fraudulent charge but did not suffer a loss from it).

[63] Note that Tennessee, Louisiana, Alaska, California, Maryland, Massachusetts, New Hampshire, North Carolina, Oregon, South Carolina, and the District of Columbia are the jurisdictions which currently allow a private right of action for violation of their respective data breach laws.

[64] 136 S. Ct. 1540, 1549 ("Congress' role in identifying and elevating intangible harms 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. Article III standing requires a concrete injury even in the context of a statutory violation. For that reason, 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.").

sufficient to constitute injury for Article III standing.[65] In *In re Horizon Healthcare*, the plaintiffs alleged a violation of the FCRA where computers containing customers' personal information were stolen from a health insurer.[66] The Third Circuit found that "a violation of FCRA gives rise to injury sufficient for Article III standing."[67]

Despite *Spokeo*, there remains confusion over whether plaintiffs have statutory standing to sue where they have only suffered a bare statutory violation (e.g., failure to timely notify a data breach victim). In jurisdictions which provide for a private right of action, this means that a bare violation of the data breach law could arm plaintiffs with standing to sue. In states without a private right of action, this risk is somewhat lessened given that statutory standing could only apply if there is an alleged violation of federal law (e.g., FCRA) and not simply a failure to follow the state data breach notification law.

B. What are the Types of Common Law Legal Claims Brought by Consumer Victims of a Data Breach?

1) Breach of Contract

Assuming plaintiffs pass the standing hurdle, the most prevalent cause of action in consumer data breach litigation is a breach of contract claim. Parties bring contract claims based on either express or implied contracts, but the standard for breach of such contracts requires the same analysis. The essential elements of a cause of action to recover damages for breach of contract are the existence of a contract, the plaintiff's performance pursuant to the contract, the defendant's breach of its contractual obligation, and damages resulting from the breach.[68] The following are just a few case examples where the plaintiffs brought breach of contract claims resulting from a data breach:

- *In re SuperValu, Inc. Customer Data Security Breach Litigation*, Case No. 14-MD-2586, (D. Minn. March 8, 2018) (dismissing breach of contract claim where there was no contract governing the relationship between SuperValu and the affected consumers).
- *Community Bank of Trenton et al. v. Schnuck Markets Inc., Case No.* 3:2015-cv-01125, (S.D. Ill. 2017) (dismissing implied breach of contract claim because the

---

[65] *See e.g.*, *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 629 (3d Cir. 2017); *Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed. App'x 384, 391 (6th Cir. 2016); *Church v. Accretive Health, Inc.*, 654 Fed. App'x 990, 995 (11th Cir. 2016).
[66] 846 F.3d at 629.
[67] *Id.*
[68] *See e.g.*, *El-Nahal v. FA Mgt., Inc.*, 126 AD 3d 667, 668 (2d Dept. 2015); *Prime Props., Ltd. Partnership v. Badah Enters.*, 8th Dist. Cuyahoga No. 99827, 2014-Ohio-206, ¶ 13.

implied contract relationship between the parties did not give rise to a duty to protect the customer's data from third party criminals).

- *Dittman v. University of Pittsburgh Medical Center*, 2017 PA Super *, No. 971 WDA 2015 (Jan. 12, 2017) (dismissing breach of contract claim on the basis that there was no implied or express contract where University of Pittsburgh Medical Center agreed to protect the plaintiffs' confidential data).

- *Sackin v. Transperfect Global, Inc.*, 2017 U.S. Dist. 164933 (S.D.N.Y. 2017) (dismissing express breach of contract claim in data breach where employment contract did not reference protection of employee personal information, while denying motion to dismiss a breach of implied contract where the company's "robust" data security created an implicit promise to protect employee data).

- *Abdale v. North Shore-Long Is. Jewish Health Sys., Inc.*, 19 N.Y.S.3d 850, 859 (2015) (dismissing breach of contract claim in the data breach context where plaintiffs failed to allege violation of a specific provision of the contract at issue).

- *Fielder v. Penn Station, Inc.*, 2013 U.S. Dist. LEXIS 63573 (N.D. Ohio 2013) (breach of contract claim brought as a class action where plaintiffs alleged Penn Station data breach led to the disclosure of credit card information to third parties).

To date, consumer plaintiffs have had very limited success in bringing breach of contract claims. The main reason for this lack of success has been the absence of an express contract between the consumer and the compromised company. Courts have been unwilling to find that an "implied" contract creates a duty for the company to protect the data.

2) Negligence

To state a claim for negligence a plaintiff must allege that a defendant (1) owed a duty of care to the plaintiff; (2) breached that duty and (3) the breach of that duty proximately caused (4) injury to the plaintiff. [69]

In general, the economic loss doctrine has prevented the success of negligence claims in the data breach context.[70] "The economic loss doctrine prevents recovery in tort of damages for purely economic loss."[71] As the *Corporex* Court explained, "'[t]he well-established general rule is that a plaintiff who has suffered only economic loss due

[69] *See e.g.*, *Aim Leasing Co. v. RLI Corp.*, 2015 U.S. Dist. LEXIS 56780 at *4 (N.D. Ohio 2015); *Caronia v. Philip Morris USA, Inc.*, 715 F.3d 417, 428 (2nd Cir. 2013).
[70] *See e.g.*, *Cumis Ins. Soc., Inc. v. BJ's Wholesale Club, Inc.*, 918 N.E.2d 36, 39-40, 46-47 (Mass. 2009) (holding that the economic loss doctrine barred negligence claims in a data breach case).
[71] *Corporex Dev. & Constr. Mgt., Inc. v. Shook, Inc.*, 106 Ohio St. 3d 412, 2005 Ohio 5409, 835 N.E.2d 701, 704 (2005).

to another's negligence has not been injured in a manner which is legally cognizable or compensable.'"[72] Moreover, some courts have even held that "economic loss" includes loss of electronic funds due to the unscrupulous acts of a third-party criminal.[73]

In the data breach context, courts have held that the economic loss doctrine bars a plaintiff's tort claim because the plaintiff has not suffered personal injury or property damage.[74] Despite limited success, plaintiffs have continued to bring negligence claims arising from data breaches. Some examples include:

- *In re SuperValu, Inc. Customer Data Security Breach Litigation*, Case No. 14-MD-2586, (D. Minn. March 8, 2018) (dismissing negligence claim arising from a data breach because of the economic loss doctrine).
- *Galaria v. Nationwide Mut. Ins. Co.*, 2017 U.S. Dist. LEXIS 185166 (S.D. Ohio 2017) (dismissing negligence claim filed pursuant to a data breach where the plaintiff failed to adequately allege injury).
- *Dittman v. University of Pittsburgh Medical Center*, 2017 PA Super *, No. 971 WDA 2015 (Jan. 12, 2017) (dismissing negligence claim arising out of a data breach based on the economic lass doctrine).
- *Abdale v. North Shore-Long Is. Jewish Health Sys., Inc.*, 19 N.Y.S.3d 850, 860 (2015) (denying negligence *per se* claim based on violations of New York's data breach notification law as "no private right of action exists with respect to G.B.L. §899-aa.").
- *Khaled v. Cox Communs.*, 2014 U.S. Dist. LEXIS 134470, (N.D. Ohio 2014) (plaintiff brought negligence cause of action resulting from alleged improper disclosure of customer account information) (dismissed on other grounds).

3) Breach of Fiduciary Duty

The elements of a claim for breach of fiduciary duty are "breach by a fiduciary of a duty owed to plaintiffs; defendant's knowing participation in the breach; and

---

[72] *Id.* at 414 (quoting *Chemtrol Adhesives, Inc. v. Am. Mfrs. Mut. Ins. Co.*, 42 Ohio St.3d 40, 44, 537 N.E.2d 624 (1989)).

[73] *See Pavlovich v. Nat'l City Bank*, 435 F.3d 560, 569 (6th Cir. 2006); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 395 F. Supp. 2d 183, 204 (M.D. Pa. 2005)).

[74] *See Banknorth, N.A. v. BJ's Wholesale Club, Inc.*, 442 F. Supp. 2d 206 (M.D. Pa. 2006) (*affirmed* in *Sovereign Bank v. BJ's Wholesale Club, Inc* ., 533 F.3d 162, 175-76 (3d Cir. 2008); *Amerifirst Bank v. TJX Cos. (In re TJX Cos. Retail Security Breach Litig.)*, 564 F.3d 489, 498 (1st Cir. 2009); *In re Heartland Payment Sys.*, No. 2046, 2011 U.S. Dist. LEXIS 34953, at *74–87 (S.D. Tex. Mar. 31, 2011); *Annett Holdings, Inc. v. Kum & Go, L.C.*, 801 N.W.2d 499, 505 (Iowa 2011) (applying economic loss doctrine to bar recovery for unauthorized charges to credit card); *In re Michaels Pin Pad Litig.*, 830 F. Supp. 2d 518, 530-31 (N.D. Ill. 2011) (applying the economic loss doctrine to bar plaintiff's negligence claims in data breach action).

damages."[75] To prove a claim for breach of fiduciary duty, the claimant must establish the following elements: (1) a duty arising from a fiduciary relationship; (2) a failure to observe the duty; and (3) an injury resulting proximately from that failure. A claim for breach of fiduciary duty is essentially a negligence claim requiring a higher standard of care.[76]

- *In re Premera Blue Cross Customer Data Sec. Breach Litig*., 198 F. Supp. 3d 1183 (D. Ore. 2016) (court dismissed breach of fiduciary duty claim stemming from a data breach where plaintiffs alleged that their healthcare provider was in a "position of trust" and therefore had a fiduciary duty to protect sensitive personal information.)

- *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012) (breach of fiduciary duty claim stemming from data breach survived motion to dismiss where plaintiff alleged that stolen identity stemmed from data breach).

- *Hammond v. Bank of N.Y. Mellon Corp., 2010 U.S. Dist. LEXIS 71996 (S.D.N.Y. 2010) (breach of fiduciary duty claim failed where there was no fiduciary relationship and no damages were alleged).*

- *Shafran v. Harley-Davidson, Inc.*, 2008 U.S. Dist. Lexis 22494, 8 (S.D.N.Y. 2008) (plaintiff's breach of fiduciary duty among other causes of action failed for failure to show damages).

While less prominent than contract and negligence claims, breach of fiduciary claims have been brought pursuant to data breaches. To date, courts have been skeptical of fiduciary duty claims in the data breach context.[77]

C. Increasing Litigation in Data Breach Incidents

The traditional consumer data breach lawsuit is brought against the company holding the data of the victim, however, increasingly data breach lawsuits are being brought in different ways and by different parties. These lawsuits include actions involving point of sale vendors, forensic investigators, banks, shareholders, and

[75] *SCS Commc'ns, Inc. v. Herrick Co.*, 360 F.3d 329, 342 (2d Cir. 2004). This standard varies slightly from state to state, but the key standard relevant in data breach actions is often the lack of the existence of a fiduciary duty. *See e.g.*, *Wells Fargo Bank, N.A. v. Sessley*, 188 Ohio App.3d 213, 2010 Ohio 2902, ¶ 36, 935 N.E.2d 70 (10th Dist.).
[76] *See e.g*., *Strock v. Pressnell*, 38 Ohio St.3d 207, 216, 527 N.E.2d 1235 (1988).
[77] Recent data breach litigation include more novel theories of harm, including that the dissemination of personal information reduces its inherent value; misrepresentation of security protections; and overpayment of the goods or services, i.e., part of the price paid included data security. *See, e.g.,* Claridge v. RockYou, Inc., 785 F. Supp. 2d 855 (N.D. Cal. 2011); *In re LinkedIn User Privacy Litig.*, No. 5:12-cv-03088, 2014 WL 1323717 (N.D. Cal. Mar. 28, 2014).; *In re Adobe Sys., Inc. Priv. Litig.*, No. 13-cv-05226, 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014).

insurers. For instance, in 2016 in *Affinity Gaming v. Trustwave Holdings Inc*.,[78] a data breach victim sued a forensic investigator for $75,000,000 alleging fraud and breach of contract. Affinity owned and operated several casinos and became aware of fraudulent credit card activity on its data systems. Shortly thereafter, Affinity hired Trustwave, a firm specializing in the field of data security that "helps businesses fight cybercrime, protect data, and reduce security risks."[79] Trustwave contracted with Affinity to identify and help remedy the causes of the data breach. After Trustwave had finished its work, Affinity learned that the breach had not been cured and that the systems were still vulnerable and sued Trustwave as a result. The lawsuit survived a motion to dismiss when the court found that Affinity had established material questions of fact. The parties eventually settled the case for an undisclosed amount.[80] This section outlines the growing trend of these instances of non-consumer data breach lawsuits.

1) Plaintiffs in data breach lawsuits are not just those whose information was compromised

When a data breach occurs, it affects more than just the consumer whose information was compromised. Banks, card issuers, and shareholders all are affected and have brought numerous lawsuits seeking compensation for their damages. Additionally, as discussed in Section II above, state attorney generals and numerous federal agencies, mainly the FTC, also are in a position to bring enforcement actions. Although these entities have not had their information compromised like the consumers, they have had more success in litigation related to breaches than consumers.

a) Banks and Credit Unions

Card-issuing banks and credit unions have been heavily involved in data breach litigation based upon the logic that, when a data breach occurs, card issuers are damaged because they are legally and/or contractually obligated to reimburse fraudulent charges and may need to reissue credit and debit cards which have been compromised.[81]

---

[78] Case No. 2:15-cv-02464, 2016 U.S. Dist. LEXIS 135818 (D. Nev., Sept. 30, 2016).
[79] *Id.* at 2.
[80] Trustwave has been a popular target in recent data breach lawsuits. In 2014, Trustwave was sued by the banks for $10,000,000 alleging that Trustwave, as Target's security vendor, neglected to ensure and maintain Target's overall network security, which ultimately resulted in the breach. *See Trustmark National Bank et al v. Trustwave Holdings, Inc. et al*, Case No. 1:14-cv-02069 (N. D. Ill. 2015). In short, the lawsuit sought to hold Trustwave liable for failing to maintain Target's ongoing compliance with the PCI-DSS. The case would eventually settle for an undisclosed amount.
[81] When retailers agree to accept the credit card issuers charge card, they also agree to comply with the credit card companies' rules for merchants and processors which typically require compliance with PCI-DDS. *See e.g.*, https://usa.visa.com/dam/VCOM/.../card-acceptance-guidelines-visa-merchants.pdf.

The Target data breach of 2013, and the myriad of litigation filings which followed the breach, is a prime example. It is well known that in 2013 Target suffered one of the largest payment card data breaches to date.[82] Target has publically stated that at least 40 million credit cards were compromised in the breach, and that as many as 110 million people may have suffered the theft of personal information such as email addresses and phone numbers.

Shortly after the breach, Target was flooded with a host of lawsuits from banks and credit unions. Trade groups representing the banks and credit unions estimated that their members incurred more than $200 million of expenses related to the breach.[83] Target would eventually settle with the banks and credit unions for $20.23 million.[84]

b) Shareholder Derivative Actions

Increasingly shareholders of publically traded companies are bringing class action shareholder derivative actions against those companies where the companies' share values have decreased as a result of the data breach. The crux of these actions asserts that when a company suffers a data breach, the price of its shares is likely to decrease in value. For instance, in the 2017 Equifax breach, Equifax's share price dropped 20.7% in the two trading days following its September 7, 2017 disclosure of the breach—reducing Equifax's market value by more than $3.5 billion. In addition to the drop in share price, Equifax has incurred significant expense in defending itself from the 30 lawsuits brought against it—money which would otherwise be used for company expenses or dividends. As a result of this loss, in February of this year, a shareholder derivative action was filed against Equifax. The lawsuit seeks to recover damages resulting from Equifax's failure to safeguard data and fulfill its fiduciary duties to shareholders. [85] The lawsuit remains pending.

The Yahoo! Inc., December 2016 data breach is another example of shareholders bringing derivative actions against the company resulting from a data breach. The Yahoo data breach is unique in that it actually involved two separate data breaches, one in 2013 involving over one billion user accounts and another in 2014

---

[82] *See* "Target says up to 70 million more customers were hit by December data breach" WASHINGTON POST, (Jan. 10, 2014), *available at*: https://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html?utm_term=.ab735481f4df.

[83] *See* "Target in $39.4 million settlement with banks over data breach" REUTERS (December 2, 2015) *available at*: https://www.reuters.com/article/us-target-breach-settlement/target-in-39-4-million-settlement-with-banks-over-data-breach-idUSKBN0TL20Y20151203.

[84] *In re Target Corporation Customer Data Security Breach Litigation*, Case No. 14-md-02522. (D. Minn. 2015).

[85] *See Teamster Local 443 Health Services & Insurance Plan v. Gamble et al*., Case No. 1:18CV577 (N.D. Ga. 2018).

involving over 500 million accounts, which were not disclosed until late 2016 in two separate announcements. Following Yahoo's first announcement, its share price dropped 3.6% and following the second announcement the share price dropped an additional 6.11%.[86]

As a result of the share price tumble, shareholders filed two separate class action derivative lawsuits against Yahoo. The first, filed in March of 2017 in California state court, alleged California statutory violations as well as breach of fiduciary duties.[87] This lawsuit is still pending in the California courts. The second, filed in January of 2018 in federal court in California, alleged violations of the Securities and Exchange Act of 1934.[88] This action settled in April 2017 for $80 million.[89]

Yahoo and Equifax are certainly not alone[90] and the successful settlement in the Yahoo case may spur more shareholder actions resulting from data breaches. This may develop even though early on investors had "a pretty dismal track record at bringing shareholder class actions and derivative suits in the wake of data breaches."[91]

2) The Companies Holding the Data are not the Only Parties Being Sued

While data breaches most often result in actions against the party holding the data, those parties are often not the only ones being sued. Numerous lawsuits have been filed following a data breach which attempt to tie liability for the data breach to

---

[86] *See Madrack et al. v. Yahoo! Inc., et al*, Case No.5:17-cv-00373 (N.D. Cal. 2018), Complaint at ¶ 7, 10, *available at*: https://dandodiary.lexblogplatformthree.com/wp-content/uploads/sites/265/2017/01/Yahoo-Complaint.pdf at paras. 7 and 10.

[87] *See Spain et al v Mayer et al*, Case No. 17CV307054 (Cal. Super. Mar. 7, 2017). The case was eventually combined with various other shareholder actions against Yahoo. *See In Re Yahoo! Inc. Shareholder Litigation,* Case No. 17CV307054 (Cal. Sup. 2017) (Consolidated Action, Including *Spain v. Mayer*, Case No. 17CV307054; *The LR Trust v. Mayer*, Case No. 17CV306525; *Plumbers and Pipefitters National Pension Fund v. Mayer*, Case No. 17CV310992).

[88] *See Madrack et al v. Yahoo! Inc., et al*, Case No.5:17-cv-00373 (N.D. Cal. 2018).

[89] *See* https://gowlingwlg.com/en/insights-resources/articles/2018/yahoo-cyber-breach-settlement-cause-for-cheer?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

[90] There are endless other examples of shareholder derivate actions resulting from data breaches, though these cases have provided plaintiffs with mixed results. *See e.g., Palkon v. Holmes*, Case No.14-CV-1234 (D. N.J. 2014) (dismissing breach of fiduciary duty claim resulting from data breach); *Kulla et al v. Steinhafel*, Case No. 14-cv-00203 (D. Minn. 2014) (resulting from the Target breach); *Bennek v. Akerman*, Case No. 1:15-cv-2999 (N.D. Ga. 2015) (resulting from a data breach by Home Depot, the case was eventually settled after plaintiffs threatened appeal of District Court's dismissal).

[91] *See* "Investors Could Find Litigation Success With Equifax Breach", LAW 360 (Sept. 11, 2017), *available at*: https://www.law360.com/articles/962711/investors-could-find-litigation-success-with-equifax-breach.

some third party vendor. These third parties have included forensic investigators or data security firms hired by the compromised entity,[92] point of sale vendors, and website providers.

For example, in 2009 seven restaurant chains that suffered data breaches sued the maker and distributor of their point of sale system.[93] The plaintiffs were all using Radiant Systems' POS system and software, which was allegedly in violation of the PCI-DDS. As a result, the plaintiffs filed a class action complaint against Radiant alleging negligence. The plaintiffs sought damages stemming for millions of dollars in penalties and fines imposed by payment card companies as a result of the breach.

In addition to the lawsuits against Trustwave holdings referenced above, there have been numerous other examples of lawsuits brought against data security firms whose clients have suffered a data breach. In June of 2005, it was discovered that information for 40 million payment cards had been stolen from CardSystems Solutions, a payment card processing company. As a result, a merchant bank brought an action against CardSystem's security assessment company alleging it had negligently certified CardSystem's security as complaint with Visa's Card Information Security Program.[94] The complaint alleged $16 million in damages, which equaled the amount that plaintiff paid to the various card associations to satisfy claims by issuing banks arising out of the breach. The case would eventually settle under an obligation of confidentiality.

Website providers have also been the target of lawsuits. In 2015, Travelers Casualty and Surety Co. of America, as subrogee of a hacked bank, brought an action against the bank's Web design company, Ignition.[95] The plaintiff alleged that Ignition maintained the host server in a substandard condition that was inappropriate for a bank website, and that it failed to place basic anti-malware software on the server. As a result of the resulting breach, the bank was forced to spend extensive resources (allegedly $150,000) to comply with the various state-specific data breach notification laws, which Travelers ultimately would pay given the cybersecurity insurance policy it had provided to the bank. The case would eventually settle.

D. Examples of Data Breach Actions in the Franchise Context

Franchises, like any other businesses, are susceptible to data breaches, however the risk is exemplified for franchisors as some recent cases have held that franchisors can be liable for their franchisees' data breaches or privacy violations.

---

[92] *See supra*, discussion of *Affinity Gaming v. Trustwave Holdings Inc.*, Case No. 2:15-cv-02464, 2016 U.S. Dist. LEXIS 135818 (D. Nev., Sept. 30, 2016).

[93] *See* "Radiant, Computer World in the lawsuit soup" (Dec. 28, 2009) http://www.greensheet.com/emagazine.php? story_id=1714.

[94] *See Merrick Bank Corp., v. Savvis, Inc*. et al, Case No. 2:08-cv-02233 (D. Ariz. 2008).

[95] *Travelers Casualty and Surety Co. of Am. v. Ignition Studio Inc.*, Case No. 1:15-cv-00608 (N.D. Ill. 2015).

1) Case Study 1: Aaron's Inc.[96]

Aaron's and its franchisees rent furniture, electronics, and appliances. Among these electronics, Aaron's rented computers. Certain franchisees installed computer-monitoring software within these rented computers. The software allowed the franchisees to disable the rented computer remotely, track the computer's location, view images through the computer's webcam, and even capture the users log-in credentials. The customers renting the computers were not made aware of this invasive software.

The FTC brought an enforcement action against Aaron's despite the fact that Aaron's did not use this technology in its company-owned stores. The FTC determined that Aaron's allowed its franchisees to access the software designer's website to use the software, used its server to transmit and store content from the monitoring, and provided franchisees with instructions and technical support for using the software. The case would eventually settle, but not until Aaron's agreed to conduct annual monitoring and oversight of its franchisees, delete all information which was obtained, and seek express consent from consumers if it wishes to continue the practice.[97]

The key lesson learned from the Aaron's case is that the FTC may seek to hold franchisors liable for the actions of franchisees even where the franchisor does not directly contribute to any privacy violation or data breach. As explained in greater detail below, there are certain actions which franchisors can take to limit liability in this context with respect to their franchisees. In the Aaron's case, the obvious action which Aaron's should have taken was to immediately put a stop to the practice. However, what the FTC really focused on was the fact that Aarons *facilitated* the FTC violations by, among other actions, providing instructions on how to download the spying software.

2) Case Study 2: Wyndham Hotels & Resorts[98]

On three occasions in 2008 and 2009, hotel franchisor Wyndham suffered a hack of its computer systems. The hackers accessed personal and financial information of hundreds of thousands of customers which led to an estimated $10.6 million in fraudulent charges on customers' payment cards.[99] While the intrusions started at the franchisee level, hackers were able to infiltrate their locations and data via Wyndham's corporate reservation and management system. Upon discovery, Wyndham had an incident response plan in place and properly notified all affected customers. Banks also reimbursed customers for any fraudulent charges stemming from the breach, so Wyndham maintained that no consumer was harmed as a result of the breach.

---

[96] *Michael Peterson, et al v. Aaron's, Inc., et al*., (N.D. Ga. June 4, 2014).

[97] *See* "Aaron's Rent-To-Own Chain Settles FTC Charges That It Enabled Computer Spying by Franchisees", FTC, *available at*: https://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer.

[98] *FTC v. Wyndham Worldwide Corp., et al.*, Case No. 2:13-CV-01887-ES-JAD (D.N.J. 2015).

[99] *See FTC v. Wyndham Worldwide Corp., et al*., Case No. 14-3514 at 6 (3d. Cir. 2015).

Even though all of the consumer information was stolen at the franchisee level and consumers were not held liable for fraudulent charges, the FTC brought an action against Wyndham alleging that Wyndham's conduct was an unfair practice and that its privacy policy was deceptive. The basis of the claim was that Wyndham engaged in unfair cybersecurity practices that "taken together, unreasonable and unnecessarily exposed consumers' personal data to unauthorized access and theft."[100] These "unfair" practices included, among other things, Wyndham allowing its franchisees to store payment card information in clear readable text and the use of easily guessed passwords to access the computer systems.[101]

After litigation in which Wyndham challenged the FTC's authority to bring enforcement actions under its Section 5 of the FTC Act authority, the case eventually settled. The settlement resulting in Wyndham being required to comply with numerous non-financial obligations over the following 20 years, including yearly annual audits to ensure conformance with PCI-DSS.[102]

The main takeaway from *Wyndham* is that the FTC may seek to hold a franchisor responsible for the data breaches of its franchisees where the franchisor allowed the franchisees to engage in insufficient data security practices. Another lesson is that a franchisor should be careful so it does not overstate its privacy practices in its privacy policy. For example, Wyndham included a statement in its privacy policy that it followed standard industry practices and that it had appropriate safeguards in place. According to the FTC, this was not the case with respect to its franchisees' and exposed Wyndham, as the franchisor, to liability. The settlement, while non-monetary, carries with it a significant burden. The FTC order requires, for a period of 20 years, annual security audits, extensive oversight over its franchisees' information security systems and procedures, and increased obligations in the event of another breach.

3) Case Study 3: Wendy's Co.[103]

Between October 22, 2015 and March 10, 2016, payment card data, including account holders' names, account numbers and expiration dates, were accessed by hackers from multiple Wendy's franchisees' locations. In February 2016, the company announced that its experts had found malware on some of its franchisees' systems. The malware, which has been installed through the use of compromised third-party-

[100] *See Wyndham*, No. 14-3514 at 8-10.
[101] *Id.*
[102] *See* "Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk.", FTC, (Dec. 9, 2015), *available at:* https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.
[103] *First Choice Fed. Credit Union v. Wendy's Co.*, Case No. 16-506 (W.D. Pa. 2017); *Graham v. Wendy's Co*., Case No.1;16-cv-1153 (S.D. Ohio 2016); *Torres v. Wendy's* Co., No. 16-0210 (M.D. Fla. 2016).

credentials, affected one particular POS system used at 300 of 5,500 franchised restaurant locations. Wendy's corporate systems were not affected.

The data breach prompted multiple lawsuits against Wendy's, which included a class action brought on behalf of affected consumers, a class action lawsuit filed on behalf of affected financial institutions, and two shareholder derivative lawsuits. This litigation is still pending and the results have been mixed thus far. The consumer class action complaint has been dismissed as the court held that plaintiffs lacked standing because any fraudulent charges were reimbursed by the named plaintiffs' financial institutions.[104] However, on April 3, 2017, the court denied Wendy's motion to dismiss the class action claims brought on behalf of 26 financial institutions which alleged that Wendy's data security practices were negligent.[105]

The derivative shareholder actions allege that the company's management made a number of poor security decisions which included requiring all franchisees to implement the flawed POS system and failing to implement sufficient date security procedures in the event of a breach. This litigation is ongoing and was recently consolidated into a single action.[106]

Like *Wyndham* and *Aaron's*, the Wendy's litigation resulted from issues at the franchisee level for which the franchisor is primarily being held accountable. Depending on the success of the Wendy's lawsuits, it could potentially lead to a new wave of litigation against franchisors, but as indicated *supra*, these consumer lawsuits must still meet the elements of their respective claims, such as standing.

4) Case Study 4: Jimmy John's[107]

In July of 2014 Jimmy John's learned of a payment card breach that affected about 216 of its franchises in 40 states.[108] Hackers were able to obtain credit card numbers, and some cases, the cardholder's name, verification code and/or the card's expiration data. The incident occurred at the franchisee level, where an intruder stole log-in credentials from Jimmy John's POS vendor and used the credentials to remotely access the POS systems at some franchised locations and install malware. Importantly, despite learning of the breach in July, Jimmy John's waited until September 24, 2014 to publically disclose the breach.

The data breach lead to a class action lawsuit which alleged nine separate counts against Jimmy John's including violations of Arizona and Illinois state laws,

---

[104] *Torres v. Wendy's* Co., No. 16-0210 (M.D. Fla. 2016).
[105] *First Choice Fed. Credit Union v. Wendy's Co.*, Case No. 16-506 (W.D. Pa. 2017)
[106] *Graham v. Wendy's Co*., Case No.1;16-cv-1153 (S.D. Ohio 2016).
[107] *Irwin v. Jimmy John's Franchise, LLC*, Case No. 2:14-cv-02275, (C.D. Ill. 2014).
[108] *See* "Data Breach at Jimmy John's Could Damage Franchisees", Bloomberg, *available at*: https://www.bloomberg.com/news/articles/2014-09-26/data-breach-at-jimmy-johns-could-damage-franchisees

various torts, and breach of implied contract.[109] The plaintiffs were able to survive a motion to dismiss, but only with respect to their breach of implied contract claim and their claim alleging violation of Arizona's Consumer Fraud Act.[110] The breach of implied contract claim alleged that the parties entered into an implied contract whereby Jimmy John's would safeguard and protect their personal information and, in the event of a breach, timely notify the class members.[111] The court noted that "there is an implicit agreement to safeguard the customer's information to effectuate the contract."[112] With respect to the claim that Jimmy John's violated Arizona's data breach law, the court held that even though the Arizona law does not provide for a private right of action, plaintiffs claim could proceed as they adequately alleged that Jimmy John's deceptively induced Arizona consumers into believing that their financial information was secure. The case would go on to settle for an undisclosed amount.

The Jimmy John's case demonstrates how one vulnerability at the franchisee level can lead to franchise system-wide liability. In the instance of Jimmy John's, a single individual accessed log-in credentials and was able to compromise 216 franchisees' payment systems. The Jimmy John's case also evidences the value of franchisees having adequate incident response measures in place, as delays in disclosure of the breach appears to have affected the court's decision to allow the consumer class action to proceed.

IV. Considerations for Structuring and Protecting the Payment System

It would be ideal if a franchise system could inexpensively and easily make their payment system easy to use for its franchisees and provide robust security for payment card data in order to, among other considerations, protect the brand. The current legal and business environments do not lend themselves to a perfect payment system that will be impervious to breach, or in light of a breach, insulate the franchise system and save the brand from any damage.

There are a variety of risks associated with a breach of payment card information. The monetary responsibility to the at-fault party can be substantial. There are not only the chargebacks to the responsible party for fraudulent charges made on customers' payment cards, but the assessments imposed by the card brands, government investigations and lawsuits and related expenses.[113] There is also the potentially significant damage to the brand from the bad publicity that a data breach can inflict. Franchising has always been about creating a perception among the public of consistency in product and service. For that reason, the public does not uniformly

---

[109] *Irwin v. Jimmy John's Franchise, LLC*, Case No. 2:14-cv-02275, (C.D. Ill. 2014).
[110] *Irwin v. Jimmy John's Franchise, LLC*, Case No. 2:14-cv-02275, ORDER (C.D. Ill. Mar. 29, 2016).
[111] *Id.*
[112] *Id.*
[113] *See also* the discussion at Section III.

distinguish between the franchisor and the franchisees, or whether the breach arose at a franchisee's location versus the franchisor's company-owned location or back office operations. Most consumers do not differentiate in this way such that any data breach experienced by the brand, regardless of its genesis, has the potential to cause significant damage to the brand name and public trust which can have significance beyond just the direct economic damages associated with the actual breach.[114]

Where franchise systems have historically resisted being too involved in their franchisees' business operations for fear of increased claims of vicarious liability, the risks associated with a data breach, that carry with it the potential for significant damage to the brand image with the public, is changing the calculus such that the traditional view may be set aside.[115] Franchisors need to assess their risk exposure in their industry and decide whether to become more involved in data security in the franchise system. If not, they risk leaving the doors open to increased risks and liability. Strategies can be implemented, and structures and protections employed, that can assist in reducing the likelihood of a data breach, and limit the potential damage to the system, while still keeping in place traditional franchise protections.

Below are set forth some areas of focus and steps for the franchise system to help protect the payment systems and to prepare for the almost inevitable breach: [116]

A. Access the Systems in Place to Identify Risks.

Franchisors should take a hard look at their payment systems and processing environments and ask where the soft spots are that may permit a breach. It is a good idea to engage qualified consultants and experts[117] to access the system(s) and recommend security policies and structures that will lessen the risks to the payment system.[118] Prevention of a security breach is money well spent when considering the risks to the brand that arise from the financial losses from a breach for quantifiable

---

[114] *See* David Katz and Bess Hinson, Key Privacy and Security Issues for Franchisor, *available at*: https://www.nelsonmullins.com/DocumentDepot/Katz-Hinson-Franchise-Handbook_05-31-17.pdf (last visited Apr. 7, 2018) for a thoughtful overview of the various considerations for a franchise system addressing privacy and security issues.

[115] *See* Len McPhee, Paul Reeve, Shelly O'Callaghan and Sally King, *Data Privacy and Security: Can any Brand Sleep at Night*, IFA 48th Annual Legal Symposium, page 25-26.

[116] We caution the reader to keep in mind the quick pace of law in this area, changes in technology, and the seemingly endless innovations of hackers and other bad actors employ to breach payment systems, these strategies will continue to need to take into account the current environment and evolve over time.

[117] The Council manages programs that will help facilitate the assessment of compliance with PCI DSS: Qualified Security Assessor (QSA). QSAs are approved by the Council to assess compliance with the PCI DSS.

[118] Nina Vellayan, *PCI Compliance: What Your Franchise Should Know*, Franchising World, November 2011, *available at*: https://www.franchise.org/pci-compliance-what-your-franchise-should-know (last visited Apr. 7, 2018).

losses such as card brand assessments and chargebacks, but also those that are not easily quantified, such as short and long term damage to the brand's reputation that can also have a negative impact on its stock value and the public trust.

B. Consider the Payment System Structure

Many franchise systems have a hodgepodge of point of sale systems and payment processing environments that have developed over time as the franchise system grew and newer franchisees adopted current technology and card processing hardware at a faster rate than existing franchisees. These variations may have even grown out of a time when franchisees were not required to adopt any particular approved system by the franchisor, or were limited in their options due to the regional limitations of offerings by vendors. Start-up franchise systems have an opportunity to take advantage of a clean slate and impose standardized payment systems from a centralized review and approval process controlled by the franchisor. Existing systems may have more challenges in imposing changes, but may be able to look to the franchisees' obligation to comply with the franchise system operations manual as the underlying obligation to upgrade to more current equipment. In addition, franchisees may need to be educated to understand how these items impact their own business and to be assured that the requirements are not punitive, but protective for their businesses.

Standardization at the franchise system level includes the franchisor identifying payment systems and vendors for use by franchisees, and enforcing standardized use across the franchise system, rather than permitting franchisees to obtain their own payment vendors. Franchise systems will want to review, vet and approve the payment systems for the franchise system and ensure that franchisees sign up with an approved vendor for their equipment and payment processing. Franchise systems will also want to ensure ongoing auditing and assessment of such payment systems and approved vendors. The processing agreements with payment processors that franchisees will enter into will often heavily involve the franchisor at the front-end to review and confirm that the agreements are reasonable for the system, including company-owned locations, and to negotiate favorable terms for franchisees. However, it is imperative that franchisees sign agreements directly with the processors in order to affirm contractual privity between the franchisee and the vendor.[119] This also ensures the franchisor is not contractually caught in the middle between the vendor and franchisee, and is not contractually liable for the franchisee's agreement.

Another sound practice is to assess whether it is feasible to have the franchisee process data directly with the processor, rather than through the franchisor's network. One of the problems highlighted in the Wyndham case was Wyndham's holding of card payment information collected by franchisees in the franchisor's network that was allegedly not properly secured and encrypted. Unless there is a very specific business or consumer need, consider whether the franchisor needs that data, and consider

[119] It is also good practice to include language in any overarching agreements between franchisors and payment processors clarifying that the franchisor is not guaranteeing any obligations of the franchisee to the processor.

instead having all payment processing transmitted directly from the franchisee to the processor without going through any systems maintained by the franchisor.

Finally, consider requiring the use of advanced technologies, including point-to-point encryption (P2PE) and tokenization services to transmit data, and upgrading point of sale terminals to EMV. Encryption takes readable text and replaces it with a format that is unusable unless you have the correct encryption key to decrypt it. Even if a hacker were to obtain the information, it would not be usable. Tokenization similarly protects data while it is being transmitted but uses a token to decipher the information transmitted such that the information is not useful without the database to which the information relates. EMV provides further protection to transactions by providing additional card authentication, card verification and transaction authorization measures over traditional magnetic stripe transactions.

C. Communication and Training

Franchisees are unlikely to become experts in information security and PCI-DSS and will look to franchisors to help them navigate the requirements. While franchisors may have been reticent in the past to be involved in some details of their franchisees' businesses due to the heightened risk of vicarious liability claims, the risk of a data breach and potential damage to the franchise system warrants consideration of a more involved approach by franchisors, where possible in that franchise industry. For example, franchisees could be educated about the importance of data security practices, data security obligations and what is required for PCI-DSS compliance. And regular communication and training and auditing for compliance may be helpful for avoiding data breaches at the franchisee level. Further, implementing and communicating system-wide standards and procedures to franchisees may not only limit the likelihood of a breach in the payment system, but may also be beneficial in limiting the scope of enforcement by authorities.[120] To promote compliance by franchisees, franchisors might consider including in their required ongoing franchisee training the basics of PCI-DSS. This may include running a table top exercise simulating a real breach scenario to educate franchisees on responding in the event of an actual breach (including, of course, one of the first calls being to the designated person at franchisor!).

D. Franchise Agreement Provisions

Franchisors will want to examine their franchise agreement's indemnification provisions, particularly as to damages resulting from data breaches that are caused due to the actions or inactions of the franchisee. A review of the franchise agreement's insurance obligations should include updating insurance coverages to cover losses due to a data breach.

The franchise agreement should require each franchisee to adopt its own data security policy and response plan. It is likely that aspects of the response plan will largely be developed from examples that the franchisor provides to the franchisee.

[120] *See* generally the discussion of *Wyndham* at Section II.A.4.

Nevertheless, franchisors should require that a franchisee's information security program and policy include an obligation to cooperate and to promptly and fully communicate with the franchisor in the event of a breach.[121]

Lastly, it is a good practice to add an express requirement that the franchisee be in full compliance at all times with PCI-DSS, and if not already covered by the general right for the franchisor to inspect the franchisee's operations, include a right to audit to verify PCI-DSS compliance.[122] It is standard practice to require franchisees to follow the franchise system's operations manual, but depending on the industry, reliance on the franchisor's operations manual may not be sufficient for protecting data security, and particularly compliance with PCI-DSS, so expressly including obligations in the franchise agreement may be preferable.[123]

E. Vendor Agreements

When entering into relationships with vendors who will have access to data of any sort, but especially payment card data, consider the provisions of vendor contracts carefully. Focus should be put on the parties' relative responsibility for breaches, including consideration of the scope of the indemnification provision, caps on (and exclusions from) liability, insurance requirements, and obligations to comply with applicable laws. There should also be express provisions requiring notification of a vendor data breach involving any of the company's data, obligations to cooperate during an investigation, as well as outlining who will provide notification to customers and bear the costs, including related costs such as call center support and credit monitoring. Vendors are (for good reason) highly resistant to taking on responsibility for data breaches or, when willing to make a concession to bear responsibility, will impose very low dollar limits on its respective liability. The ability of a franchisor to negotiate an appropriate apportionment of risk with a payment processor is difficult as payment processors are very resistant to accepting any significant risk or financial exposure.

---

[121] *See* Len McPhee, Paul Reeve, Shelly O'Callaghan and Sally King, *Data Privacy and Security: Can any Brand Sleep at Night*, IFA 48th Annual Legal Symposium, page 27.

[122] The payment systems utilized in the franchise system should be reviewed by the franchisor periodically to ensure PCI DSS compliance by franchisees, and to the extent that franchisor is providing certain services or, for example, payment applications to aid franchisees in PCI DSS compliance, those services or software should also be evaluated.

[123] The PCI DSS Quick Reference Guide ("PCI Guide") issued by the PCI Security Standards Council ("Council") *available at*: https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf. The PCI Data Security Standard (PCI DSS) "applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS." *See* pg. 7 of the PCI Guide.

F. Insurance Coverage

Consider purchasing cyber insurance coverage for a data security breach; however, evaluate carefully the coverage provided. Cyber insurance policies do not follow an industry standard and can vary considerably in what is covered, excluded from coverage and sub-limits on coverages. Consideration should be given not only to coverage for actual damages incurred to third parties for the breach, but expenses related to the incident response, legal representation, notices to impacted parties, credit monitoring, and engagement of experts such as a forensic investigator to investigate and assess the breach, all of which can be substantial.[124] Consider also requiring franchisees to carry cyber insurance in the event of a breach originating from the franchisee's operations, which could also provide some benefits to the franchisor.

G. Prepare, Implement and Practice an Incident Response Plan[125]

In accordance with the PCI-DSS requirements which require a response plan, appoint a cross-functional committee of people inside the organization who will be engaged in the investigation, mediation and response to a breach and detail those various individuals' responsibilities and chain of reporting. The organization will be very busy dealing with the data breach, so it is important to have a detailed plan and set of responsibilities for each party on the incident response committee. Practice the response plan at least annually by conducting tabletop or similar exercises.

In the plan, require that a detailed chronology of the breach and actions be kept so that memories can be refreshed in the (unfortunate, but likely) event of later litigation or governmental investigations.[126]

Further, identify experts in advance of a breach who will need to be brought in to assist with the assessment and investigation. PCI Forensic Investigators (PFIs) will investigate a suspected occurrence of a cardholder data breach, including when and how it may have occurred. PFIs are qualified by the PCI SSC's program and must work for a Qualified Security Assessor that has a dedicated forensic investigation practice.[127] Also, consider whether the franchisor would want to retain its own privileged investigator, and if so, in what circumstances.

---

[124] *See* Jena Valdetero and David Zetoony, *Data Security Breaches, Incident Preparedness and Response*, published in 2014 by the Washington Legal Foundation, *available at*: https://www.bryancave.com/images/content/2/2/v2/2285/DataBreachHandbookValdeteroandZetoony.pdf (last visited Apr. 7, 2018) at page 10, et seq.

[125] For a detailed discussion of incident preparedness and response, see Jena Valdetero.

[126] *See* Valdetero at page 23.

[127] *See* https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators (last visited Apr. 7, 2018) where the Council provides a search function on its website to locate an approved forensic investigator.

Create plans of action for communication during and following a breach, including a plan for communicating with affected cardholders, employees and franchisees, including social media responses and press releases or statements. There are a number of states that have statutes specifying the type of notification, its content and timing. Having this information readily at hand will significantly speed compliance with these requirements.[128]

H. When it Happens, Learn and Take Corrective Steps

Franchise systems and other companies need to assume that a data breach will happen and plan accordingly. When it does happen, whether to your franchise system or to a third party, it is an opportunity to learn from the details of that situation and assess its impact on your own security and breach preparedness. In light of some of the breaches experienced by other franchisors, franchisors can better identify the weaknesses in their own systems and preparedness and create better plans and infrastructure to limit the likelihood of a future breach.

Nevertheless, when a breach does occur, and it will, use it as an opportunity to identify and fix the problem. With the ever-evolving technology and the relentlessness of hackers constantly looking for soft spots in your security to steal information, this process is not a one-time exercise for franchisors or franchisees, but requires regular and consistent evaluation and modification of security and response plans. Almost certainly, once franchisors think they have it right, it will change again.

V. Conclusion

Data security presents an ever-evolving environment, both in terms of legal obligations, industry obligations, and threats. Legal obligations, contractual obligations, brand considerations and others are some of the factors companies should review when assessing their cybersecurity risk and determining how best to mitigate those risks, both to the franchisor and the entire franchise system.

[128] *See* generally discussion at II.C.2. above.