The Soul of Franchising

October 14-16, 2015
Sheraton New Orleans Hotel New Orleans, LA
DATA BREACH: NOW WHAT?

Erin Nealy Cox
Stroz Friedberg

Jim Goniea
Wiggin and Dana LLP

Genevieve Beck
International Dairy Queen, Inc.
Agenda

• Cyber Threat Environment
• Breach Preparedness
• Case Scenario
• Data Breach Incident Response
• Legal Landscape
• Questions
Cyber Threat Environment
Threat Landscape

December 2013

Target
- 40 million credit cards & 70 million customer records
- 150 tax returns
- 3 million customers
- 145 million users
- 1.3 million SSNs
- 33 restaurants
- 56 million cards
- 76 million households and 7 million small businesses
- 800k employees
- IP theft and sensitive info disclosure
- 48k government employees
- $1 billion ATM theft
- 11 million medical and financial records

1.1 million credit card
- 500k users
- 900 citizens
- 50k drivers
- 1.6k users
- 2.8k patient records
- 5.4 million patient records
- 25k federal employees
- 330 locations
- 210 stores
- 1.2 million payment cards
- 80 million patient records

March 2015
Cyber Threat Environment

“We face sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas – things of incredible value to all of us.”

Statement of FBI Director James B. Comey, Jr., Senate Judiciary Committee, Oversight Of The Federal Bureau Of Investigation, at 4 (May 21, 2014)
Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"

EXECUTIVE ORDER

---

BLOCKING THE PROPERTY OF CERTAIN PERSONS ENGAGING IN

SIGNIFICANT MALICIOUS CYBER-ENABLED ACTIVITIES

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,
Breach Discovery

2015

31% Discovered Internally
Down from 33% in 2014

69% Externally Notified

M-Trends “A View from the Front Lines” 2015 Report
Time from Earliest Evidence of Compromise to Discovery of Compromise

205

median number of days that threat groups were present on a victim’s network before detection

24 days less than 2013

Longest Presence: 2,982 days

M-Trends “A View from the Front Lines” 2015 Report
2015 Ponemon Study (cite to this 2015 Cost of Data Breach Study: Global Analysis, Ponemon Institute).
Breach Preparedness
What’s On Your System?

• What types of sensitive data exist on your System?
  – PII
  – Credit card information
  – Trade secrets
  – Regulated data
What is PII?

- Data that can be used to distinguish or trace a person’s identity
- Data that is linked or linkable to an individual
- Legal definition may vary by jurisdiction
Mapping Your System

• What are the entry and exit points?
• Where is data stored?
  – Is sensitive data segregated?
  – What security measures are in place?
  – Who has access?
• How often is this information updated?
Who’s On Your Team?

• Executive leaders
• Information technology & security
• Legal
• PR
• HR
• External consultants?
Cyber Insurance

• What should be covered?
  – First party loss
  – Third party loss

• What is typically not covered?
Contract Review

• What do your contracts say?
  – Franchise agreements
  – Ancillary agreements
  – Operations manual
  – Public statements concerning privacy
  – Vendor agreements
Other Contingency Planning

• Pre-Selection of third party incident responder
• Evaluation of key business continuity measures
  – Can your business continue to operate in a data breach environment?
  – Can you take segments of your business off-line and still function?
Case Scenario
Case Scenario

• Company is notified by local PD in an area with a franchise that there are fraud reports relating back to one store.
• Company starts an investigation but finds nothing unusual.
Case Scenario

• Several days later the Company is notified by a processor that MasterCard and Discover are reporting to it possible card-present fraud levels above their thresholds at 10 different locations (not including the one previously investigated). No official reporting by the card brands has occurred.
Case Scenario

• A week later US Secret Service calls to report that some information tracing back to the Company may have been located on a server that was recovered in a search warrant. They will not give the Company any information other than to say that the Company needs to monitor its VPN (remote) access.
Case Scenario

• Company is now engaged in an investigation but has nothing to report in terms of anomalies.

• PR gets a call from Brian Krebs at 4:41 pm on a Friday. He has “reliable sources” that tell him the Company has been breached and wants a comment from the Company.
Data Breach Incident Response
First 24 Hours

At what point does the Company:
• Activate breach response team?
• Determine its breach response plan?
• Communicate with executive team?
• Communicate with employees?
• Communicate with franchisees?
• Communicate with media?
Next Few Days

When should the Company:

• Retain forensic investigator?
• Retain outside legal counsel?
• Communicate with insurers?
• Review potentially applicable laws?
• Review potentially applicable contracts?
Next Few Months

When and how should the Company:

• Notify consumers?
• Notify governmental and other authorities?
• Establish a toll-free number, contract with call center and/or otherwise prepare to respond to consumer inquiries?
• Prepare for potential litigation?
Legal Landscape
Legal Landscape

- FTC enforcement
- State law
- Private actions
- Credit card companies
FTC Enforcement

• *Wyndham* - 3rd Circuit confirms that FTC has jurisdiction over cybersecurity matters under the “unfairness” prong of section 45(a)
  – Failure to take reasonable measures
  – Misrepresenting state of security measures
• Fair notice issue
State Law

- Almost all states have cyber-breach statutes
- Apply when a resident’s PII is compromised
- One incident may lead to requirement to comply with multiple state laws
- Lack of uniformity
  - Timing and notice requirements
  - Civil penalties for non-compliance
Private Actions

• Article III standing remains threshold issue
  – Need to show injury-in-fact
  – Hypothetical injury not sufficient
• Statutory violation?
• Other creative theories?
Credit Card Companies

• What is PCI-DSS?
• Potential liability emanates from contractual obligations in merchant agreements with banks
• Can liability extend to franchisors for franchisee transaction?
Questions
DATA BREACH: NOW WHAT?

Genevieve Beck
International Dairy Queen
Minneapolis, MN

and

James Goniea
Wiggin and Dana LLP
Philadelphia, PA

October 14 – 17, 2015
New Orleans, LA

©2015 American Bar Association
Table of Contents

I. INTRODUCTION 1

II. PRE-BREACH PLANNING 1
   A. Identifying And Classifying Sensitive And Proprietary System Data, How And Where It is Stored, And How It Enters And Leaves The System 2
      1. Classifying And Categorizing System Information 2
   B. Other Necessary Pre-Data Security Breach Planning 5
      1. Identify A Post-Data Security Breach Response Team 5
      2. Obtain Cyber Insurance 5
      3. Review/Revise Vendor Contracts For Provisions Potentially Applicable To Data Breach 6
      4. Review/Revise Franchise Agreements And Ancillary Agreements For Provisions Applicable To Data Breach 6
      5. Review/Revise Privacy Policies And Notices Containing Representations Regarding Protection Of Personally Identifiable Information 7
      6. Interview And Pre-Select A Third-Party Information Technology Consultant 7
      7. Evaluate And Implement Key Business Continuity Measures 7

III. DATA BREACH INCIDENT RESPONSE 8
   A. THE FIRST 24 HOURS 9
   B. THE NEXT FEW DAYS 9
      1. Conduct a Forensic Investigation 10
      2. Identify Legal Obligations 10
         a. Review applicable state and federal regulations 10
         b. Review contracts such as merchant agreements and insurance policies 11
      3. Address Public Relations 11
C. THE NEXT FEW MONTHS

1. Notification 12
2. Assessment Of Response 12

IV. THE LEGAL LANDSCAPE 12

A. The FTC 13

B. State Laws and State Attorneys General Actions 14

C. Private Actions 15

D. Credit Card Companies 17

E. Assessing Litigation Risk And Minimizing Exposure 20

V. SPECIAL CONSIDERATIONS OF FRANCHISE SYSTEMS 21

A. Whose Data Has Been Compromised And Where Is It Located? 21

B. What Should The Franchise Agreement Say About Data Security? 21

C. Weighing Potential Vicarious Liability Associated With Post-Breach Actions 22

D. Mandating System Change To Prevent Future Data Breaches 23

VI. CONCLUSION 23
DATA BREACH: NOW WHAT?

I. INTRODUCTION

Many papers addressing data breach risks begin with a litany of horrors. They start by noting the ubiquitous vulnerability to the risk of theft of sensitive information in today’s computer saturated and data driven society. They then catalogue numerous examples of large, well-known international companies that have suffered data security breaches. Finally, they emphasize the dire consequences associated with inadequate data security by pointing to the millions of consumers who have been affected and the millions of dollars in fines, remediation expenses, litigation expenses and lost brand value suffered by companies that have been victimized by such data security breaches. Readers are informed that they should expect that this inevitably will happen to their company or client and that they should “be prepared.” This paper assumes that the reader is aware of the scope of the risks involved in data security breach scenarios and already is scared half to death. If you are not already concerned about the possibility of a data breach affecting your company or clients, you have been living under a rock. We are not revisiting that already well-trodden ground in this paper.

Rather, this paper is an effort to provide practical guidance to in-house and outside counsel dealing with the following real world scenario:

You have just learned that your company, or your client, has been the victim of a data security breach whereby sensitive or proprietary information, potentially including Personally Identifiable Information (“PII”) of customers or employees, has been compromised and may have been accessed by unauthorized parties.

What do you do next?

The goal of the paper is to provide a general roadmap to be referenced in the event the reader is faced with this unfortunate situation. The aim is to identify the primary factors that need to be considered when a data security breach is encountered and the sequence of actions that should be taken to address and isolate the breach, identify continuing vulnerabilities, assess legal exposures and begin the process of mitigating those exposures. Thus, the paper assumes that a data security breach already has occurred and that the reader is responsible for advising his or her company or client concerning appropriate action to take to address that event. Inherent in this assumed scenario is the recognition that the breach is likely, by its nature, to constitute a “crisis” that requires both quick thinking and decisive action while at the same time juggling numerous variables, including many “unknowns.”

II. PRE-BREACH PLANNING

The scenario addressed by this paper assumes that an actual data security breach already has occurred. However, it also assumes that the incident has not happened in a vacuum. In other words, the reader, being a diligent, proactive and responsible advisor to his or her company or client, undoubtedly previously has engaged in efforts to prepare for the possibility of a data security breach. This section of the paper identifies things a company should do in anticipation of the possibility of a data security breach to provide a proper foundation for mitigating such an event.
A. Identifying And Classifying Sensitive And Proprietary System Data, How And Where It is Stored, And How It Enters And Leaves The System

Every company should know, and fully document, the sensitive and proprietary data that exists on its computer systems. In addition, every company should know where and how that sensitive and proprietary information is stored on the system, if it is segregated from less sensitive information, what levels of security protect the information, who has authorized access to the information and what the entry and exit points within the company’s computer system are for that information. Auditing electronic systems to document this type of information may be even more critical in a franchise environment because there may be multiple locations where the same sensitive information is stored (some within the franchisor’s control and others not), the uniformity with which security measures are applied to such information may differ depending on its location, and the number of entry and exit points in the system are likely to increase.

Having this information fully documented and readily available at the time a data security breach is discovered may be one of the single most important factors in determining how quickly the breach can be effectively contained. One can imagine how disconcerting it would be for the company’s Data Breach Response Team to assemble in a conference room for the first time upon learning of a newly discovered data security breach only to realize that no one in the room has any idea of what information potentially is at risk, where that information is located in the company’s computer system or how to stop the information from being further compromised.

1. Classifying And Categorizing System Information

Sensitive or proprietary information can take many forms. Of primary concern is identifying what information exists on the company’s computer systems (or may be stored in the company’s paper files) and whether any of the information is subject to special statutorily mandated security requirements. For example, statutes such as the Gramm-Leach-Bliley Act (“GLBA”) 1 (concerning certain financial information) or the Health Insurance Portability and Accountability Act (“HIPAA”) 2 (concerning certain health information) create affirmative data security standards that must be complied with to ensure that the privacy of information concerning affected individuals is protected. Other pertinent federal laws relating to cybersecurity may include the FTC Act, the Health Information Technology for Economic and Clinical Health Act (“HITECH”), the Controlling the Assault of Non-Solicited Pornography and Marketing Act (“CANSPAM”) and the Children’s Online Privacy Protection Act (“COPPA”).

For most franchise systems, however, the relevant inquiry will be determining what PII exists within the company’s systems relating to, for example, (1) consumers who purchase products or services from franchisees or company-owned retail outlets; (2) employees of the franchisor; or (3) franchisees or their employees.

PII, as the term generally is used in U.S. privacy law, is typically recognized to be information that can be used on its own or with other information to identify, contact or locate a single person, or to identify a single person in context. For legal purposes, the definition of PII

---

1 GLBA requires financial institutions to “develop, implement, and maintain a comprehensive information security program” and additional safeguards. 16 C.F.R. § 314.3(a).

2 HIPAA requires covered entities to “[p]rotect against any reasonably anticipated threats or hazards to the security or integrity” of electronic health information. 45 C.F.R. § 164.306(a)(2).
will vary depending upon the jurisdiction. The National Institute of Standards and Technology defines PII as:

any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.³

Examples of PII include but are not limited to:

- Name, such as full name, maiden name, mother’s maiden name, or alias;
- Personal identification number, such as social security number (SSN), passport number, driver’s license number, taxpayer identification number, or financial account or credit card number;
- Address information, such as street address or email address;
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry); and
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographic indicators, employment information, medical information, educational information, financial information).⁴

PII may be stored in the company’s paper records and electronic systems as a result of the gathering of such information from (1) customers of the franchisor, franchisees, or related entities; (2) employees or persons seeking employment; (3) franchisees or persons applying to become a franchisee; or (4) various other sources. Obviously, the likelihood of harm caused by a breach involving PII is greatly reduced if an organization minimizes the amount of PII it uses, collects and stores. Accordingly, organizations should regularly review their holdings of previously collected PII to determine whether the PII is still relevant and necessary for conducting the organization’s business.

In addition to PII, other sensitive or proprietary information that may exist within the company’s paper and electronic records includes trade secrets, proprietary financial data and proprietary business data concerning the company or its business partners.


In addition to documenting the extent of potentially sensitive or proprietary information existing in the company’s electronic systems, the company should document and understand how that information enters the system, where it is stored, what security measures apply to the

⁴ Id.
information, who has authorized access and ultimately when and how the information exits the system and is disposed of or destroyed.

A franchise system may have multiple points where sensitive information can enter the system. For example, some franchisors require franchisees to use a Point of Sale ("POS") system that pushes information, such as real-time retail sales data, directly to the franchisor's main computer servers where that information is stored and subsequently accessed to, among other things, calculate gross revenues and royalties due from individual franchisees. Other franchisors may have different methods for acquiring sales data from franchisees that may include the intentional or inadvertent transfer from the franchisee to the franchisor of customer PII. PII may also enter a franchisor's electronic system via information supplied to the franchisor from its Website or in many other ways. Many times PII from retail customers is acquired and stored on a franchisor's computer servers to facilitate future advertising and marketing efforts. Regardless, it is important for a company gathering PII and other sensitive information to identify and document its sources for obtaining that information and, in doing so, identify all of the access points that potentially could be used by a hacker to infiltrate the company's computer systems.

Equally important is documenting and understanding what happens to sensitive information once it enters the company's electronic systems. Where is it physically stored? Local computer servers? Individual computer hard drives? Off-site servers? The Cloud? Does the company segregate sensitive information and customer and employee information containing PII on a computer server that is separate from the system it uses to operate the rest of its business? What security measures have been implemented to protect the sensitive information? Are appropriate firewalls in place? Is the information password protected? How frequently are users required to change their passwords? Has the company identified and recorded the identities of all individuals who have authorized access to the sensitive information? How frequently does the company update that information? What measures are taken to ensure that former employees are denied access upon termination? What happens to the electronic devices used by employees when they leave the company? Is sensitive information encrypted when being transferred from one location or device to another?

In addition, portals for the outward flow of information from the company's computer systems have to be fully assessed and documented. Are sensitive documents stored in "read only," non-downloadable form or can they easily be electronically transferred via the internet or downloaded to a disk, flash drive or other portable media device? Is the company able to identify each person who has accessed the sensitive information, the duration of the access and when that occurred?

A comprehensive audit of the company's data storage and management systems should answer all of these questions. Having this information readily accessible at the time a data security breach is discovered may be critical to evaluating how the breach occurred, what computer systems need to be disabled to isolate the breach and what remedial action is needed to quickly reconstitute the company's computer systems so that business disruptions are minimized.

Finally, but importantly, how often is documentation concerning the company's mapping of electronic data flows, storage systems and security controls updated? Technologies change rapidly and are upgraded. Employees come and go. Laws change. Companies merge with, or are acquired by, other companies. New mobile devices are deployed. Websites are revamped. New online marketing campaigns are born, fully implemented and abandoned. Business is a
dynamic enterprise. A fully realized document auditing all of the company’s key electronic systems, functions and vulnerabilities may become obsolete upon the occurrence of any of these events (and many others not listed). Accordingly, for any system documentation to be helpful when it is actually needed – that is, when a data security breach is discovered – ongoing assessments have to be performed to keep the information contained in the documentation fresh, accurate and relevant.

B. Other Necessary Pre-Data Security Breach Planning

1. Identify A Post-Data Security Breach Response Team

A company should identify and document in advance which individuals are required to participate in its response team upon the discovery of a data security breach. Ideally these individuals’ names and contact information will be recorded in a readily accessible document so that the individuals can be immediately contacted and assembled when necessary. Because response to a data security breach requires consideration of many factors, the response team necessarily will be multi-disciplined. Persons a company should consider including in any post-data security breach response team include the following:

- Executive Leaders
- Information Technology and Security
- Legal Counsel
- Public Relations
- Customer Care and Human Resources
- Law Enforcement
- External Incident Responder/Forensic Investigator

2. Obtain Cyber Insurance

Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data security breaches, business interruption and network damage. A robust cyber insurance policy can help a company weather the storm more effectively when a data security breach has occurred. Cyber insurance is widely offered today as a separate product (rather than, for example, as an add-on to a company’s errors and omissions coverage). Policies can differ considerably in their coverage. However, cyber coverage typically provides for some combination of four different components: errors and omissions, media liability, network security and privacy. Different insurers sometimes use different terminology in their cyber coverages, making it difficult to compare individual cyber insurance policies. Ideally, cyber insurance policies should cover both first-party costs and third-party costs.

Examples of first-party costs that may be covered by cyber insurance include: (1) forensic investigation of the breach; (2) legal advice to determine notification and regulatory obligations; (3) notification costs of communicating the breach; (4) costs associated with offering credit monitoring services to affected customers; (5) public relations expenses; and (6) business interruption expenses.

Examples of third-party costs that may be covered by cyber insurance include: (1) legal defense; (2) liability (i.e., settlements or damages awarded associated with the data security breach); (3) liability to banks associated with the re-issuance of credit cards; (4) costs
associated with responding to regulatory inquiries; and (5) regulatory fines and penalties (including Payment Card Industry fines).

Things that typically would not be covered by cyber insurance include: (1) reputational harm; (2) loss of future revenue; (3) costs associated with necessary improvements to the insured's technology systems; and (4) loss of value to the insured's own intellectual property.

3. Review/Revise Vendor Contracts For Provisions Potentially Applicable To Data Breach

A company should review and understand the provisions of its key vendor contracts to evaluate how those provisions might come into play in the event of a data security breach. Do the contracts expressly provide that the vendor will indemnify the company in the event that the data security breach results from a security lapse on the part of the vendor? Is the vendor required to purchase cyber insurance and name the company as an additional insured? Does the vendor contract contain affirmative representations and warranties concerning the vendor's obligations with regard to data security? Does the vendor contract address how the company's interests and business continuity will be protected in the event the vendor's business is compromised by a data security issue? The importance of these considerations is multiplied when the vendor at issue may be providing IT solutions that potentially affect the entire franchise system, such a vendor providing a POS system mandated for use by franchisees or a vendor developing proprietary software that will be implemented by all franchisees.

However, consideration of these types of cyber security issues is not limited to purveyors of technology solutions. Any third-party business partner that regularly interacts with or accesses the company's computer system might provide a back door for hackers to infiltrate the company's electronic systems. The company's contracts with vendors should reflect this vulnerability and provide adequate assurances, protections and indemnifications.

4. Review/Revise Franchise Agreements And Ancillary Agreements For Provisions Applicable To Data Breach

Remarkably, despite the fact that news stories reporting on major data security breaches have become a nearly daily occurrence, many franchise agreements continue to fail to expressly address the allocation of risks and responsibilities between the franchisor and franchisee in the event that a data security breach affects the franchise system. A franchisor should carefully review the terms of its franchise agreements to determine which provisions are likely to be implicated in the event of a data security breach. Does the franchise agreement provide for appropriate indemnifications in the event of a data security breach? Is the franchisee required to purchase cyber insurance? Does the franchise agreement or the operations manual identify how the franchisee is to store customer PII or the levels of security that the franchisee must employ to protect customer PII? Does the franchise agreement or the operations manual address the circumstances in which PII should be retained, disposed of or destroyed? Do ancillary contracts between the franchisor and franchisee, particularly those relating to the licensing of proprietary software, contain appropriate waivers or disclaimers? Does the franchise agreement mandate the franchisees' cooperation in the event of a data breach? In short, if the franchisor has not already done so, it should review all of the relevant documents defining the relationships with its franchisees to evaluate the parties' respective rights and obligations in the event of a data security breach affecting the entire system.
5. Review/Revise Privacy Policies And Notices Containing Representations Regarding Protection Of Personally Identifiable Information

The Federal Trade Commission regularly takes the position that a company’s failure to comply with representations and assurances made in a posted privacy policy constitutes a deceptive trade practice under the FTC Act. The same is true of state attorneys’ general and other enforcement agents charged with enforcing federal and state consumer protection laws. As such, companies should regularly review any privacy policies and notices that may contain assurances or representations regarding the sharing or protection of personally identifiable information and other types of data and make sure that their actual practices are consistent with their policies.

Companies should anticipate that their privacy policies will be scrutinized in the event of a breach. Providing assurances to consumers that the company takes “reasonable measures” or uses “industry standard practices” to protect consumer data can result in fines, penalties and other damages, along with injunctive relief and other oversight, if it turns out that the company’s practices fail to actually achieve those standards. It is essential for companies to ensure that they are not over promising or making unnecessary representations or assurances. Regular review is critical because the types of data a company collects and maintains, and the way it uses data, as well as industry best practices, inevitably will change over time.

6. Interview And Pre-Select A Third-Party Information Technology Consultant

Data security breaches require prompt and decisive action. The middle of a data security crisis is the wrong time to be identifying and interviewing technology consultants to help alleviate the crisis. Ideally, prior to a data security breach taking place, the company should already have established a relationship with a reputable third-party information technology consultant who can be called upon on short notice to help the company assess and isolate the breach, determine the extent of the data compromised and provide a comprehensive report concerning the breach to the company’s management. In addition, by negotiating the terms of that relationship in advance, before the company is in crisis mode, the company is likely to be able to achieve more favorable contract terms and conditions than it might get after the data security breach has occurred and the company is desperate for immediate action. Simply stated, given the high likelihood of data security breaches occurring in the life of any company, and the foreseeability of the need under such circumstances to employ the services of an information technology specialist to help navigate the crisis, it simply makes sense to plan ahead by negotiating the terms of that relationship in advance.

7. Evaluate And Implement Key Business Continuity Measures

Could your company, or your client, continue to do business if suddenly required to turn off all of its computers and disconnect from the Internet? It’s a scary prospect. However, it could be the question the company needs to immediately address in the face of an ongoing data security breach that it cannot isolate. A savvy company will consider this issue in advance and provide for appropriate contingencies. Is sensitive data appropriately segregated within the company’s computer system, so that servers containing the sensitive information could be disconnected and taken off line without materially affecting the remainder of the company’s computer system? Are the company’s telephone systems so fully integrated with the computer system that a compromise of the computer system would jeopardize the ability of the company
to communicate with the outside world? Could the telephone systems and computer systems be decoupled and remain independently functional? Does the company have redundancies in its computer systems that would permit it to unplug compromised servers and replace them with fresh, uncompromised computer servers efficiently and effectively?

Planning ahead for a data security breach means anticipating disruption in the key systems that are used by the company to communicate both internally and with the outside world at a time when the need for uninterrupted ability to communicate is paramount. The most effective planning assumes the worst and hopes for the best. In the data security breach context, assuming the worst means assuming that all of the company’s major computer and communications systems are compromised and need to be shut down to prevent further data loss, evaluated, de-bugged if possible or replaced, at a time when it is the least convenient for that to occur. A comprehensive pre-data security breach plan will consider this scenario and consider alternative methods for ensuring that the company will continue to be able to operate and that communications with franchisees, employees and the public will remain uninterrupted.

III. DATA BREACH INCIDENT RESPONSE

A company may be alerted to a data security incident or potential data breach in any number of ways. It may detect an issue internally or it may receive a call from federal or local law enforcement, the media, a consumer, a vendor, a contractor or, in the case of a franchise system, from the franchisor or a franchisee. After being alerted to a possible breach, the company likely will face a multitude of unanswered questions and important decisions will have to be made.

When first alerted to a possible data security incident, it often is not at all clear whether the report of the incident is legitimate. Moreover, not every data security incident constitutes a breach. Even if an actual data security breach is confirmed, the source, cause and extent of the issue may not be readily apparent. This is particularly true in a franchise system, where potential sources for data leakage can include not only the franchisor’s own systems, networks, employees, vendors and other vulnerabilities but also those of each individual franchisee. Yet it is absolutely critical for the company to quickly identify and contain the issue.

As Luis Aguilar of the US Securities Exchange Commission said during his speech at the Cyber Risks and Boardroom conference held in June 2014:

... the primary distinction between a cyber-attack and other crises that a company may face is the speed with which the company must respond to contain the rapid spread of damage. Companies need to be prepared to respond within hours, if not minutes, of a cyber-event to detect the cyber-event, analyze the event, prevent further damage from being done and prepare a response to the event.

So where does one start when a data security breach is discovered?

A. THE FIRST 24 HOURS

The first 24 hours after confirmation of a data security breach is a critical period. If the company has a pre-determined breach response plan, now is the time to implement it by alerting members of the company’s breach response team, including in-house counsel. If the company does not have a pre-determined response plan, it will need to determine the individuals from the company who should be involved, pull that team together and have them build out a plan as they go. A franchisee that discovers a data security breach should immediately alert its franchisor so that the franchisor is aware of the breach and can provide appropriate assistance with the investigation, containment and response, as well as manage ensuing public relations and media inquiries.

The response team should record the date and time of discovery of the breach, as this may be important in the future in assessing (and perhaps defending) the character of the company’s response. Within the first 24 hours after confirmation of a breach, the response team should meet to review any pre-established breach response plan and adjust it based upon the specifics of the particular breach and any information known at the outset. They should assess what they know and don’t know about the breach, determine priorities and risks, and consider whether and when to consult outside legal counsel, retain and mobilize technical and forensics experts and notify and involve law enforcement. If loss of payment card data is suspected or confirmed, the company may also have an obligation to immediately notify the card brands and/or the company’s acquiring bank or processor, and the response team should consider when and how to do so.

At this stage, the response team’s greatest priority will be determining how to contain the data breach. If the source of the breach and steps needed to contain it are known, the company will want to immediately take the steps necessary to stop any additional loss of data. This might involve immobilizing devices, implementing anti-virus or anti-malware programs capable of deactivating and quarantining viruses or malware, disconnecting systems from the network or changing locks, codes, encryption keys and passwords. If criminal activity is suspected, the company should consider how any actions it may take might impact law enforcement’s ability to identify, capture and convict the criminals. If appropriate, the company should first consult with law enforcement.

If the source and extent of the issue are not known, the team should consider whether there are any immediate steps that can be taken to stop or at least minimize additional data loss while the source and extent of the issue are investigated. The team should determine who to involve in an investigation and how best to document and preserve relevant information, as well as how and when to designate reports and communications as attorney-client privileged or attorney work product. Team members should also start thinking about when and how to communicate with other key stakeholders, including the executive team, shareholders, employees, franchisees, vendors and other key business partners and the public.

B. THE NEXT FEW DAYS

With an initial response plan in place, the team’s priority over the next few days will undoubtedly be to evaluate and determine the full extent and cause of the breach and to fix the issues that allowed the breach to occur. Team members will also need to identify their legal obligations, determine deadlines for compliance with those obligations, and develop and implement a communications and public relations plan. The company may need to hire and
consult with outside experts to assist with these steps, including technical and forensics experts, experienced legal counsel and public relations professionals.

1. **Conduct a Forensic Investigation**

   Particularly if the cause and extent of the breach remain unknown, a company should seriously consider hiring outside forensics experts to assist with an investigation. Forensics experts can assist with determining the cause of the breach, the types of data that were compromised, how to contain the breach, and the start date and end date of the breach. All of this information is critical to determining what future actions may be necessary for the company. Forensics experts can also provide recommendations on how to protect against future compromises.

   The company should work with its internal and/or external technical experts to identify and delete any hacker tools, such as malware or skimming devices that may have caused the breach. If servers and devices cannot be debugged, they should be replaced. The company will also need to determine and review all affected systems and networks to close any gaps that might have allowed the breach to occur, such as a firewall that is open or not whitelisted (i.e., configured to allow access only to sites known and necessary for the business), use of insecure passwords or failure of other security features.

   The company will need to determine the extent of the breach, including the time, duration and affected systems, networks and locations. It will also need to assess the types of data that were compromised, i.e., whether it was payment card information or other PII. It will need to determine what happened to the data: was the data deleted, modified, viewed or copied, was it encrypted or unencrypted, and the number of people that may have been affected. If possible, the company should begin to align compromised data with customer names and addresses for purpose of sending notifications.

2. **Identify Legal Obligations**

   a. **Review applicable state and federal regulations**

      Depending on the nature of the breach, the company may have legal obligations to notify affected individuals, regulators and attorneys general. As described in more detail below, there exists today a patchwork of federal, state and local laws and regulations that govern data security issues. Nearly every individual state, as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands, each has its own laws requiring companies to notify individuals of security breaches involving personal information and, in some cases, imposing obligations on companies to safeguard PII relating to consumers. Companies may also have an obligation to notify regulators or state attorneys general under applicable laws.

      In addition to the specific breach notification and data security laws, a company may have obligations under industry-specific laws such as the GLBA, the Privacy Act, HIPAA, Sarbanes-Oxley, the Fair Credit Reporting Act, COPPA, the Electronic Signatures in Global and National Commerce Act, the Federal Information Security Management Act and the Homeland Security Act.

      Internationally, more than a dozen other countries have enacted mandatory breach notification laws that require companies to notify individuals and/or government regulators in the event of a data breach and other countries have issued voluntary data-breach notification
guidelines. More than 90 countries now have comprehensive privacy laws, most of which are more comprehensive than those of the United States.

In the days following a data breach, a company must determine which of these laws is triggered and what they require the company to do. This is potentially a large and complicated undertaking, as individual state privacy laws typically are triggered by the fact that PII concerning a consumer residing in the state has been implicated, regardless of whether the actual data security breach occurred somewhere else. For franchise systems serving nationwide and international customer bases, the number of privacy laws potentially implicated by a system wide data security breach may be overwhelming. Accordingly, the company will likely want to hire experienced legal experts to help them understand their legal obligations and prepare for possible regulatory action and claims.

b. **Review contracts such as merchant agreements and insurance policies**

In addition to notification obligations that may exist under applicable law, companies may also have contractual obligations to notify third-parties in the event of a data security incident or breach. For example, if the company accepts and processes credit cards, they will undoubtedly have an obligation under their merchant or card processing agreement to notify the credit card companies. Franchisees may have a contractual obligation to notify their franchisor and vendors may have an obligation to notify their customers. Companies will also be obligated to notify their insurers in order to trigger possible coverage.

Contractual reporting obligations may include specific timeframes and procedures. It is therefore essential that the company quickly determine all entities to whom they may have a contractual reporting obligation to ensure they are not in breach.

3. **Address Public Relations**

Data breaches are news and any sizeable breach will undoubtedly make headlines. In addition, news of a breach, even a smaller one, can travel fast and far through social media and the Internet and potentially may have far reaching and detrimental effects on a franchise system’s brand image (and consequently, sales). In the days following a breach, the company needs to develop and implement a public relations and communications strategy and communicate that strategy to affected stakeholders, including franchisees, employees, key business partners and vendors. The franchisor likely will want to coordinate and manage public relations in order to avoid potentially conflicting, inaccurate or damaging reports across the system. The team should consider how to work with franchisees to accomplish that goal so that communication to the public is consistent and speaks with one voice. The company may want to retain and work with an outside public relations company that is experienced in responding to data security breach incidents.

In summary, after the company’s computer systems have been secured, the data breach isolated and the risk of future data leakage stemmed, the next few days will be a period of assessment and communication with affected parties. The company will need to determine what data was compromised, the extent of the compromise (both in terms of content and duration), the system deficiencies that allowed the compromise to occur, and the actions that will need to be implemented to address the consequences of the data security breach, both legally and as necessary to mitigate negative consequences to the brand’s image.
C. THE NEXT FEW MONTHS

1. Notification

Over the next few months, the company will need to determine exactly who needs to be notified, when they need to be notified and how they must be notified. Early on, the company will need to begin the process of linking compromised data to the identities and contact information of affected individuals. If the company has contact information for the affected individuals and can notify them directly, it may be obligated to do so. If the company is not able to directly notify those affected, it may be required to satisfy its notification obligations through substitute notification, which potentially could involve issuing a national press release and/or posting pertinent information concerning the data security breach on the company’s website.

Whether direct or substitute, the notification should include a well-crafted description of what happened, the type of data that was compromised, and the actions the company has taken to stop the further loss of data. Companies also generally include information on what they are doing to assist affected persons and what those persons can do to help themselves. Depending on the circumstances, the company may be required to or may voluntarily elect to offer affected individuals free credit monitoring services or identity theft protection services.

Also, depending upon the number of affected individuals and the company’s own internal resources, the company may want to consider setting up and implementing a call center to field calls and answer questions from consumers and other interested parties. The call center could be staffed with the company’s own employees or, alternatively, could be outsourced to a third party whose employees have been specially trained to respond to consumer inquiries concerning the data security breach. The company may want to establish a toll-free number that is dedicated to calls related to the data security breach. Regardless, the company will want to ensure that the individuals taking calls and fielding questions are knowledgeable about the incident and trained to respond appropriately to provide consistent and accurate information. The company should consider the types of inquiries and questions they are likely to get and develop scripted responses for those fielding calls. The company may also want to consider posting a set of frequently asked questions with responses on its website.

2. Assessment Of Response

A company should not consider the process of dealing with a data security breach to be completed until it has conducted a comprehensive assessment of the underlying mechanisms that allowed the breach to occur, the security measures that have been implemented to prevent another incident from occurring in the future and has conducted a critical evaluation of the company’s response efforts to identify how things could have been done more efficiently, more effectively and more economically. Every crisis is also an opportunity. A data security breach provides the company with an opportunity to evaluate what went wrong and to take the actions necessary to prevent such events from occurring in the future.

IV. THE LEGAL LANDSCAPE

At the present time, in the United States there is no one law that addresses the obligations of an entity that has experienced a data security breach. National preemptive data breach legislation continues to languish at the federal level. Thus, enforcement of data privacy issues remains decentralized and continues to take place through a tangled web of laws, regulations, contractual obligations, common law rights, industry standards and enforcement
authority. These varying sources of obligations and legal enforcement authority frequently overlap and rarely are preemptive of one another. Not surprisingly, this results in considerable confusion concerning what laws will apply in the event of a data security breach, which individuals or entities have the right to enforce post-data breach obligations and what obligations must be satisfied (and exposures evaluated) by a company that has experienced a data security breach.

At the present time, the most active enforcers of post-data breach obligations and liability include the Federal Trade Commission (the “FTC”), various state attorneys general, private class action attorneys and major credit card companies.

**A. The FTC**

On the federal level, for U.S. businesses the FTC is the default federal authority for enforcing privacy and data security requirements. Section 5 of the Federal Trade Commission Act empowers the FTC to prevent persons from engaging in unfair and deceptive acts or practices in or affecting commerce. In addition, the FTC Act grants authority to the FTC to prescribe rules that specify which acts or practices constitute unfair or deceptive acts and to commence civil actions in federal district court against violators of the standards. The FTC has interpreted its mandate as extending to situations involving data privacy and security.

In addition, courts have specifically recognized that the FTC has authority to enforce data security under its “unfairness authority.” In June 2012, the FTC filed suit against Wyndham Worldwide Corporation alleging that (1) the breach of its franchisees’ computer systems, giving intruders access to Wyndham’s customers’ personal and financial information, constituted an unfair business practice, and (2) Wyndham made deceptive representations to consumers that it employed reasonable and appropriate security measures. Wyndham moved to dismiss the complaint. First, Wyndham argued that Congress’s passage of various laws that touch on data security (such as the GLBA and COPPA) effectively limited the FTC’s authority to regulate data security issues. The court rejected Wyndham’s argument, holding that “the FTC’s unfairness authority over data security can coexist with the existing data-security regulatory scheme.” Second, Wyndham argued that the FTC had failed to promulgate sufficiently clear regulations in violation of the due process clause. The court rejected this argument as well, finding that the test established under Section 5(n) of the FTC Act, and the host of publically available prior FTC complaints and consent orders, collectively provided actors with sufficient notice of what constitutes noncompliant activity. The Wyndham case has been appealed to the Third Circuit Court of Appeals.

---


10 Id. at 613.

11 Id. at 621.
In the past year, the FTC has continued to aggressively pursue consent agreements related to cybersecurity and data breaches. For example, the FTC recently obtained consent decrees relating to data privacy issues from companies such as Fandango, Credit Karma, Accretive Health, Genelink and GMR Transcription Services. These settlements required the companies involved to, among other things, establish comprehensive security programs and consent to biennial privacy audits for the next 20 years.

B. State Laws And State Attorneys General Actions

Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals about data security breaches that involve the unauthorized disclosure of the individual’s PII. Security breach laws enacted by states typically have provisions regarding who must comply (e.g., businesses, data/information brokers, and government entities) definitions of “personal information” (e.g., name combined with SSN, driver’s license or state ID, or account numbers); what constitutes a breach (e.g., unauthorized acquisition of data); requirements of notice (e.g., timing or method of notice, who must be notified) and exemptions (e.g., for encrypted information).

These laws typically apply whenever PII concerning a resident of the state has been implicated in a data security breach without regard to where the company does business or the geographic location of the actual security breach. Thus, a single data breach event involving PII from individual in multiple states may obligate the company to deal with many state laws. In addition, to further complicate matters, the actual triggering events creating an obligation to provide notice to a consumer of unauthorized acquisition of the consumer’s PII vary by state. States typically require that consumers receive notification by a written letter. In certain circumstances, however, such as when individual consumer information is difficult to ascertain, notice may be provided in a substitute form, such as by electronic notice on websites, press releases and other similar methods. State laws frequently specify the information that must be included in the written notice to a consumer; however, there is no uniformity of approach among the states. Consequently, different forms of notice may be required for individuals who are residents of different states. Some state laws cover paper records in addition to electronic records, while others do not. Depending upon the extent of the breach, state laws may also impose requirements that the company involved in the data security incident notify state enforcement authorities, affected credit card companies and consumer reporting agencies.

Many of the state laws provide for an exemption from the notification requirements if the company can demonstrate that the consumer PII was encrypted and, thus, inaccessible. In addition, some states laws provide an exemption from compliance with the statute where a company maintains its own breach notification policy and the policy is consistent with the requirements of the statute. Thus, although these state laws share certain characteristics, they

---

12 id. at 636 (motion to certify interlocutory appeal granted).

13 http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. This website provides a comprehensive listing of each applicable state security breach notification statute and links to the text of each statute.

14 id.
differ from each other in enough material ways to make compliance a logistical feat when the
data security breach involves PII from a nationwide consumer database.

Concerning the timing of notification, some states permit companies to delay notification pending an investigation assessing the breach and while attempts to restore the integrity of the
data are underway. Other states require notification within a specified time period. However, even those states that permit delays in notification impose outside limits on when notification must occur after an investigation has concluded. While some states require that notice be provided "without reasonable delay," other states require notice within 45 days of a breach and may require that specified state agencies be notified of the data security breach within 10 days. Special care must be taken to evaluate and determine compliance deadlines for any states implicated by the data security breach. Since the notification timeframes under these statutes sometimes are very short, efforts must be undertaken as soon as possible after a data security breach has been confirmed to evaluate which state laws will apply.

A company that fails to comply with a state data breach notification statute may be subject to civil penalties enforced through the state's Attorney General. And state Attorneys General have not been shy about commencing investigations into data security lapses and filing enforcement actions against companies that have failed to comply with notification requirements. For example, the State of California initiated an enforcement action against Kaiser Foundation Health Plan, Inc. ("Kaiser") alleging that Kaiser had delayed notifying its employees after an unencrypted USB drive was discovered at a Santa Cruz thrift store that contained over 20,000 employee records. Kaiser ended up stipulating to entry of judgment against it and payment of $150,000 in penalties and attorneys' fees. In addition Kaiser agreed to comply with California's data breach notification law in the future, provide notification of any future breach on a rolling basis and implement additional training regarding the sensitive nature of employee records.

In the past several years, state Attorneys General appear to be expanding their focus on joint enforcement activity and multistate investigations including investigations involving franchise systems. For example, in September 2014, the Illinois Attorney General's Office announced that it was leading a multistate investigation into a data breach involving 216 Jimmy John's Franchise LLC's franchised sandwich shops across 37 states.

C. Private Actions

The plaintiffs' bar continues to bring class action litigation claims associated with data security breaches involving consumer PII. In addition to substantive data privacy law, these cases have tended to wrestle with legal concepts such as plaintiff standing, pleading requirements and the enforceability of arbitration clauses and class action waivers.

In data breach cases, standing is a significant issue when PII has been exposed or stolen but there is no evidence that it has been misused. In these cases, plaintiffs seek to


\[\text{id.}\]

\[\text{17 The Jimmy Johns data breach has also resulted in the filing of at least one private class action, Barbara Irwin v. Jimmy Johns, No. 2:14-cv-02275-HAB-DGB (C.D. Ill. Nov. 6, 2014) (putative class action based on credit card fraud resulting from data breach at over 200 Jimmy Johns' locations and theft of thousands of consumers' PII).}\]
establish standing based on a fear of potential future harm, such as identity theft or fraud. However, many data security breach defendants have been successful at filing motions to dismiss for lack of standing, relying on the 2013 Supreme Court case, Clapper v. Amnesty International, 133 S. Ct. 1138 (2013). In Clapper, the plaintiffs challenged the constitutionality of an amendment to the Foreign Intelligence Surveillance Act that made it easier for the government to obtain wiretaps on intelligence targets outside of the United States. The plaintiffs were all U.S. citizens and included attorneys who asserted that they had standing to challenge the statutory amendment because their work involved telephone and email communications with likely foreign targets of surveillance and that such communications could be intercepted in the future. The Supreme Court held that the allegations of potential interception of attorney-client privileged communications were too speculative to sustain a claim and that the plaintiffs could not manufacture standing by merely "inflicting harm on themselves based on their fear of hypothetical future harm." Based on Clapper, several lower courts considering standing issues in the context of a data security breach have held that an increased risk of future harm is insufficient to establish standing.

Thus, defendants in data security breach cases continue to assert Article III standing challenges to plaintiffs' claims in data privacy cases. As observed in In re Google, Inc. Privacy Policy Litigation:

>D)espite generating little or no discussion in most other cases, the issue of injury-in-fact has become standard fare in cases involving data privacy. In fact, the court is hard-pressed to find even one recent data privacy case, at least in this district, in which injury-in-fact has not been challenged. Second, in this district's recent case law on data privacy claims, injury-in-fact has proven to be a significant barrier to entry. And so even though injury-in-fact may not generally be Mount Everest, as then-Judge Alito observed, in data privacy cases in the Northern District of California, the doctrine might still reasonably be described as Kilimanjaro.

The observation that injury-in-fact has proven to be a significant barrier to entry to data privacy plaintiffs largely continues to hold true, even in the face of recent decisions showing an increased tolerance for claims predicated on theories of future harm or statutes requiring no showing of actual harm.

In situations where data security breach plaintiffs might not otherwise be able to demonstrate injury-in-fact and, thus, be able to satisfy Article III standing requirements, they have seen increasing success in predating privacy claims on statutory rights of action, which some courts have found do not require actual injury. For example, in Robins v. Spokeo, Inc.,

---

16 id. at 1148.


20 In re Google, Inc. Privacy Policy Litigation, 2013 WL 6248499, at *4 (N.D. Cal. Dec. 3, 2013) (finding that allegations of loss of PII were insufficient to establish injury-in-fact, but certain alleged economic and statutory injuries were sufficient to support Article III standing).
742 F.3d 409, 414 (9th Cir. 2014), the Ninth Circuit held that the plaintiff could adequately plead Article III standing, despite lack of actual harm, by alleging a claim for a willful violation of the Fair Credit Reporting Act. Thus, the Ninth Circuit has given plaintiffs in putative privacy class actions a potential foothold upon which to satisfy the Article III standing requirement and seek enforcement of federal or state statutes concerning data privacy rights. The United States Supreme Court recently granted a petition for certiorari of the Robins v. Spokeo, Inc. case. See, 135 S.Ct. 1892 (Apr. 27, 2015). Thus, it may not be long before practitioners receive further guidance concerning whether an alleged statutory violation alone is sufficient to create Article III standing where the plaintiff fails to allege any actual harm.

While the issue of Article III standing based solely on a statutory violation (without allegations of actual harm) remains hotly debated, the plaintiffs’ bar is also pursuing other creative theories of harm in the data breach context. For example, in In re Target Corp. Customer Data Sec. Breach Litigation, 2014 WL 7192478, at *2 (D. Minn. Dec. 18, 2014), the court found that plaintiffs satisfied standing requirements at the pleading stage by alleging plaintiffs suffered "unlawful charges, restricted or blocked access to bank accounts, inability to pay bills, and late payment charges or new card fees." In addition, in In re Google, Inc. Privacy Policy Litigation, 2013 WL 6248499, at *6-7 (N.D. Cal. 2013), the court found that the plaintiffs had adequately alleged standing at the pleading stage by including allegations concerning battery and bandwidth usage and overpayment.21

D. Credit Card Companies

Credit card companies have tremendous power to influence industry standards concerning data security. They have primarily exercised that power through the Payment Card Industry Security Standards Council (the "Council"), an industry association whose members include all of the leading credit card companies, including Visa, MasterCard, Discover and American Express. The Council has established the Payment Card Industry Data Security Standard ("PCI-DSS"). PCI-DSS is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and to protect cardholders against misuse of their personal information. PCI-DSS is mandated by the major credit card companies and administered by the Council. The PCI-DSS specifies 12 requirements for compliance, organized into six logically related groups called "control objectives".22 A retail merchant’s failure to comply with PCI-DSS can result in penalties and in extreme cases the revocation of the merchant’s right to engage in credit card transactions.

The frequently asked questions section of the PCI Compliance Guide found at https://www.pcicomplianceguide.org, provides the following information.

Q: What are the penalties for noncompliance?

A: The payment brands may, at their discretion, fine an acquiring bank $5,000 to

---

21 However, establishing standing at the pleading stage does not necessarily settle the question. The United States Supreme Court held in Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992), that a plaintiff bears the burden of proving standing under Article III "with the manner and degree of evidence required at the successive stages of the litigation." So, for example, the summary judgment stage of litigation potentially provides a defendant with an opportunity to mount a secondary challenge to the standing issue by demonstrating that the plaintiffs standing allegations are not supported by actual evidence.

22 The PCI Data Security Standard can be found at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.
$100,000 per month for PCI compliance violations. The banks will most likely pass this fine on downstream till it eventually hits the merchant. Furthermore, the bank will also most likely either terminate your relationship or increase transaction fees. Penalties are not openly discussed nor widely publicized, but they can be catastrophic to a small business.

It is important to be familiar with your merchant account agreement, which should outline your exposure.

Thus, by virtue of contractual obligations contained in the merchant agreements that each retail outlet accepting credit card payments must enter into to be permitted to process those payments, retail outlets, including most franchisees, may be subject to heavy, even business-threatening, penalties in the event of a data security breach resulting from PCI-DSS noncompliance. In addition, credit card companies may assess penalties against acquiring banks on a per card basis and demand reimbursement for actual fraud and reimbursement of the expense of re-issuing card to consumers. Banks typically have the right under merchant agreements to pass these costs downstream to the merchant/retailer.

Many franchisors take the position that because franchisees typically maintain their own merchant accounts and have their own contracts with an acquiring bank, for PCI compliance purposes, franchisees are independent from their franchisor and responsible for their own PCI compliance. However, at least one commentor\(^{23}\) has posited that the franchisor/franchisee relationship falls within the parameters of the Council’s “Third Party Security Assurance Guidance” and that, therefore, a franchisor who shares PII with its franchisees through “chaining”\(^{24}\) (such as by transmitting to a franchisee reservation information that contains PII) must:

- Conduct due diligence and risk assessment when engaging [franchisees] to help organizations understand the services provided and how PCI-DSS requirements will be met for those services.
- Implement a consistent process for engaging [franchisees] that includes setting expectations, establishing a communication plan, and mapping third-party services and responsibilities to applicable PCI-DSS requirements.
- Develop appropriate agreements, policies and procedures with [franchisees] that include considerations for the most common issues that arise in this type of relationship.
- Implement an ongoing process for maintaining and managing [franchisee] relationships throughout the lifetime of the engagement, including the development of a robust monitoring program.\(^{25}\)


\(^{24}\) “Chaining” is the transfer of card data from the consumer to multiple parties. *Id.* Mr. Durko suggests that the risks that chaining presents to consumers and the implications to franchisors and franchised entities “will make it a hotbed topic.” *Id.*

\(^{25}\) *Id.*

18
Other commenters have noted that the level of integration that exists between some franchisors and their franchisees as a practical matter precludes franchisors from avoiding exposures for data security issues affecting their franchisees. As one commenter noted:

The best example of technology creating a PCI compliance nightmare for a franchisor is Speedpass from Exxon/Mobil. Speedpass is a great customer convenience and probably one of the more innovative uses of RFID technology. The customer registers one or more credit cards at the Exxon/Mobil Web site and is mailed a Speedpass RFID fob. At the service station, the customer merely waves the Speedpass RFID in proximity to the Speedpass logo on the gas pump and they are validated and pay without a credit card ever being used. From a PCI compliance perspective, this sounds like a very secure approach and it is. However, because of Speedpass, franchised operations have to send their Speedpass transactions through Exxon/Mobil's central data center. That data center is where the Speedpass RFID serial number is translated to a credit card number that the Speedpass customer entered into the Exxon/Mobil Web site. That credit card number is then used with the franchisee's merchant number to process the transaction. As a result, Exxon/Mobil is on the hook for not only their own PCI compliance, but also all of their franchisees that accept Speedpass. The lesson of Exxon/Mobil is that if the franchisor requires franchisees to process their transactions through the franchiser's data center, then the franchisor is responsible for everyone's PCI compliance. The franchiser also is responsible for the monitoring and compliance of all franchisees.27

Indeed, major credit card companies have weighed in on the subject. In June 2010, Visa introduced the concept of "Corporate Franchise Servicer" as a third party agent category under its Visa Third Party Agent Program to "help ensure that Corporate Franchise Servicer agents protect card data by, at a minimum, complying with the Payment Card Industry Data Security Standards (PCI DSS)."28 According to Visa, a Corporate Franchise Servicer is "a corporate entity or franchisor that provides or controls a centralized or hosted network environment irrespective of whether Visa cardholder data is being stored, transmitted or processed through it."29 A Corporate Franchise Servicer will qualify for registration under the Third Party Agent Program if it does any of the following: (1) provides card payment processing services but does not meet merchant PCI DSS validation criteria; or (2) owns or operates a centralized or hosted network environment, connecting physical and logical assets or locations which are used by the corporation, franchisees or other entities.30 Visa further notes that

---

26 RFID (radio frequency identification) is a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object, animal, or person.


29 Id.

30 Id.
according to PCI DSS "non-compliance of franchisors or other organizations performing aggregator or gateway functions may potentially expose acquirers to non-compliance penalties and increase potential liability in the event of a data compromise."31

As a practical matter, both the introduction of new technologies facilitating the electronic sharing of consumer information between franchisor and franchisees and the public's perception of "brand" that is integral to the concept of franchising make any system data security breach a potential exposure for a franchisor, regardless of whether that breach emanated from an individual franchise location or from the franchisor's own computer systems. Accordingly, franchisors have a vested interest in ensuring that their own systems and the systems of each of their franchisees are PCI-DSS compliant (even if the measures that the franchisors take to ensure such compliance potentially create additional exposure under a vicarious liability theory).

E. Assessing Litigation Risk And Minimizing Exposure

When a data security breach is discovered, it may be unclear at the outset whether the company's greatest exposure will take the form of potential federal or state enforcement actions, private lawsuits or the imposition of penalties by credit card companies for lapses in compliance with PCI-DSS. A franchisor may face the additional risk of being sued by its own franchisees for actual or perceived malfeasance in the implementation of its own data security systems. Regardless, one of the tasks that in-house or outside counsel will be asked to undertake following a data security breach will be to assess the company's litigation risk and to implement a plan to contain and minimize litigation exposure.

To minimize litigation exposure, counsel should participate in all aspects of responding to a data security breach and, where appropriate should label documents "Attorney-Client Privileged" with an eye toward maintaining confidentiality for sensitive documents or information that potentially could be used to the company's detriment in a future litigation. Counsel should remind management and other members of the response team that the "crisis" environment of responding to a data security breach is also potentially a pre-litigation environment, and that written and oral communications concerning the breach should be tempered to reflect that reality. To avoid potential spoliation assertions in a future litigation, counsel should also remind management and the response team that documents concerning the data security breach and the company's response to it should be maintained and not destroyed.

Counsel should also fully examine all opportunities that may exist to shift litigation risk and response costs to third parties. The company's insurance contracts should be reviewed and insurance carriers timely notified. The company's pertinent vendor contracts and franchise agreements should be reviewed, particularly the sections of the contracts that address indemnification obligations or liability under circumstances involving a data security breach. Counsel should examine whether any company employees have any personal exposure or liability associated with the data security breach. Counsel should also coordinate with and provide assistance to law enforcement officials who may be investigating the data breach with the goal of apprehending those engaged in criminal acts.

31 Id.
V. SPECIAL CONSIDERATIONS OF FRANCHISE SYSTEMS

A. Whose Data Has Been Compromised And Where Is It Located?

Each franchise system is unique and the amounts and types of information collected and maintained by, and shared between, franchisors and franchisees will vary depending upon the type of business and the structure of the franchise system. For example, the PII that a health care franchise system will collect and maintain is likely to be more voluminous and more sensitive than that of many other types of franchises. In contrast, a retail franchise system may not collect or maintain much in the way of sensitive customer PII but may process a much higher volume of payment card transactions. Hotel, health club or car rental chains may collect, store and share large volumes of PII, whereas a QSR chain may have and share very little. It is critical that franchisors and franchisees know what types of information each is collecting, how and where it is stored and who is authorized to access it. It is equally important that both the franchisor and the franchisee know who is responsible for protecting that information. If the sensitive information is transferred and shared across the data platforms of both the franchisor and the franchisee, it is important that encryption or other security mechanisms are in place to prevent the information from falling into unauthorized hands.

In the franchise context, the question of who owns and should have access to certain data can be complicated, and countervailing considerations often come into play. On the one hand, a franchisor may assert that it owns and should have access to all data collected as part of the franchise business so that it can use the data for marketing and other purposes that benefit the entire franchise system and so that former franchisees can be restricted from using the data after the franchise relationship ends. On the other hand, it may be in the franchisor’s interest to distance itself from customer data collected by franchisees in order to reduce the risk of being held responsible to third parties for a data breach. Because every franchise system is different, it is incumbent upon each franchisor to take the time to think through questions of ownership of, and access to, franchisee-generated customer data on the front end and to clearly state its position in the franchise agreement, the franchise disclosure document, or operations manuals and policies, as appropriate, in order to avoid any misunderstanding. Regardless of who actually owns the data, each party should be aware of the types of data it is collecting and should know where the data is located and who is responsible for protecting it.

B. What Should The Franchise Agreement Say About Data Security?

In addition to addressing who owns certain specific data generated by or associated with franchise operations, franchisors should consider whether and how to address data security in the franchise agreement. Many franchise agreements have terms of 10, 15 or even 20 years. Consequently, some franchise agreements in place today were entered into before the issue of data security became a prominent business risk. In addition, given the rapid pace of technological change, franchise agreements being entered into today may not be able to fully anticipate and address the type of data security issues likely to arise during the life of the franchise relationship. Thus, language in some franchise agreements may be too narrowly focused to address today’s data security concerns and may be inadequate to protect the system from unforeseen data security threats. Rather, the preferable approach may be to address the topic broadly in the franchise agreement and to provide mechanisms allowing for the parties’ respective obligations to change as necessary to reflect shifting legal and technological realities.
Most franchise agreements deal with potential changes in the business and legal environment by generally providing that the franchisee must comply with "applicable law" and must abide by the franchisor’s system standards and operational requirements, as set forth in an operations manual, which may be updated from time to time. Many franchise agreements today also require franchisees to upgrade their business systems to comply with the franchisor’s operational requirements. Franchisors should make clear in the franchise agreement that such equipment upgrades may include computer and other technology systems, electronic point-of-sale systems and related hardware and software.

The decision of whether to address data security issues in the franchise agreement or instead to reserve discussion of such issues to the operations manual (which may allow for more flexibility over the life of the franchise agreement), or simply through regular training and education of franchisees, ultimately may depend upon the nature of the franchise involved and the franchisor’s assessment of the risk associated with a potential data security breach. Regardless of where the obligation is articulated, retail franchises that anticipate multiple payment card transactions will almost certainly want to require that franchisees abide by sometimes evolving data security and industry-specific laws, regulations and standards, such as PCI-DSS. In addition, franchises in the health care industry will need to mandate HIPAA compliance.

Franchisors should consider including within their operations manual suggestions concerning basic data security practices and policies, such as changing of default credentials, use of strong passwords and the periodic changing of passwords, log monitoring and physical inspection of hardware. Franchisors should also require, or provide suggestions concerning, specific data security measures such as segregating their payment card environment and any additional systems containing PII from other systems and networks, implementing anti-virus protection and having firewalls in place that are managed (i.e., continuously reviewed and updated by the firewall vendor) and whitelisted.

As mentioned above, the franchise agreement should specifically obligate the franchisee to communicate and cooperate with the franchisor in the event of a data security breach. In addition, the franchisor may wish to expressly address in the franchise agreement the allocation of risks and responsibilities in the event of a data security breach, including the parties’ indemnification obligations and whether a franchisee is required to purchase and maintain cyber insurance.

C. Weighing Potential Vicarious Liability Associated With Post-Breach Actions

Franchisors have long understood that from a vicarious liability perspective, the more control they assert over a particular aspect of their franchisees’ businesses, the more likely it is that they may be held responsible if a third-party suffers harm associated with the controlled instrumentality. As a result, franchisors struggle to determine the appropriate level of control to assert over franchisees’ data security practices. Some franchisors may be reluctant to mandate specific data security requirements and prefer to stand on the concept that the franchisee, as an independent business owner, is solely responsible for ensuring its own data security. Others understand that the financial risk of a finding of vicarious liability may pale in comparison to the public relations risk and substantial brand damage that could occur in the event of a data security breach. Consumers frequently fail to distinguish among a single franchised location, the franchisor or the brand as a whole, particularly when it comes to technology and data security. As a result, a data incident at a single franchised location has the potential to
negatively impact all franchisees in a way that a slip-and-fall incident simply would not. Consequently, in some respects data security may be more analogous to health and safety considerations than to other types of business risks, and may warrant the same level of franchisor involvement in setting mandatory standards and enforcing those standards (regardless of whether those actions may increase vicarious liability risk).

D. Mandating System Change To Prevent Future Data Breaches

While most established franchisors today likely acknowledge the need to mandate some data security measures for franchisees, many still struggle with implementation. Franchise systems with older franchise agreements that do not directly or expressly address data security may not provide an obvious mechanism for permitting the franchisor to require franchisees to adopt specific data security measures. Even when there is express language in franchise agreements and operations manuals, franchisors may find it difficult to police and enforce data security requirements due to limited field resources and lack of internal technical expertise. Additionally, some data security measures come with a substantial price tag, particularly where they involve hardware upgrades or ongoing service contracts. Smaller franchisees may find it difficult, or may simply be reluctant, to make the investment when they know they won't see an immediate return. And with requirements and technology ever changing, franchisors and franchisees must also consider the inevitable fact that they may need to do something more or different in the not too distant future in order to keep up with industry standards.

All of these considerations make system enforcement of data security standards difficult to achieve. Nevertheless, the alternative to enforcement, i.e., simply ignoring the issue and hoping that each franchisee independently adopts adequate data security measures to protect itself and the brand, is the business equivalent of "Russian roulette." Franchisors that have not done so need to evaluate the potential risk that data security poses to their franchise systems and, in the absence of contractual mechanisms, work collaboratively with their franchisees to agree upon the data security standards that should be adopted across the system.

VI. CONCLUSION

The enormous financial and public relations risks associated with a potential data security breach require all businesses that maintain sensitive information in their internal systems to assess their vulnerabilities and plan ahead. When an actual data breach is discovered, affected parties will need to act rapidly and with purpose to contain the breach, assess the timing and extent of the breach, implement mitigation measures and evaluate exposures. The ability of a company facing a data security breach to take timely, effective action, and to minimize potential liability, will largely be a function of the level of pre-planning and forethought given to the issue.

Knowing what to do, and appreciating the sequence of activity that should be followed, is not necessarily intuitive. It requires a plan. A data security breach should not be dealt with "off the cuff." This paper has attempted to identify relevant issues that should be considered in the development of a data security breach plan and to discuss the sequence and priority of issues that should be considered and addressed in the face of a data security "crisis".

Data breach vulnerabilities are magnified under the standard franchise business model because, as discussed above, multiple parties frequently maintain sensitive information in their systems, and responsibility for implementing appropriate security measures, and even what constitutes appropriate security measures within the franchise system, may be ill defined. Thus,
developing a data security breach plan and mitigation strategy is more challenging in the franchise context ... but also more critical. Careful planning and foresight are key to minimizing the effects of a data security breach should one occur.
GENEVIEVE A. BECK

Genevieve A. Beck serves as Vice President and Assistant General Counsel for International Dairy Queen, Inc. Before joining International Dairy Queen, she worked as in-house counsel for a global hotel company and, prior to that, worked as a litigator principally representing franchisors.

Ms. Beck has spoken at the ABA Forum on Franchising, served as editor of *The Franchise Lawyer*, and written a number of articles on franchise-related issues that have been published in *The Franchise Law Journal*, *The Franchise Lawyer* and other publications.

She received her law degree *cum laude* from the University of Minnesota Law School, where she was a member and editor of *The Minnesota Journal of Global Trade*. She is a member of the Minnesota bar.

JAMES A. GONIEA

James A. Goniea is a partner in the Philadelphia office of Wiggin and Dana LLP. Prior to joining Wiggin and Dana, Mr. Goniea was the Vice President and General Counsel of American Driveline Systems, Inc., the company that owns the AAMCO Transmissions and Cottman Transmission brands. Mr. Goniea’s practice is almost exclusively devoted to representing mature and growing franchise companies. His representation of franchisors encompasses the full range of legal issues affecting such companies.

Mr. Goniea recently was named Philadelphia Franchise Law “2014-2015 Lawyer of the Year” by *Best Lawyers in America*. He is nationally ranked in the Franchise category of Chambers USA 2015. In addition, Mr. Goniea has been named a Legal Eagle numerous times by *Franchise Times Magazine* and as “being among the world’s leading franchise lawyers” by *Who’s Who Legal*. Mr. Goniea is serving his second term as a member of the Governing Committee of the ABA Forum on Franchising and presently serves as the Forum’s Publications Officer. He has written papers and presented programs on a wide variety of franchise law issues for numerous seminars and symposia including both the ABA Forum on Franchising and the International Franchise Association Legal Symposium.

ERIN NEALY COX

Erin Nealy Cox is one of five executive managing directors that serve on Stroz Friedberg’s executive leadership committee. She is also in charge of the firm’s global Incident Response Business, leading a vast team of first responders, threat intelligence analysts and malware specialists. Ms. Nealy Cox regularly advises a full portfolio of corporate clients, providing consulting and technical expertise in the areas of cybercrime investigations, data breach response, digital forensics, and investigations.

Although she is a technical consultant now, her background comes from law – prosecuting cybercrime cases for almost a decade on behalf of the Department of Justice as an Assistant United States Attorney in the Dallas office. Ms. Nealy Cox left DOJ in 2008 to open the Dallas office of Stroz Friedberg. Throughout her career with Stroz Friedberg, Ms. Nealy Cox has successfully led some of the firm’s biggest and most high profile data breach matters, plus many of its large-scale, complex electronic evidence engagements. In one representative case, she led an internal incident response team as independent forensic investigator in the Heartland Payment Systems breach— still the largest disclosed payment card information (PCI) data breach. More recently, Ms. Nealy Cox has marshalled the firm’s
highly-skilled incident response teams to assist an array of significant retailers and hospitality clients, including Target Corporation, Neiman Marcus Group, Genesco, Inc., Aldo Corporation, and Wyndham Worldwide Corporation. Additionally, she has led economic espionage investigations in many other sectors such as energy, financial institutions, healthcare and technology. Finally, she routinely advises Boards of Directors and Audit Committees of Fortune 500 companies on leading security practices within the context of today’s cyber risks.