International Franchise Association
52nd Annual Legal Symposium
May 5-7, 2019
Washington, DC

Navigating the Changing Privacy and Data Security Landscape

David J. Allsman, Esq.
Fisher Zucker
Philadelphia, PA

Shawn Clark, MBA Information Officer
Paul Davis
Jacksonville, FL

Linda C. Emery, Esq.
Quarles & Brady LLP
Milwaukee, WI

Elizabeth Simpson, CIPP/US
Regulatory Counsel
Home Instead Senior Care®
Omaha, NE

I. INTRODUCTION

Many see effective use of data as synonymous with success. Franchise systems collect a variety of information about franchise owners, current and prospective employee's current and prospective customers and clients as well as their friends and family members through numerous channels. Franchise systems gather these volumes of data to better target marketing campaigns, improve quality of service, identify inefficiencies, and otherwise improve their business and bottom line.

However, there are multiple legal and business risks that come with the benefits of using that data. When businesses do not take appropriate steps to protect the data, individuals may lose control of their information and their privacy. Businesses may fail to properly secure the data they collect either because they fail to appreciate the value of that individual's data or they hoard data beyond their capabilities in hopes of realizing its value in the future. Simultaneously, bad actors are unleashing more and more sophisticated cyberattacks on businesses that fail to properly secure data. Careless or disgruntled employees may delete data or expose it to theft. Former employees may take data as they leave for another employer. As a result of the data privacy risks associated with the collection of personal data, governments and agencies are creating new laws and regulations to protect individuals' personal data and enforcing existing laws and regulations.

Most privacy and security laws and regulations require the business to notify affected individuals, regulators, and even the media in the event that unsecured data was accessed by a real or perceived bad actor. Suddenly, the data that was valuable for enhancing the client/customer experience can become not just an asset, but a liability. Even franchisors and franchisees putting forth an earnest good faith effort to protect data can experience a data security incident and experience damage to the brand.

In order to prevent a data asset from becoming a data liability, a franchisor must:

(1) appreciate the importance of privacy and security laws;

(2) be educated and stay current on the ever-changing privacy and security landscape;

(3) be prepared for what is next in privacy and security law;

(4) set the bar for its network;

(5) provide any necessary support for franchisees;

(6) develop a comprehensive data security program; and

(7) develop an incident response plan.

II. THE CURRENT PRIVACY AND SECURITY LAW ENVIRONMENT

A. No Uniform US Standard

The United States does not have one comprehensive federal data privacy law. Rather there are over 80 federal laws which address data privacy and security. While there is no express grant of a right to privacy in the United States Constitution, the United States Supreme Court has concluded there are implied grants of a right to privacy against government intrusion based upon the 1st, 3rd, 4th and 5th Amendments.

Instead of a comprehensive law, the United States has adopted a patchwork quilt of privacy laws, largely on an industry by industry basis. One of the very first privacy laws was the Cable Communications Privacy Act[1] which protects the privacy of cable subscribers. The regulations promulgated under Health Insurance Portability and Accountability Act, and amended by HITECH, protect healthcare information created or held by organizations such as physicians, hospitals, or insurers. The Gramm-Leach-Bliley Act was designed to protect personal financial information. There are also data breach notification laws in all 50 states as well as a plethora of other privacy and security statutes at the state level.[2] A chart containing a summary of federal privacy and security laws, regulations, and common state privacy and security laws has been attached to this paper. In addition to all these laws, there are a number of industries that have developed their own standards for handling personal data, such as the automotive industry and the credit card industry.

B. The Regulators

The Federal Trade Commission (FTC) is the primary federal agency regulating and enforcing consumer privacy and data security protection in the United States. The FTC derives its authority from its mandate to protect consumers from unfair deceptive trade practices.[3] The FTC has brought over 60 enforcement actions[4] against companies that have failed to comply with their own privacy policies or have failed to use adequate security measures in storing or using personal data.

The FTC has issued several guidance documents that are helpful to businesses with regard to reducing the risk of a data breach. For example, the FTC released a publication entitled Data Breach Response: A Guide for Business. This was written to assist companies in preparing for and responding to a data breach. The FTC has also issued a statement explaining that the National Institute of Standards and Technology (NIST Cybersecurity Framework) is consistent with the FTC's reasonable and standard approach to data security enforcement.

---

[1] 17 U.S.C. § 551.

[2] https://www.quarles.com/data-privacy-security/data-breach-preparation-and-response/

[3] 15 U.S.C. § 45.

[4] https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf.

In addition to the regulatory authority exercised by the FTC, a number of other federal agencies regulate data privacy and security, such as the Department of Health and Human Services (HHS) with regard to protected health information.

C. A Patchwork of States

The states are not to be outdone in the enforcement of data privacy and security laws. All 50 states now have data privacy laws which require an organization to disclose a data breach to the affected individuals. Many of those laws also require notification of a breach to a state regulator, such as the State Attorney General or the state Consumer Protection agencies. Many of these states include specific time frames to provide notice of a data breach, typically between 30 and 45 days.

In addition to these data breach notification laws, about 16 states have passed data security laws which dictate how companies that collect personal data must store and protect that personal data. In most of those states, organizations that store personal data must use reasonable technical, physical and administrative security measures to protect personal data stored in their computer systems.[5]

III. PREPARING FOR WHAT'S NEXT IN PRIVACY AND SECURITY LAW

A. Expansion of State Data Privacy and Security Laws

California recently passed a new data law known as the California Consumer Privacy Act ("CCPA"), which is scheduled to take effect January 1, 2020. Some call CCPA a US version of the European Union's General Data Protection Regulation ("GDPR"). Under the terms of GDPR, organizations have to ensure that personal data is gathered legally and under strict conditions. Additionally, an organization that collects and manages personal data will be obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners - or face penalties for not doing so. While the California law has some similarities to GDPR requirements, it is narrower than GDPR in certain respects. For instance, CCPA only requires a written disclosure of information. On the other hand, the CCPA is broader than GDPR in a few respects. For instance, CCPA covers information about households, not just individuals. Likewise, the CCPA includes a broad definition of what constitutes a sale of data.

Under the CCPA, organizations doing business in California are required to disclose information regarding the storage of an individual's personal data upon request

[5] Alabama (Ala. Code 1975 § 8-38-2 (West)), Arkansas (Ark. Code Ann. § 4-110-104 (b) (West)); California (Cal. Civ. Code § 1798.81.5 (West)); Colorado (Colo. Rev. Stat. § 6-1-713.5; Connecticut (Conn. Gen. Stat. § 4e-70); Delaware (Del. Code § 12B-100); Florida (Flor. Stat. § 501.171 (2); Indiana (Ind. Code § 24.4-9-3-3.5); Kansas (K.S. § 50-6,139b); Louisiana (La. Rev. Stat. § 3074); Maryland (Md. Code Ann., Com. Law § 14-3501 (West)-503); Massachusetts (Mass. Gen. Laws ch. 93, § 2 (a)); Minnesota (Minn. Stat. §325 M.05); Nebraska (Neb. Rev. Stat. Ann. § 87-801 (West)-807 (2018 L.B. 757); Nevada (Nev. Rev. Stat. § 603A.210, 603A.215(2)); New Mexico, N.M. Stat. § 57-12C-4, 57-12C-5 (2017 H.B. 15, Chap. 36); Ohio (Oh. Rev. Stat. §1354.01-1354.05); Oregon (Oregon Rev. Stat. § 646A.22); Rhode Island (11 R.I. Gen. Laws § 11-49.3-2), South Carolina (S.C. Code §31-1-902012), Texas (Tex. Bus. & Com. Code Ann. § 521.052 (West)), Utah Code Ann. § 13-44-101 (West)-201, 301 and Vermont (Vt. Stat. Ann. tit. 9, § 2446-2447 (West)).

by that individual. Other states are similarly adopting data privacy laws and the varying state law regulations will easily prove more difficult for industry compliance than one comprehensive federal law. At the time of this article, 9 additional states have introduced bills which seem to be based upon the California Consumer Privacy Act.[6] The State of Washington has introduced a bill similar to the CCPA in the rights it provides individuals to their data. This bill, SB 5376, has now passed the Senate, passed committee in the House and is on the floor calendar.[7]

Furthermore, as states emboldened by the passage of the CCPA seek to pass their own legislation, there is the potential for companies to be more significantly impacted by a difference in state laws. Differing breach notification laws is much less burdensome than handling different laws that require prompt verification of an individual requesting data, disclosure of such data, or deletion of an individual's data. The breadth of differences between states would continue to grow.

State laws, such as the CCPA or Washington's proposed Washington Privacy law, make important concessions by exempting data protected in compliance with existing industry-specific federal laws (e.g. HIPAA or GLBA). However, confusion and difficulty may result where data protected by state law/regulation falls outside what is traditionally protected by the industry-specific federal law. For example, what would happen if one state required a HIPAA covered entity to maintain its information not subject to HIPAA in the same manner as information that is considered protected health information? Would HIPAA security standards apply as well such that all internet lead forms need to be encrypted even if they contain no health information (such as a newsletter sign-up)? What if the neighboring state's law conflicted and required a HIPAA covered entity to use its *state* standards for all information not covered by HIPAA?

B. Continued Attempts to Pass a Uniform Privacy and Security Law

To date, the US has been unable to reach consensus on a comprehensive US data privacy law. However, some large technology companies (Amazon, Apple, AT&T, Charter, Google and Twitter) have urged Congress to pass comprehensive legislation, which would preempt state laws and regulations in favor of federal privacy regulation. These industry players may be willing to adopt industry regulation for a variety of reasons. This may be because they are already ready for such changes after having to become GDPR compliant. Likewise, they may be trying to avoid a patchwork of state laws which are inconsistent as to the necessary steps businesses must take to provide protection of personal data.

Despite the requests by the large data mining companies such as Google and Facebook, it will be difficult for the US to pass a comprehensive federal data privacy and security act. This is true because there is already an extensive set of laws and regulations to protect personal data on an industry-by-industry basis. Each of those industries has a

[6] Hawaii, Maryland, Massachusetts, Mississippi (died in committee February 5th), New Mexico, New York, North Dakota and Rhode Island.
[7] Washington State Legislature: https://app.leg.wa.gov/billsummary?BillNumber=5376&Year=2019&Initiative=false (accessed 4/22/2019).

strong financial incentive to rely on their current regulatory practices, rather than trying to switch to an entirely new regulatory scheme.

We will however continue to see members of Congress introduce bills suggesting that there should be a US version of the GDPR. Some speculate that such a law is inevitable because of the GDPR. What is inevitable is that the topic of data privacy and security is not going away.

IV. WHY DATA PRIVACY AND SECURITY MATTERS TO FRANCHISORS

A. Brand Protection

There are certainly many practical reasons why franchisors need to protect the data and information they store and correct in compliance with data privacy and security laws and industry best practices. The most obvious of these reasons is to protect the brand. If a data breach occurs, there will be a harm to the brand. Customers may lose confidence in the company and the company will experience customer churn.

B. Direct Cost of Breaches

Companies incur extremely extensive costs in responding to a data breach. IBM sponsors an annual Cost of a Data Breach Study prepared by the Ponemon Institute, an independent research company that is an oft cited source of information about the costs of a data breach. According to the results of the 13th Annual Cost of a Data Breach Study, the average cost of a data breach in 2017 was $3.86 million. In that report, Ponemon also opines that the likelihood of a global data breach for such companies in the following 2 years is almost 30%.

Those costs include hiring forensic experts who will analyze the technical reason for the breach, attorneys to respond to the legal concerns and determine notification requirements under applicable law, and public relations costs for responding to the incident. In addition, just the costs of identifying the impacted individuals, preparing and providing written notice, mailing services assisting with the notification process, determining the cause, hiring experts to identify and notify affected individuals and hotline support will be significant. Companies are also likely to incur the costs of credit monitoring services, future discounts and coupons on products or services to try and gain back customers, and potential customer loss as a result of the breach. Finally, there is the risk of regulatory proceedings and class action litigation. None of these are happy topics for a company which has experienced a data privacy or security incident.

There are a number of well-known franchisors that have had to respond to data security incidents in the last few years. They include Burger King, Wendy's, Dairy Queen, Noodles & Company, Cici's Pizza, Panera Bread, Arby's, Pizza Hut, Chili's and Sonic.

Hotels also seem to be a major source of data breach issues. Notably, Hilton, Hyatt, Mandarin Oriental, Marriott, Rosen, Starwood and Trump Hotels. UPS and Goodwill have all suffered major data breaches in recent years.

Most of these data breaches involved personal information of consumers including theft of credit card information.

Even if it was the franchisee that caused the breach, the breach is likely to harm the franchisor as customers are unlikely to differentiate between the brand and the franchisees.

C. Vicarious Liability for Franchisee Data Security Incidents

Franchisors work hard to protect the legal boundaries between the franchisor and its franchisees. Franchisors must respect that the franchisees are independent businesses, not controlled by the franchisor.

However, the reality is that if the franchisee experiences a data breach, the franchisor shoulder the bulk of the blame in the media. As can be seen in the examples in this paper, the FTC will most certainly pursue a claim against the franchisor even if the breach was the responsibility of the franchisee.

Because of the nature of the technology used to operate franchise businesses, franchisors are often requiring their franchisees to utilize certain types of computer systems. This maintains uniformity between franchisees and helps give the customer a predictable experience, just like making sure the products and services maintain consistency between each franchisee. However, these computer systems can lead to technical insecurities which may give rise to a data breach and potential liability to the franchisor.

The FTC has taken enforcement actions against over 80 companies resulting from failures in their data privacy and security practices. Two cases involving franchisors are most commonly referenced in this regard.

The first is the Wyndham Hotel case. In Wyndham, the FTC pursued an enforcement action against Wyndham Hotels due to data breaches which occurred at several franchised hotels. The FTC sued Wyndham Hotels alleging that it used ineffective privacy and security practices[i] related to its computer systems where it required franchisees to store personal information. These security breaches happened on several occasions over a two-year period which exposed data to a Russian internet domain.

The FTC raised the issue of whether a franchisor, who requires use of a uniform computer system, is then responsible for establishing a reasonable franchisee security program. The FTC alleged that Wyndham failed to establish a reasonable information security program. The FTC also reviewed the hotel chain's privacy policy and held them responsible for the statements made within the policy.

The case was ultimately resolved when Wyndham entered into a settlement agreement with the FTC in 2015. The FTC did relieve Wyndham of vicarious liability for

the actions of its franchisees.[8] However, Wyndham still experienced significant harm to its reputation and was required to incur significant costs in responding to the breach allegations and defending the FTC's action. They were also required to develop a comprehensive information security program designed to protect cardholder data and to conduct annual information security audits and maintain safeguards in connection to its franchisees' servers consistent with PCI-DSS standards. The settlement agreement is in place for 20 years.

In contrast, the FTC brought an enforcement action against Aaron's in 2014[9] alleging that Aaron's improperly supervised its franchisees' privacy practices. Approximately 700 franchisees installed privacy invasive software called PC Rental Agent on computers they rented to their customers. This software allowed the franchisees to disable computers remotely and included a detective mode. If a franchisee used the detective mode, they could surreptitiously monitor the customer's activities, including using the computer's webcam. This, of course, was not disclosed to customers. Company owned stores did not use the PC Rental Agent software.

The FTC concluded that a franchisor can be liable for data security and privacy violations that were committed only by franchisees if the franchisor "knowingly assisted" the franchisees in committing the violations.

The FTC found Aaron's responsible for the acts of its franchisees because: (i) they were aware of mass communications between franchisees about the software; and (ii) because of IT support platforms that were provided to the franchisees by the franchisor.

The FTC noted, in particular, that the franchisor allowed franchisees to access the software designer's website without which the software could not be activated. The franchisor's server was used to transmit and store emails containing content obtained from the software and the franchisor provided franchisees with technical support. The franchisor provided franchisees with important technical support about the software program and how to use it, such as publishing trouble-shooting advice about installing the program on rented computers and avoiding conflicts with antivirus software. The franchisor both knew of and facilitated the use of the software in violation of the data privacy laws.

Aaron's entered into a settlement agreement and consent order with the FTC in 2018.[10] The terms of the settlement agreement and consent order prohibited Aaron's from using any monitoring technology to gather data or information from or about a consumer from a computer rented to a consumer receiving, storing or communicating any data or information from or about a consumer that was gathered from a computer rented

[8] Federal Trade Commission, Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk (December 9, 2015), available at https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.

[9] *In the Matter of Aaron's, Inc.*, CFTC No. C04442, File No. 122-3264, 2014 WL 1100702 (Mar. 10, 2014).

[10] Federal Trade Commission, Aaron's Rent-to-Own Chain Settles FTC Charges that It Enabled Computer Spying by Franchisees (Oct. 22, 2013), available at https://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer.

to a consumer using monitoring technology except with respect to assistance with the device.

Second, Aaron's was required to provide clear, express notice of its use of geophysical location tracking technology to consumers and must obtain their affirmative consent before using it. For computer rentals, the notice has to be given both at the time of the rental and at the time the tracking technology is activated unless the consumer reported the computer stolen or lost. Aaron's was also prohibited from deceptively gathering customer information through software. Aaron's also had to delete or destroy any information it improperly collected.

Third, Aaron's is required to conduct annual monitoring and oversight of its franchisees. They must also hold franchisees to the same standard they hold corporate stores regarding privacy. Last, they must terminate a franchise agreement if the franchisee does not meet the requirements.

There have also been additional cases whereby the courts have found that a franchisor in a privacy matter exercised actual control over the business operations of the franchisee, including its point of sales processes, policies and procedures. For instance, in a Nebraska federal court case, the court found that the defendant was sufficiently involved in the day-to-day operations of the franchisee to survive a motion to dismiss.[11]

In the case of *Patterson v. Denny's Corporation*[12], a customer sued the franchisor and its franchisee alleging a violation of the Fair and Accurate Credit Transactions Act of 2003 because a franchisee included the expiration date of a customer's Visa card on a printed receipt. The Federal District Court in Pennsylvania denied the motion to dismiss finding that the vicarious liability of the franchisor may be found if the franchisor exercised control over the franchisee's relevant processes.[13]

Ownership of data and protecting that data can become extremely important for franchisors. For example, in the case of *Sears Authorized Home Town Stores, LLC*,[14] Sears was sued because a Michigan franchisee and its guarantor failed to properly dispose of customer data after closing the business. Sears was prohibited from using or disclosing any personal information about the franchisees customers.

In the case of *Irwin v. Jimmy John's Franchise LLC*,[15] Jimmy John's was sued for a data breach over the alleged theft of customer data and financial information obtained from credit and debit cards used at the chain's sandwich shops. The company moved to dismiss and the court granted seven of the nine claims. Jimmy John's learned of the breach at the end of July but failed to notify customers until September 24 and the notification itself was inadequate. Jimmy John's neither emailed customers nor posted about the breach on Facebook or Twitter. Instead it posted an inconspicuous link to a

[11] See *Keith v. Back Yard Burgers of Nebraska, Inc.*, No. 8:11CV135, 2012 WL 1252965 (D. Neb. Apr. 13, 2012).
[12] *Patterson v. Denny's Corp.*, 2008, WL 250552, (W. D. Pa. Jan. 30, 2008).
[13] Id. at *2.
[14] See Wolters Kluwer Antitrust Law Daily, 2017 WL 370774 (Jan. 26, 2017).
[15] 175 F. Supp. 3d 1064 (C.D. Ill. 2016).

news release on its website and then from August 2 until September 2 they had five fraudulent charges on a credit card that the plaintiff claimed was the fault of Jimmy John's for failing to notify of the breach. Melissa Sachs, Jimmy John's Chews Off Most Claims in data breach suit, 2016 IPDBRF 0080 (April 12, 2016).

In 2018, Wendy's agreed to settle claims related to malware which infected franchisee locations and compromised customer payment information. (ttps://www.restaurantbusinessonline.com/financing/wendys-agrees-pay-50-million-settle-data-breach-claims). Wendy's entered into the settlement agreement to settle class action lawsuits brought by multiple financial institutions which alleged that from 2015-2016 the point of sales system of certain franchisees contained malware that compromised customer personal information. Under the settlement, Wendy's was required to pay $50,000,000, design and implement reasonable safeguards to manage its data security risks, continue to maintain Wendy's Technology LLC or as similar entity to provide foundational security services to franchisees and continue to maintain and update security standards for its franchisee operations manual or similar document that is distributed to franchisees to include information regarding franchisee's independent obligations to comply with card security requirements.

FRANCHISORS SET THE BAR

As a franchisor, you must look to data privacy and security as both an issue to be protected at the franchisor level AND at the franchisee level, keeping in mind the issues of vicarious liability. As a franchisor, you must ensure that your own cybersecurity program is in order AND you must develop minimum uniform data security policies for adoption by franchisees.

In order to do that, a franchisor should ensure it takes the following steps:

1) *Know all applicable laws*: A franchisor needs to identify which data privacy laws apply to that franchisor. For instance, are you governed by HIPAA? Do you have credit card data, requiring you to comply with PCI-DSS requirements? Are you using biometric data for employees to sign in at work?

2) *Map data*: Determine what type of data it is collecting, why it is collecting that data, where it is storing that data and what it is doing with that data. It must also determine what third parties may have access to that data. It must also determine when and how it will properly dispose of data.

3) *Develop a data comprehensive security program:* Develop comprehensive policies and procedures. This may be scalable to the franchisees as well.

4) *Obtain cyber insurance:* Franchisor should negotiate and obtain appropriate data security insurance policies. The cybersecurity insurance covers a variety of different items of third party coverage such as disclosure injury, content injury, reputational injury, impaired access injury and first party coverage such as privacy notification expenses, crisis management expenses, business

interruption, and e-theft coverage. Franchisors should give serious consideration to obtaining cybersecurity insurance coverage. However, a word to the wise, undertake a careful analysis as there are many policies being offered, but the insurance carriers are quickly adding exclusions and finding ways to deny coverage under those policies.

5) *Develop an incident response plan:* As part of developing an incident response plan(s), franchisors should retain subject matter experts to assist in developing that policy well in advance of the possible data incident so that it can respond as quickly as possible. These should include a lawyer, a forensic IT expert, a public relations team, an e-discovery team and a notification company, to name a few. The time to hire these subject matter experts is not once the breach has occurred. In fact, the forensic IT vendors are so very busy that they must be retained prior to a breach or they will be unable to help you when you reach out to them when you are experiencing a data breach. This is not the time to have to go shopping for help. It is important to remember that an incident response plan is not one and done. You must regularly review and update the plan and related policies/procedures as necessary. You need to train people on those policies. You need to engage in network penetration testing and table top exercises to look for points of vulnerability in the system security and in your ecosystem.

6) *Training for employees and other workforce members:* Not only do many privacy laws require training, but it is incredibly helpful in ensuring standards are followed. Access to a learning management system is ideal.

V. SUPPORT YOUR FRANCHISEES AND SUPPORT YOUR BRAND

No matter the size of your franchise system, your franchisees will benefit from training and guidance in their cybersecurity practices. Many franchisors provide training to their franchisees to show adequate security practices.

Clearly, there is an ongoing and direct tension between the efforts of franchisors to maintain an appropriate legal separation from franchisees and the involvement of the franchisor in the activities of the franchisees. Some of these activities are primarily reputational—where a franchisee has a security breach, the headlines are likely to involve the franchisor even if direct legal responsibility under the breach notification regulations rests with the franchisee. (Obviously, a class of plaintiffs may bring a claim against the franchisor as well, and the actions of a franchisee may invite an investigation from appropriate regulators).

The franchisor will have to walk the line between the need to provide guidance and support to the franchisees, protect the brand, and the risk of vicarious liability claims brought against the franchisor.

In order to do that, a franchisor may wish to provide the following for its franchisees:

1) An awareness of applicable laws: A franchisor should include a general description of the legal and regulatory requirements for franchisees in its franchise disclosure document.

2) Template documents for a franchisee to customize and use in its data privacy security program, such as policies and procedures.

3) Information on cyber insurance: It is advisable for a franchisor to require its franchisees to obtain cybersecurity coverage as well as other types of insurance coverage in case of a data breach. Not only do you need the traditional CGL coverage, it is important to consider cybersecurity coverage which deals with both data breaches and cybercrime coverage. Many franchisors require their franchisees to maintain cybersecurity coverage. Some franchise agreements contain provisions that allow the franchisee to maintain additional coverages if requested by the franchisor during the term of a franchise agreement.

4) Training Resources: Some franchisors require their franchisees to participate in data security training programs. They may require third party programs and require certification of completion of the training. For instance, for those franchisees that take credit card payments, in order to comply with PCI-DSS, those franchisees must be trained on:

   - Regularly checking POS Systems for spyware
   - Best practices for taking payment or personal data from customers
   - Backing up data regularly to mitigate loss of data
   - Using technical safeguards such as malware screens, anti-virus software and encrypt data in transit and at rest.

5) Update Franchise Agreement Requirements: Franchise agreements themselves are often long term agreements, running for 10 or more years. As a result, many franchise agreements do not address data security and privacy issues or do not contain provisions which would be considered critical today.

   Ideally, a franchisor wants to update franchise agreements to reflect the realities of today's connected environment. A best practice is to include provisions which require a certain level of security and clearly state the franchisee is responsible for maintaining and protecting personal data. This could be important because if there was a large scale data breach caused by a franchisee, the franchisor may need to terminate the franchisee in order to protect the overall brand, other franchisees and the customers.

   The franchise agreement may require a franchisee comply with brand standards or an operating manual. In such a case, the franchisee can have the

flexibility to update its data policies with changes in law, technology, and institutional knowledge. Such data policies may:

- identify what data franchisees may collect, what data they should not collect, what anti-virus programs they are using and how often they are updating their software.
- require training on how to transfer data and how to avoid phishing attacks.
- require the franchisee to promptly notify the franchisor if they experience a data security incident or breach.
- require the franchisee to cooperate with the franchisor and provide access to the franchisee's IT systems, to halt the attack and conduct an investigation.
- provide franchisor the right to name counsel to control the defense and media communications.
- contain a provision that prohibits the franchisee from making public statements about the breach without the franchisor's approval.
- require a separate indemnity for costs and claims associated with a data breach that could help shift the cost of the response to the responsible franchisee.[16]

All these steps can reduce the risk to both the franchisees and franchisor.

In addition, there are international data privacy issues to be considered in franchise relationships. Franchisors who properly address those risks can thrive. What you must do to prepare is to update franchise documentation to compliance with GDPR, amend the manuals to address international data privacy standards, put in place that breach response plan and consider how you collect data.

VI. LET'S GET DOWN TO BRASS TACKS: PRACTICAL SUGGESTIONS TO REDUCE RISK

There are many ways in which a franchisor can reduce the risk of a data security incident by either the franchisor or the franchisee.[17]

1. The franchisor should create a comprehensive data response plan. This is not just a set of papers which are developed and forgotten. It requires regular review, practice and updating.

2. The franchisor must include strong security measures and have an effective incident response plan. It is advisable to consider hiring a chief information security officer. Having a comprehensive plan, strong security measures and a CISO have been

[16] Gavin George and Marc Legrand, Law 360, a LexisNexis Company, *Franchisors Must Find The Right Data Security Balance,* available at www.law360.com/articles/693653/franchisors-must-find-the-right-data-security-balance? (last visited April 25, 2019).
[17] See, Jason Adler, Meghan Demicco and Jon Neiditz, *Critical Privacy and Data Security Risk Management Issues for the Franchisor*, 35 Sum. Franchise L.J. 79 (Summer 2015).

shown to so significantly reduce the risk of a data breach that by budgeting these measures, a company can save money by significantly reducing the risk of a data breach.

3. Adopt best practices for data security. The FTC has indicated that companies must use best practices when protecting data and having data security practices in place.[18]

4. Obtain cyber insurance coverage. However as with all insurance, they are subject to exclusions and attempts to avoid coverage.

5. Review your privacy policy to confirm you are handling data in accordance with that privacy policy. Update it as needed on a recurring schedule.

6. Use the franchise agreements to address data protection. The franchise agreement should include provisions requiring franchisees to take reasonable steps to protect information.

7. Know who owns the data. One major consideration is whether the franchisor or franchisee owns customer data. Generally, franchisors will own the customers, including all data relating to the customer. However, the franchisee can freely use and manipulate the data and engaging a direct relationship with the customer. As a franchisor, you will need to determine whether the cost of managing the data you own and the associated risks from a breach outweigh. It is not going to be sufficient for the franchisor to attempt to distance itself completely from the franchisee's actions in the case of a data breach of the franchisor's data.

8. Update the Operations Manual. It is also possible to address data security in the operations manual for a franchisee. For instance, you can include administrative, technical and physical safeguards requirements such as only using a franchisee owned Wi-Fi connection. The franchisee must use strong passwords and a unique encryption key for secure Wi-Fi. The franchisees must be trained not to write down or store credit card numbers. The franchisee must take steps to avoid one customer from seeing the credit card information of the other customer. It is very important to use strong passwords for access to point of sales and other systems that store email addresses or other personal information. Franchisees must train staff members on how to see tampering: for instance, inspect their point of sale machines on a regular basis for missing screws, wiring -- which are other sides of tampering.

9. Security Audits. Develop a data security audit procedure for franchisee customer service or field teams. These teams can check for compliance with system wide policies.

10. Communications. Franchisors can send system wide reminders to franchisees to be vigilant of their systems and their customer's information. Additionally,

[18] David B. Ramsey, *Data Security: Evolving Legal Duties and Challenges for Franchise Systems*, 20 No. 3 J Internet L. 3 (September 2016).

franchisors should periodically provide updates about system upgrades to keep franchisees informed of the latest measures and practices in place to protect the data.

11. System Wide Plan. Franchisors can put together a system wide plan for responding to a data security incident. Because of the nature of a data breach, the brand will be impacted In light of the possibility of press coverage and the speed of social media. To create a plan it will require multiple constituencies within the organization including legal, compliance, IT, marketing and HR.

12. Train. Training is an extremely important part of any data incident plan response which needs to be routinely communicated.

13. Privacy Policy. Review privacy policies and make sure you comply with the commitments you have put into those policies. Make sure your data security practices meet your claims. You must confirm that the privacy policy does not contradict the actual actions of the franchisor.

14. Third Party Service Providers. If any third party service provider will process data for a franchisee, they must have in place the same levels of security and be contractually bound to meet those requirements. Franchisors should require contracts with third-parties such as point-of-sale vendors to have adequate protection, including warranties, audit rights, and indemnification for data breaches.

15. Technical Standards. Implement network security guidelines in place such as requiring franchisees to maintain firewall logs for certain period of time to create an audit trail if needed.

16. Review Cross-Border Transfer Practices for international entities.

17. Require franchisees to meet third-party security standards such as PCI-DSS or ISO 27001 information security standards.

18. Post breach. Data security provisions that reference independent standards and audits should help ensure franchisees take reasonable steps to prevent data breaches while avoiding direct franchisor meddling that may lead to increased liability under the law.

VII. SO MANY US LAWS; SO MANY REQUIREMENTS

There are a vast number of data security laws and regulations in place that impact franchisors depending on the industry and the type of information being collected. In addition, there are a number of industries that have developed their own data security practices, most notably the credit card industry.

Franchisors need to identify the type of data they are collecting: personal data, credit card data, health data, and data about financial services, geolocation data, biometric data, or similar questions. We have addressed the most likely ones to impact franchisors and franchisees.

A. Payment Card Industry -- Data Security Standards

Many franchisees take credit card payments from their customers. Franchisees that collect credit card data will be required to comply with what is known as the Payment Card Industry Data Security Standard ("PCI-DSS"). Those standards were established in 2004 by the major credit card companies to increase controls around cardholder data and diminish credit card fraud.

PCI-DSS contains a set of security requirements that uses current technology and physical security best practices to protect cardholder data. All organizations that process, store, or transmit credit card information must be PCI DSS compliant.

A franchisee that collects credit card information will be required to notify the credit card company of a data security incident or be subject to substantial penalties. The notification must be within a specific time frame mandated by the credit card companies in their agreements with customers.

Under PCI DSS, at a minimum, organizations taking credit card payments must conduct self-assessments of their data security procedures and conduct quarterly compliance perimeter scans of all information technology systems involved in the transmission, storage, and processing of credit card transactions. These requirements apply to anyone in the processing chain, including the merchant's hosting company, payment gateway, payment processor, and acquiring bank.

Failure to meet this notice requirements can lead to penalties payable to the credit card companies ranging from a few thousand dollars to hundreds of thousands of dollars. They are imposed by the credit card companies on the banks that issue the cards. The banks in turn pass those costs to non-compliant merchants whose practices trigger the penalties.

Many organizations use third-party service providers to implement and maintain security controls required to meet PCI DSS. Organizations should develop and implement processes to monitor the compliance status of its service providers to determine whether a change in status requires a change in the relationship. The PCI Security Standards Council ("PCI SCC") has published the "Information Supplement: Third-Party Security Assurance," which provides further guidance on implementing third-party assurance programs. The PCI SSC continues to regularly update the standard to reflect current best practices, and in January of this year, it released version 2.0 of the "Information Supplement: Best Practices for Maintaining PCI DSS Compliance."

The Payment Card Industry has established fines of up to $500,000 per incident for security breaches when merchants are not PCI compliant. Notification in writing to all individuals whose information is believed to have been compromised is also required so those individuals can be on alert for fraudulent charges. As such, the potential cost of a security breach can far exceed $500,000 when the cost of customer notification and recovery is calculated.

Sonic Drive Inc. recently was sued in a class action related to a data breach which exposed credit card and debit card information at 325 of its locations. It happened at the point of sale system with malware that copied and transmitted the information from consumer payment cards when they made a purchase. Sonic contended it had adequate security precautions.

Sonic agreed to settle for $4,325,000 in a settlement agreement which is pending court approval. Settlement Agreement and Release, *In re Sonic Corp. Data Security Breach, No. 1:17-mo-02807 (N.D. Ohio).* Among other things, in the settlement Sonic agreed to require that its franchisees comply with PCI-DSS facilitate data privacy reporting and discussions among its franchisees to members of Sonic's corporate cybersecurity team and report on at least a quarterly basis to a franchise owner committee on issues concerning the Sonic information security and data privacy program related to Sonic drive in locations.

Franchisors may be at risk of violations if franchisees have a loose adherence to PCI provisions or poor security controls in their storefronts and businesses. Recent news of franchise breaches that occurred via a franchisee point-of-sale terminal are cautionary tales of how substandard PCI compliance and lacking cybersecurity measures can expose an entire enterprise. Additionally, many franchisees lack security expertise and cite PCI DSS as too costly and difficult to maintain. This view is highly problematic because the costs of a security breach and reputational harm can far outweigh the costs of PCI compliance.

A specific challenge in a franchise environment is that each location is independently owned and one weak link in that chain can create negative public relations. This can affect consumer confidence, which could be reflected in lower sales system-wide, not just in the compromised location.

So what should franchises do to ensure franchisees are providing proper PCI security in their stores, restaurants, and other businesses? Some card brands and financial services organizations are leading the compliance charge by providing their franchisor merchants a summary of compliance options to help periodically validate franchisee PCI-related equipment, processes, and systems. This offering can reveal vulnerabilities, improve data security awareness, and include options such as leveraging a security portal, which can capture PCI transactions and compliance at the time of submission. Other options include using an outside Qualified Security Assessor to verify compliance and controls, or deploying various franchise-guided templates that report franchisee PCI activity.

Franchisors must be diligent in their franchisee PCI compliance management or run risk of a breach that will undoubtedly impact the entire organization. Particularly high-risk franchise systems include: lodging; quick service restaurants; services with automated recurring payments, such as gyms and educational services; and any systems utilizing IP connections for processing payments.

B. HIPAA

One of the most well-known of the federal data privacy laws is HIPAA -- the Health Insurance Portability and Accountability Act of 1996 -- handles the collection of health and medical information.

Protected Health Information

Franchise business models that require access to an individual's identifiable health information like patient data are subject to special privacy and security rules and regulations under federal and state law. If a franchise model requires such access or collection of an individual's health information, then the most important law for both the franchisor and franchisee to understand and comply with are the Health Insurance Portability and Accountability Act (HIPAA) of 1996.[19]

HIPAA imposes privacy and security protections for an individual's health information, along with enforcement standard for non-compliance and notification requirements in the event of a breach of an individual's health information. In implementing HIPAA, the Department of Health and Human Services (HHS) issued two main rules[20]: (1) the HIPAA Privacy Rule, which set national standards for the protection and privacy of individually identifiable health information; and (2) the HIPAA Security Rule which established national standards for the security of electronic protected health information or PHI.

HIPAA has been amended multiple times since becoming law, but most importantly through the Health Information Technology for Economic and Clinical Health (HITECH) Act[21] and the Affordable Care Act of 2010 (ACA).[22] In 2013, HHS issued comprehensive regulations[23] that finalized these changes by imposing privacy, security, and breach notification standards along with prescribing enforcement actions against entities that fail to comply with these regulations.

These HIPAA rules and regulations apply to a franchisee or franchisor that are "Covered Entities".[24] A franchisee or franchisor is a "Covered Entity" if they are a health plan, a patient data clearinghouse, or a healthcare provider who conducts certain health care transactions in electronic form (for example, electronic billing and fund transfers). Most franchisees or franchisors that provide some sort of healthcare related services, and would need or have access to PHI would be considered "Covered Entities".

HIPAA also applies to third parties called "Business Associates" that would create, receive, maintain, or transmit PHI on a Covered Entity's behalf. Covered Entities are required to enter into a written agreement with a Business Associate called a "Business Associate Agreement" in order to disclose PHI to the Business Associate. A Business

[19] The Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 100 Stat 1936, (August 21, 1996).
[20] 45 C.F.R. § 160.
[21] American Recovery and Reinvestment Act of 2009, Pub. L. 111–5, 123 Stat 115, (Feb. 17, 2009).
[22] Patient Protection and Affordable Care Act (Pub. L. No. 111-148,124 Stat 119 (March 23, 2010).
[23] 78 Fed. Reg. § 5566 (Jan. 25, 2013).
[24] 45 C.F.R. § 160.103.

Associate Agreement or BAA would contain written assurances from the Business Associate limiting the use of PHI for only purposes necessary to carry out its obligations to the Covered Entity, safeguarding the information from misuse, complying with HIPAA regulations, and making information regarding disclosure and breaches available to the Covered Entity.[25]

If the franchise model requires a flow of individual health information between a franchisee and franchisor, both parties will need to establish privacy and security policies and procedures to stay compliant with HIPAA. This would including establishing and implementing safeguards to protect PHI and other health information, notification procedures in the event of a breach, and training their respective workforce on the proper use and handling of individual health information.

A franchisee or franchisor that fails to comply with HIPAA rules and regulations are subject to significant criminal and civil penalties.[26] HHS's Office of Civil Rights (OCR) is primarily tasked with enforcement of HIPAA regulations including investigating complaints against or breaches by Covered Entities and Business Associates.[27] OCR coordinates with other state and federal agencies, including the Department of Justice, in the investigation of breach of HIPAA rules and regulations. OCR has imposed multi-million dollar penalties, and may require corrective action plans for non-compliant Covered Entities and Business Associates. For example, in October 2018, HHS announced a $16 million settlement and a corrective action plan with Anthem, Inc., following cyberattacks in 2014 and 2015 that resulted in the theft of PHI for nearly 80 million individuals.[28]

C. Gramm-Leach Bliley Act

Title V, Subtitle A of the Gramm-Leach-Bliley Act ("GLBA"),[29] also known as the Financial Services Modernization Act of 1999, regulates the collection, use, protection and disclosure of nonpublic personal information by financial institutions.

It applies to "Financial Institutions" which is broadly defined to include "any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities…."[30] Examples of businesses that qualify as financial institutions under the GLBA include banks, consumer lending companies, real estate appraisers, title companies, insurance companies and tax preparers (with an exemption for public accountants).

---

[25] 45 C.F.R. § 164.502(e).
[26] 45 C.F.R. §§ 160.400-26; 42 U.S. Code Part C - Administrative Simplification, §1320d–5.
[27] 78 Fed. Reg. § 5566 (Jan. 25, 2013).
[28] HHS Press Office, Health and Human Services, *Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History*, available at https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html (Last accessed April 15, 2019).
[29] 15 U.S.C. § 6801 *et seq.*
[30] 12 C.F.R. § 1016.3(l)(1).

GLBA regulates nonpublic personal information ("NPI"), which is "(i) personally identifiable financial information; and (ii) any list, description, or other grouping of consumers… that is derived using any personally identifiable financial information that is not publicly available,"[31] with some exceptions.

Personally identifiable *financial* information is broadly defined to include nearly all personally identifiable information a financial institution receives from or about a consumer when the consumer engages in a transaction with the financial institution, even information that one might not typically consider "financial." "Personally identifiable financial information" is defined as any information:

> (i) A consumer provides to a financial institution to obtain a financial product or service from the institution;
>
> (ii) About a consumer resulting from any transaction involving a financial product or service between financial institution and a consumer; or
>
> (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer."[32]

Furthermore, a financial institution's obligations under the GLBA with regard to notice, disclosures and opt-outs often depend on whether the individual is a consumer or a customer of the financial institution. A consumer is an individual who obtains or has obtained financial products or services from a financial institution primarily for personal, family or household purposes,[33] whereas a customer is a consumer with a continuing relationship with that financial institution.[34]

The Financial Privacy Rule.

The Financial Privacy Rule of the GLBA dictates the timing and content of privacy notices, disclosures and opt-outs that financial institutions must make to consumers with regard to the collection, use and disclosure of NPI.[35]

Generally, a financial institution must provide prior notice to a consumer before disclosing NPI to affiliates, but the consumer is not required to consent and cannot opt-out of such disclosure. Further, a financial institution must typically provide prior notice and a notice of its privacy practices, and the option to opt-out prior to disclosing NPI to non-affiliated third parties. There are several exceptions to the generalizations made in this Section.

If the consumer qualifies as a customer, the financial institution must provide a privacy notice to the customer before or at the time of creating the

[31] 12 C.F.R. § 1016.3(p)(1).
[32] 12 C.F.R. § 1016.3(q)(1).
[33] 12 C.F.R. § 1016.3(e)(1).
[34] 12 C.F.R. § 1016.3(i); 12 C.F.R. § 1016.3(j)(1).
[35] 12 C.F.R. § 1016 *et seq.*

customer relationship. In addition, financial institutions must send customers an annual privacy notice. The GLBA and its implementing regulations provide a sample privacy notice that financial institutions may use.

Safeguards Rule.

The Safeguards Rule of the GLBA requires financial institutions to establish appropriate standards relating to:

> "administrative, technical, and physical safeguards (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[36]

A franchise might trigger the GLBA when it engages in certain financial activities such as providing financial products or services to consumers. Examples include providing consumer loans, credits cards, financiering and insurance. In these cases the franchise would qualify as a "financial institution" that is collecting NPI and therefore trigger GLBA.

D. State Data Breach Notification Laws and Data Security Laws

There are also a variety of state data privacy and security regulations. All 50 states have data breach notification requirements. In addition, many states now have data security laws which require that companies that hold personal data meet certain requirements. Because franchisees are typically located throughout a large geographic area, there are many data security laws that must be considered tracked and evaluated.

Most notably, the State of New York issued regulations in 2017 known as the New York Cybersecurity Statute (23 NYCRR 500). Under those regulations banks, insurance companies and financial service organizations that are regulated by the New York Department of Financial Institutions must establish and maintain a cyber program, must adopt a written cybersecurity policy that involves third party service provider management, must use technological controls and an incident response plan, periodic audits and risk assessments, must appoint a chief information security officer, and must be in compliance with additional training and technology requirements.

E. Biometrics Data

One of the most discussed areas of data privacy laws in the last few months is the law related to biometrics data. “Bio” refers to biological characteristics and “Metrics” refers to a system of measurement. Biometrics data includes measurements such as retina scans, finger prints, voice prints, hand scans, and face geometries. Increasingly,

[36] 15 U.S.C. § 6801(b)(1)-(3).

biometrics data is being used in a variety of innovative way. For example, biometrics data is being used to enhance security by acting as a replacement for passwords. The IPhone 10 face recognition feature is a recent example of biometrics data being used to authenticate a user. Biometrics data is also being used to monitor an individual's movement and activity. For example, Fitbit wristbands may track and compile a user's heart rate, steps walked per day and sleeping patterns.

In 2008, Illinois was the first state to enact the Biometric Information Privacy Act (BIPA).[37] BIPA requires employers to adopt policies regarding biometric data collection and obtain consent before collecting biometric data. Additionally, employers are prohibited from selling or profiting from any individual's biometric information. BIPA contains a private right of action for $1,000 in statutory damages for each negligent violation ($5,000 for each intentional or reckless violation), as well as injunctive relief and attorney's fees.

BIPA is the only state law allowing private suit and recovery of damages for violations. Years after BIPA was enacted, the law has caused a recent stir due to the recent *Rosenbach v. Six Flags Entertain. Corp.*[38] decision. In *Rosenbach*, the plaintiff's son was required to submit a fingerprint scan in order to use a theme park season pass. The plaintiff's son was never informed why his fingerprint was necessary or given details as to how his fingerprint would be used and stored by the theme park. It is important to note the plaintiff never stated a claim for financial harm or violation.

The Illinois Supreme Court accepted the plaintiff's argument that the theme park had violated BIPA and violation of BIPA alone was sufficient to bring suit. Specifically, the court decided that an Illinois resident may have been violated under BIPA even if he or she has not alleged some actual injury or adverse effect. The *Rosenbach case* has opened the floodgates of litigation under BIPA within the Illinois court system and resulted in a nationwide conversation to best address biometric data.

L.A. Tan Enterprises, Inc. recently settled a class action lawsuit based upon a violation of the biometrics statute for $1.5 million dollars.[39] The plaintiff claims that L.A. Tan violated the BIPA by collecting fingerprints from its members for verification during check-in. The settlement involved around 37,000 class members who had their fingerprints scanned during a three year period. L.A. Tan agreed to comply with BIPA in the future and ensure the compliance of its franchisees.

It is important to note that L.A. Tan salons stored those member fingerprints in a company-wide database. The plaintiffs alleged that part of their violation was disclosing member fingerprints to an out-of-state third party vendor without consent. The plaintiffs also complained that they were not given a written data retention policy that disclosed guidelines for permanently destroying its customers' fingerprints.

---

[37] The Illinois Biometric Information Privacy Act 740 ILCS 14/1.
[38] *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 (Jan 25, 2019).
[39] See *Sekura v. L.A. Tan Enterprises, Inc.*, Case No. 2015 -CH- 16694 (Cook Cty. Dec. 1, 2016).

Currently, Texas and Washington[40] are the only other two states with laws on the books that directly address biometric data. Each of these states requires some type of notice and voluntary consent before biometric information is collected by a private company. Only the state attorney general may bring suit to enforce biometric laws in Texas and Washington. Similarly post the *Rosenbach* case, a bill has also been introduced in the Illinois state legislature to remove the private right of action under BIPA and calls for enforcement by the Illinois Attorney General and Department of Labor.[41]

Comparable legislation is pending in multiple other states. New York has a proposed bill that awaits being signed by the governor. If signed, the proposed bill will require private entities in possession of biometric identifiers or biometric information to develop a written policy establishing a retention schedule and guidelines for permanently destroying biometric data.[42] Similarly, the California Consumer Privacy Act of 2018 includes a definition for "Biometric Information" indicating future legislation tailored toward protecting biometric markers.[43]

The European Union has taken a more active approach. Under the GDPR (General Data Protection Regulation), biometrics is considered a “special category of personal data requiring additional protection.” Any biometric data collected from a European Union resident requires a special legal basis for processing and an accompanying data protection impact assessment.

Given the overall rise in biometric state-level laws, franchisors should carefully consider the types of biometric data collected from any of their employees or customers. To err on the side of caution, franchisors should provide transparent notice to their employees and customers about any biometric collection processes and update their policies to account for the collection of any such data. Furthermore, franchisors should obtain voluntary consent prior to any biometric data collection and clearly notify how such data will be used, stored, and eventually deleted. In particular, franchisors should be cautious when collecting data from residents located in Illinois and Europe. It is recommended that franchisors keep an eye on newly-enacted state biometric laws to ensure they can comply with new obligations and monitor the effects of active litigation and amending bills under BIPA in Illinois.

With respect to biotechnologies, Illinois, Washington and Texas have laws in place that regulate the use of biometric technologies and California has incorporated it into its nearly passed California Consumer Privacy Act. In those laws, if you require your employees to provide biometric information you have to tell them how it is going to be used and how it is going to be secured. Illinois allows a private cause of action for a violation of the Illinois Biometric Information Privacy Acts meaning that the private parties can sue companies for alleged violations.

---

[40] Tex. Bus. & Com. Code 503.001; RCWA 19.375.010 *et seq.*
[41] IL - SB2134.
[42] A9793, Assemb., Reg. Sess. (N.Y. 2018).
[43] California Consumer Privacy Act of 2018 (“CCPA”), CAL. CIV. CODE § 1798.140(b).

VIII. AND OF COURSE, DO NOT FORGET GDPR. WHAT IS ALL THE FUSS ABOUT?

By now, you are likely to have heard about the European Union's General Data Protection Regulation (GDPR). GDPR is the European Union (EU) legal framework that regulates and governs personal data. GDPR went into effect on May 25, 2018.[44]

The first question many US based companies ask with regard to GDPR is that it must not apply to them because they only do business in the US. That view point is quite naïve.

GDPR protects Personal Data of European Union (EU) residents. GDPR requires legal entities that obtain "Personal Data" from EU residents to follow an extensive regime of governance, legal, process and training practices to protect Personal Data. The GDPR greatly expands the obligations of any entity processing the Personal Data of an EU resident.

Under the EU Regulation, Personal Data is defined as any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Art. 4(1).

Mostly notably, unlike in the US, even business contact information of an EU resident is considered "Personal Data" for purposes of GDPR.

There are many reasons why US entities need to be performing many of the same evaluations, process changes and improvements with regard to obtaining, processing, storing, using, securing and sharing personal data under various federal and state laws.

Some of the key considerations related to GDPR for US based companies with international operations doing business in the EU are as follows:

IX. DOES GDPR APPLY?

The first step in evaluating issues related to GDPR compliance is to confirm that GDPR applies. Under Article 3 of the GDPR, GDPR applies to

Companies that offer goods or services in the EU

Companies that monitor the behaviors or individuals that take place in the EU or

[44] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.

Companies with EU operations or employees.

If the answer to any of these is yet, GDPR applies.

It is notable that the EU regulators have commented that if all you have is a website where EU residents can visit and ask for information by itself, that use case does not require GDPR compliance. However, if we are intentionally targeting EU residents, GDPR applies to you.

X. OVERVIEW OF IMPORTANT STEPS TO TAKE TOWARDS GDPR COMPLIANCE.

To those of you who are late to the GDPR game, it is still very important to take steps towards compliance. While the topic of GDPR is so massive that we cannot address it in any detail in this paper, you need to consider the following steps to comply with GDPR.

1. **Governance Documentation.** Develop documentation and internal controls to ensure compliance with GDPR. The organization must show that it is committed to protection of Personal Data as defined under GDPR.

2. **Data Mapping.** The organization needs to go through a data mapping process if it has not already done so. This will help determine what Personal Data you are receiving, where you are storing it, why you collect that Personal Data and how long you keep the Personal Data.

3. **Website Policies.** Review your website privacy policy to ensure that it addresses GDPR concerns or create a separate Privacy Policy which addresses GDPR. Don't forget the cookie policy as well.

4. **Consider Unambiguous Consent.** Many organizations include a website drop down box allowing EU residents to provide Personal Data. Make sure you have proper consents associated with those drop downs.

5. **Vendor Contracting**. Under GDPR, you are responsible for ensuring that your contractors who have access to Personal Data from your organization comply with the data security and privacy requirements of GDPR. (This is also true under US law). In order to undertake this process you will need to:

- **Identify those vendors you do business with that have access to Personal Data.** Usually, HR, IT, Marketing and Finance are the key areas which have agreements which are impacted by GDPR.

Violations of GDPR can result in fines of up to 4% of annual global turnover or €20 million, whichever is greater.

GDPR applies to franchisors established in the EU, and to franchisors outside of the EU that either (1) offer goods or services to individuals in the EU, or (2) monitor the behavior of individuals that takes place in the EU.

Recently, the FTC brought an action against TES Franchising In The Matter of TES Franchising LLC[45] alleging that the respondent had made false representations regarding its participation in the safe harbor program, to consent to prohibit them from making misrepresentations about its membership and any privacy and security programs sponsored by the government or self-regulatory or standard setting organizations.

[45] In re TES Franchising, LLC, FTC Docket No. C-4525 (May 29, 2015).

US--Marketing & Telecommunications	Telmarketing and Consumer Fraud and Abuse Prevention Act (includes Telemarketing Sales Rule (TSR)	Telephone Consumer Protection Act of 1991 (TCPA)	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)
Law Citation(s)	15 U.S.C. §§ 6101-6108	47 U.S.C. 227	15 U.S.C §§ 7701-7713
Corresponding Regulatory Citation(s)	16 CFR 310	FCC regulation 47 CFR 64	16 CFR 316
Summary	Telemarketers and Sellers are generally prohibited from: deceptive telemarketing acts or practices; engaging in a pattern of unsolicited telephone calls that a reasonable consumer would consider coercive or an invasion of privacy; calling during certain hours of the day and night; and failing to disclose of the nature of the call at the start of an unsolicited call made to sell goods or services. This includes a requirement that accurate call identification information be transmitted, telemarketers cannot abandon calls unless they meet the safe harbor of not abandoning more than 3% of outbound calls, allowing the phone to ring four times of 15 seconds, play a recorded message stating the name and phone number of the seller if a live person is not available within two seconds, and maintains documentation of the foregoing. Consumers may consent to receive calls in writing. The U.S. National Do Not Call (DNC) Registry is a well know feature of the TSR and does not apply to calls to customers with an established business relationship in the last 18	An automatic telephone dialing system cannot make calls to any cell phone or other service "for which the called party is charged for the call." Resources are available on the FCC website: https://www.fcc.gov/general/telemarketing-and-robocalls	This Act establishes requirements for those who send unsolicited commercial email. The Act bans false or misleading header information and prohibits deceptive subject lines. It also requires that unsolicited commercial email be identified as advertising and provide recipients with a method for opting out of receiving any such email in the future. In addition, the Act directs the FTC to issue rules requiring the labeling of sexually explicit commercial email as such and establishing the criteria for determining the primary purpose of a commercial email. This act is behind the "opt-out" links provided at the bottom of emails, which senders must honor promptly (within 10 business days).
Regulated Parties	**Seller**- any person who provides, offers to provide or arranges for others to provide goods or services to the customer in exchange for consideration in connection with telemarketing. **Telemarketer**- any person who initiates or receives telephone calls to or from a customer or donor in connection with telemarketing. Telemarketing is a "plan, program or campaign conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call. "	Any person or entity using an automatic telephone dialing system or an artificial or prerecorded voice to make calls	Any person considered a sender of a commercial electronic communication. This excludes a transactional or relationship message as defined by the Act.
Whose data is protected?	**Data of a Consumer**-"any person who is or may be required to pay for goods or services offered through telemarketing."	N/A- purpose of law is to control use of consumer data and conduct of telemarketers	Any person considered a recipient of commercial electronic communications.
Scope of data protected?	N/A- purpose of law is to control use of consumer data and conduct of telemarketers	N/A- purpose of law is to control use of consumer data and conduct of telemarketers	N/A- purpose of law is to control use of consumer data and conduct of telemarketers
Private Right of Action?	No, enforced by FTC, FCC and state attorneys general with civil penalties.	yes	No

US--Health	Health Information Portability and Accountability Act of (1996) (as amended by The Health Information for Economic and Clinical Health Act (HITECH)	American Recovery and Reinvestment Act of 2009 (ARRA) (section 13407)- Health Breach Notification Rule	21st Century Cures Act
Law Citation(s)	42 U.S.C. § 17937 and 17953	42 U.S.C. § 17937	
Corresponding Regulatory Citation(s)	45 CFR 160-164	16 CFR 318	
Summary		Provides requirements for notification (60 calendar day maximum) to individuals when there is a breach of security with respect to the individual's unsecured personal health records. Notice must also be provided to the media if 500 or more personal health records for residents of a state or jurisdiction are reasonably believed to have been acquired. Notice must also be provided to the FTC, either through an annual report or within 10 business days, depending upon the size of the breach.	This is not primarily a privacy law, but it requires the OCR to issue new guidance on the issue of communicating to caregivers of adults with serious mental illness to facilitate treatment. Creates a new "certificate of confidentiality" process to protect privacy in the research filed- for researchers generally not covered by HIPAA- also more guidance in connection with patient authorizations under HIPAA for research purposes. Includes req for new study to address "patient matching" and individual access to medical records
Regulated Parties	A "covered entity" is a health plan, health care provider or health care clearinghouse that engages in electronic transactions subject to HIPAA. A "business associate" collects, uses, or discloses data on behalf of the covered entity.	**Vendor of Personal Health Records**-- "any entity that maintains an electronic personal health records of "individually identifiable health information" that is "managed, shared, and controlled by or primarily for the individual." *It does not apply to HIPAA covered entities or business associates.* Also applies to **Third-Party Service Providers** of the Vendor of Personal Health Records.	
Whose data is protected?	Individuals whose data is collected, used or disclosed by or on behalf of a "covered entity" or the "business associate" of a covered entity. *(The focus on who is collecting the data rather than whose data is collected)*		
Scope of data protected?	"Protected health information (PHI)"-is an individual's health information, including demographic information, that: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (I) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.		
Enforcement Authority	DOJ, Federal Attorney General, State Attorneys General		
Private Right of Action?	No		

US--Financial	Fair Credit Reporting Act (FRCA)	Fair and Accurate Credit Transactions Act of 2003 (FACTA)	Gramm-Leach-Bliley Act of 1999 (GLBA)	Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank)	The Bank Secrecy Act of 1970 (BSA)	International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (part of US Patriot Act)
Law Citation(s)	15 U.S.C. §§ 1681-1681x	15 U.S.C. §§ 1681-1681x	15 U.S.C. §§ 6801-6809, §§ 6821-6827	12 U.S.C. § 5301, §§ 5481-5603, and in laws amended (Title X); and 12 U.S.C. § 5481 note, 15 U.S.C. § 1601 note, § 1602, and § 1631 et seq. (Title XIV)		
Corresponding Regulatory Citation(s)	16 CFR 602 et seq.	16 CFR 602 et seq.	16 CFR 313 and 16 CFR 314			
Summary	The Act (Title VI of the Consumer Credit Protection Act) protects information collected by consumer reporting agencies such as credit bureaus, medical information companies and tenant screening services. Information in a consumer report cannot be provided to anyone who does not have a purpose specified in the Act. Companies that provide information to consumer reporting agencies also have specific legal obligations, including the duty to investigate disputed information. In addition, users of the information for credit, insurance, or employment purposes must notify the consumer when an adverse action is taken on the basis of such reports. The Fair and Accurate Credit Transactions Act added many provisions to this Act primarily relating to record accuracy and identity theft. The Dodd-Frank Act transferred to the Consumer Financial Protection Bureau most of the rulemaking responsibilities added to this Act by the Fair and Accurate Credit Transactions Act and the Credit CARD Act, but the Commission retains all its enforcement authority.	This Act, amending the Fair Credit Reporting Act (FCRA), adds provisions designed to improve the accuracy of consumers' credit-related records. It gives consumers the right to one free credit report a year from the credit reporting agencies, and consumers may also purchase, for a reasonable fee, a credit score along with information about how the credit score is calculated. The Act also requires the provision of "risk-based-pricing" notices and credit scores to consumers in connection with denials or less favorable offers of credit. The Act also adds provisions designed to prevent and mitigate identity theft, including a section that enables consumers to place fraud alerts in their credit files, as well as other enhancements to the Fair Credit Reporting Act. Certain provisions related to data security ("red flags" of possible identity theft) were amended by the Red Flag Program Clarification Act of 2010, Pub. L. 111-319, 124 Stat. 3457, to clarify and narrow the meaning of "creditor" for purposes of those provisions. The Dodd-Frank Act transferred most rulemaking and one ongoing study requirement under this Act to the Consumer Financial Protection Bureau, but the Commission retains responsibility for two data security rules ("red flags" and "disposal") as well as all rulemaking under the Act relating to certain motor vehicle dealers.	Title V, subtitle A, of this Act (15 U.S.C. § 6801 et seq.) requires the FTC, along with the Federal banking agencies and other regulators, to issue regulations ensuring that financial institutions protect the privacy of consumers' personal financial information. Such institutions must develop and give notice of their privacy policies to their own customers at least annually (except where exempted under section 75001 of the Fixing America's Surface Transportation Act (FAST Act), Pub. L. No. 114–94, 129 Stat. 1787, codified at 15 U.S.C. 6803(f)), and before disclosing any consumer's personal financial information to an unaffiliated third party, and must give notice and an opportunity for that consumer to "opt out" from such disclosure. Under the Dodd-Frank Act, this rulemaking authority transferred to the Bureau of Consumer Financial Protection (except with respect to certain motor vehicle dealers), but the FTC continues to have enforcement authority. Subtitle A also requires the FTC and other agencies to issue regulations for the safeguarding of personal financial information; this authority did not transfer. The Act also limits the sharing of account number information for marketing purposes. Subtitle B of Title V (15 U.S.C. § 6821 et seq.) prohibits obtaining customer information of a financial institution by false pretenses. The FTC enforces these provisions with regard to entities not specifically assigned by the provision to the Federal banking agencies or other regulators. Also, Sections 131-133 of the Act (15 U.S.C. §§ 41 note; 12 U.S.C. §§ 1828b, 1849) clarify the application of the FTC Act and other FTC statutes to subsidiaries and other affiliates of depository institutions, and provide for certain interagency information sharing.	Title X of this Act creates a new Bureau of Consumer Financial Protection within the Federal Reserve Board as a new supervisor for certain financial firms and as a rulemaker and enforcer against unfair, deceptive, abusive, or otherwise prohibited practices relating to most consumer financial products or services. The Act transfers most of the FTC's rulemaking authority and one study requirement to the Bureau but the FTC retains all of its enforcement authority and some rulemaking authority. The Act further provides for FTC/Bureau coordination regarding certain rulemaking and enforcement activities. The Act provides authority for each agency to enforce some of the other's rules with respect to consumer financial practices. The Act also authorizes FTC rulemaking for certain motor vehicle dealers under standard Administrative Procedure Act procedures rather than the procedures set forth in the FTC Act. In addition, the Act amends the Electronic Fund Transfer Act (a) to provide for limitations on interchange transaction fees; (b) to prohibit exclusive payment networks and routing restrictions for debit cards; (c) to limit the restrictions that credit and debit card networks may impose on retailers regarding discounts or transaction amount limits based on form of payment, and (d) to provide standards for remittance fee practices. It also provides for improved financial disclosures, including integration of mortgage disclosures under the Truth in Lending Act and the Real Estate Settlement Procedures Act. Title XIV of the Act amends the Truth in Lending Act, the Equal Credit Opportunity Act, and other consumer financial laws to prevent mortgage-related abuses and to improve availability of responsible, affordable mortgage credit. It addresses compensation-based incentives; inappropriate steering, discrimination, and other abusive, unfair, deceptive, or predatory practices; minimum federal lending standards; high-cost mortgages; mortgage servicing; and appraisals. Title XIV provides a new enforcement role for the FTC regarding home appraisals.		
Regulated Parties	1. Consumer Reporting Agencies 2. "Users" of consumer reports 3. "Furnishers" of info to CRA's 4. Companies that extend credit to consumers (regardless of use of consumer reports)- with regard to "Red Flag" program.		applies to "financial institution"- (securities, insurance, banking)-entity that engages in following activities: 1) lending, exchanging, transferring, investing for others, or safeguarding money or securities; 2) insuring guaranteeing, or indemnifying against loss or ohar or providing annuitiees, or acting as a principal, agent or broker for purposes of the foregoing; 3) providing financial, investment, or economic advisory services, etc.			
Whose data is protected?						
Scope of data protected?			"Nonpublic personal information"- personally identifiable financial information provided by a consumer (excludes publicly available information)- includes lists derived from any nonpublic personal information (consumer means individual who obtains services or their legal representative)			
Rule-making authority	Consumer Financial Protection Bureau (CFPB)	Consumer Financial Protection Bureau (CFPB)	Consumer Financial Protection Bureau (CFPB) and SEC			
Enforcement Authority	CFPB shares with FTC and banking regulators	CFPB shares with FTC and banking regulators	FTC	CFPB shares with FTC and banking regulators		
Private Right of Action?						
Disclosure Requirements			opt-out (6802)-clear and conspicuous disclosure, consumer opportunity to not disclose, and explanation of non-disclosure (exception third party performing services for or functions on behalf of the institution (such as marketing) that is fully disclosed to consumer, and under a contractual agreement requiring confidentiality.			
marketing-specific limitations			no account number may be shared (exception			
notes			exceptions to opt out and no account # sharing: 1) to effect or enforce a transaction/service a financial product/maintain the consumer's account requested or authorized by the consumer; 2) to maintain or service an account with the institution or another entity under a private label credit care program; 3) at consent or direction of consumer; 4) to protect info; 5) to provide info to insurance rate advisory organizations, guaranty funds or agencies; 6) required by law; 7) to consumer reporting agency in accordance with the FCRA; 8) sale of business concerning consumers of the business unit.			
Privacy Policy			1) required at time of establishing a customer relationship and annually (unless not changed or only provides non-public personal information under an exception to the opt-out or general exceptions to disclosure prohibitions. (model provided- safeharbor applies)			
Relation to State laws			shall not supersede any state rule, except to the extent that such statute/rule/reg/etc. is inconsistent with the provisions (and then only to the extent of the inconsistency)			

US--Online Activity	Children's Online Privacy Protection Act of 1998 (COPPA)
Law Citation(s)	15 U.S.C. §§ 6501-6506
Corresponding Regulatory Citation(s)	16 CFR 312
Summary	This Act protects children's privacy by giving parents tools to control what information is collected from their children online. The Act requires the FTC to promulgate regulations requiring operators of commercial websites and online services directed to children under 13 or knowingly collecting personal information from children under 13 to: (a) notify parents of their information practices; (b) obtain verifiable parental consent for the collection, use, or disclosure of children's personal information; (c) let parents prevent further maintenance or use or future collection of their child's personal information; (d) provide parents access to their child's personal information; (e) not require a child to provide more personal information than is reasonably necessary to participate in an activity; and (f) maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information. In order to encourage active industry self-regulation, the Act also includes a "safe harbor" provision allowing industry groups and others to request Commission approval of self-regulatory guidelines to govern participating websites' compliance with the Rule.
Regulated Parties	"Operators" are regulated. An "Operator" means any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that Web site or online service, where such Web site or online service is operated for commercial purposes involving commerce among the several States or with 1 or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45).
Whose data is protected?	Data of a child under age 13
Scope of data protected?	Personal information of a child under age 13. "Personal information" is defined as individually identifiable information about an individual collected online, including: (1) A first and last name; (2) A home or other physical address including street name and name of a city or town; (3) Online contact information as defined in this section; (4) A screen or user name where it functions in the same manner as online contact information, as defined in this section; (5) A telephone number; (6) A Social Security number; (7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier; (8) A photograph, video, or audio file where such file contains a child's image or voice; (9) Geolocation information sufficient to identify street name and name of a city or town; or (10) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.
Private Right of Action?	No

US--States	State Unfair and Deceptive Acts and Practices (UDAP) statutes	State Data Security Laws* (excludes CCPA other 2019 updates)	State Data Breach Statutes	State Spam Laws	California Consumer Protection Act (CCPA)
Resources/Links to Laws from the National Conference of State Legislatures (NCSL)	http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx	http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx	http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx	http://www.ncsl.org/research/telecommunications-and-information-technology/state-spam-laws.aspx	N/A- See the CA Attorney General's web page for resources: https://oag.ca.gov/privacy/ccpa
Summary:	These laws either specifically prohibit false or misleading statements in privacy policies, or may be used to pursue companies that provide false or misleading information about use of data to consumers.	A variety of laws that provide requirements specific to a company's online services/presence- may require companies to provide specific privacy notices	Protects personally identifiable information. While the terminology and definition differs by state, it is frequently a first and last name (or first initial and last name) along with some other piece of identifying information, such as a date of birth, driver's license number, passport number, and so on. Breach notification laws incentivize companies collecting data to protect it (encryption and other reasonable procedures) in order to prevent the trigger of notification to customers/ regulators/ law enforcement	Limits unsolicited email advertisements	Focuses upon providing an individual a right to control and transparency with regards to their own data. A California resident (currently including any consumer, including employees, will have a right to ask for a disclosure of data collected, used and dislcosed over the prior 12 months