Attention Franchisors

Beware and Avoid the Myths about Data Privacy & Security

Data breaches and compliance failures continue to threaten companies and put individuals' personal identities, payment card data, finances, and medical information in jeopardy. For companies that experience those breaches, reputational harm can have a significant impact on their business and brand reputation. This is true in most industries, many of which operate under the franchise model. Lack of attention to this issue by a franchisee can hurt not only the franchisee, but also the brand of the franchisor, particularly when the business is one that maintains substantial amounts of personal information belonging to employees and customers. However, perceptions about risk can inhibit appropriate action. Some of those perceptions derive from common myths about data security that all companies, including franchisees, should avoid.

Myth #1: Our franchisees are too small to be a target.

The size of a company, whether measured by annual sales volume, number of employees, locations or certain other metrics, is not always the best measure of data risk. A small medical transcription company with 8-12 employees could easily maintain sensitive personal information on thousands of individuals. A neighborhood restaurant can process credit card data for hundreds of customers every week. This coupled with the perception (reality) that the business does not have strong safeguards, may present an attractive target for an outsider, as well as from the inside of the organization.

This point was made clear in a recent L.A. Times article, and should not be overlooked. Certain small businesses may be even more likely to be targets than larger organizations, even if their breaches do not make national headlines. These companies are viewed as having significant amounts of personal data, with less sophisticated safeguards in place and fewer resources to react to an attack.

> ***"But for every high-profile case, there are dozens of threats to confidential data held by everyday enterprises."***
>
> ***--L.A. Times***

Myth #2: We are located in State X, and laws in other states do not apply to us.

When it comes to certain data privacy and security requirements, state laws are important, but consumer personal information enjoys significant protection by the Federal Trade Commission (FTC), as well. The FTC regularly enforces the requirements that businesses not engage in unfair and deceptive trade practices,. These include those practices related to consumer personal information, such as the statements companies have on their website describing the steps they take to protect the personal information of the customers visiting their sites.

Businesses, however, cannot look solely to federal law and the state laws in which they are located. Franchisees often have multiple locations with employees and customers who reside in a number of states, even if the franchisee does not have locations in those states. In addition, some states' data protection laws are being applied extra-territorially.

For example, the Massachusetts data security regulations (201 CMR 17.00) set forth

extensive privacy and security requirements that apply to companies that "own or license" personal information about Massachusetts residents. According to the regulations, the term "own or license" refers to circumstances where a company: ***receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment***. Thus, a business that maintains personal information concerning a Massachusetts resident arguably must comply with those data security regulations, even if the business does not have a location in the Bay state or does not do business in the state.

For this reason, like other businesses, franchisees need to look closely at the kind of personal information they maintain, as well as the state(s) of residency of the individuals to whom the information relates, in order to have a more complete understanding of their obligations.

Myth #3: Our franchisees own the data, and they have the reporting obligations.

It is true that all of the 47 state data breach notification laws provide that the obligation to notify affected individuals rests with the entities that own the personal information. It also may be true that the data is owned by the franchisee, of course, that would depend on the particular business model, who the information breached is about (employee or customer) and franchise relationship.

Entities that maintain personal information and discover a breach of that information must notify the owner(s).

The determination of which entity owns the personal information may not always be an easy one. But, either way, if a franchisee experiences a data breach pertaining to the personal information of its customers, it will have notification obligations and how it responds to those obligations could have significant impact on the brand and other franchisees. Frequently, the investigation and response to the incident requires coordination between the franchisee and the franchisor. Determining what happened, who will provide the notice, what the notice will say, whether to provide credit monitoring, and so on, all can cause significant delays in the notification process, particularly when two or more entities are involved and where their interests many not be exactly aligned.

Myth #4: We have a privacy policy in our handbook and require strong passwords, so we are good.

Having a well-drafted handbook policy and a requirement for strong passwords is a good start. But those two items by themselves are insufficient to satisfy just about any of the data security standards required under federal or state law. In states such as California, Connecticut, Florida, Maryland, Massachusetts, and Oregon, a written information security program (WISP) in one form or another is required. Although the FTC has not articulated detailed data security standards, a comprehensive WISP covering customer and employee information will be a good step toward compliance.

For many franchisees that handle payment cards, PCI compliance is required. Depending on the manner and volume of payment cards processed, the business can have significant PCI obligation. Note, however, that those obligations extend only to the payment card data, and most businesses leave it there. However, those same businesses also have large amounts of other customer data – such as marketing information and lists – that warrant similar protections. So, **PCI compliance alone, like a handbook privacy policy, is not sufficient.**

WISPs start not with policies, but assessments. That is, even before an organization puts pen to paper or finger to key to create a policy or policies, it must assess a number of factors concerning the risk the personal information it maintains poses. This includes learning more about the kinds of personal information the company maintains, who has access to it, how and where is it being stored, along with a number of other considerations. At that point, the company is in a better position to address the administrative, physical, technical and

organizational risks to that information in the form of policy…a WISP.

A WISP can be a competitive advantage by providing comfort to existing and potential customers concerning the safeguarding of personal information.

Depending on the business, for many franchisees a WISP can be a competitive advantage by providing comfort to existing and potential customers concerning the safeguarding of personal information. For example, potential customers of a document destruction franchise might be more likely to select that company because it touts its privacy and data security practices. A WISP also will better position a company when defending claims related to a data breach, help the company manage and safeguard critical information, and may even avoid whistleblower claims from employees.

Myth #5: Our IT Department is on top of this.

No doubt, an organization's IT Department is critical to the process of safeguarding all of the organization's information assets. However, leaving that responsibility solely in the hands of IT personnel can be problematic for a variety of reasons:

- The increasing complexity of IT systems often makes it very difficult for upper management to understand an organization's needs and whether its IT department is addressing those needs or has the expertise to do so.
- Putting data privacy and security in the silo of an IT department may stifle collaboration among other departments, making it difficult to identify risks as well as solutions.
- IT departments may not be in a position to keep up to date with legal developments or know the best way to apply them.
- Fearing discipline, IT departments may not be as quick to address data incidents or may be too aggressive in downplaying risk of harm.

Data privacy and security is an enterprise-wide issue that requires the involvement of key stakeholders in the organization and possibly coordination with the franchisors' systems and IT teams.

Myth #6: Our insurance covers these situations.

Like many other risks, information risk can be addressed in part through insurance. Increasingly, carriers are developing products designed to deal with personal information risk, and specifically data breach response. Acquiring this kind of coverage certainly should be considered by any organization as part of its plan to address information risk.

But, don't assume your current policies will cover you in the case of a data breach. When a company claimed data breach coverage under its commercial general liability policy, a New York court disagreed. However, faced with similar claims under a similar policy, a U.S. District Court for the Central District of California found coverage existed under the policy.

Thus, companies have to be careful about understanding the coverage they have and the coverage they select; they should be working closely with their brokers and appropriate counsel.

Do not assume your current policies cover data breaches.

Summary

What franchisors may think of as fact is really fiction, for there are multiple myths with regard to data breach risks and responsibilities. The personal data that both franchisors and franchisees maintain requires them to take certain precautions. It is

important to realize that small firms are being targeted as much, if not more, than large ones. It is critical to examine the states of residence of those in the firms' databases. franchisees are responsible for notification just as much as the customers themselves. A Written Information Security Program (WISP) should be incorporated into company policies. Organizations should not rely solely on their IT department for breaches. They should examine their insurance policy and acquire the appropriate protection, if needed. By debunking these myths, franchisors can see the truth and take the proper action.

About the Author

Joe Lazzarotti is a partner with the Jackson Lewis law firm and head of its Privacy, eCommunications and Data Security Practice Group.