# Five Lessons All Companies Can Learn From The Equifax Data Breach

By Scott C. Hall and David (Duff) Beach

The Equifax data breach has dominated news headlines for weeks, and Equifax will be dealing with the legal and financial fallout from the breach for many years. While many companies may be relieved not to be in Equifax's position right now, no company is immune to data breaches. Those who fail to learn key lessons from Equifax's mistakes may find themselves in the next headline. Accordingly, companies in every industry, and of every size, that maintain any type of sensitive personal data—whether it be of customers, employees, or data maintained on behalf of others—should study the Equifax situation and ensure that they are better prepared for a data breach incident.

## 1. Everyone (yes, everyone) will experience a data breach.

When it comes to data breaches, the question is not if, but when. This makes the more important question how will you respond? Data breaches do not only result from malicious hackers or phishing scams. They can occur when employees inadvertently access and/or mistakenly share personal data. They can occur when company laptops, flash drives, or even personal phones or tablets that contain company data, are lost or stolen. These kind of events occur in every company in every industry. As a result, everyone needs to prepare to respond. Indeed, the manner in which Equifax handled this most recent data breach—including: (1) the several weeks that elapsed before notifying affected individuals,(2) the executives who sold stock during the period between discovery of the breach and notifying the public, and (3) the company's offer to provide credit monitoring services to affected individuals, but only in exchange for a waiver of certain legal rights against the company—indicates that Equifax was not sufficiently prepared to deal with this kind of a data breach.

Every company should have a basic data breach response plan in place that at a minimum identifies who (among IT, HR, business operations, public relations, and other personnel) will respond to the breach, what their respective roles will be, and who will be the ultimate contact point and decision-makers with respect to the response. The plan should also include a timeline and enumerated steps to follow regarding discovering the scope of the breach, investigating the cause, remedying or mitigating the breach, notifying affected individuals, and contacting law enforcement as necessary.

Because of the widely publicized nature of Equifax's data breach, as well as other recent high-profile data breaches, no company will get a "free pass" or be able to argue that they had no idea a data breach could happen to them. In effect, these high-profile breaches put everyone on notice that data security must be a priority for all. Any company that chooses to put its head in the sand, does so at its own (certain) risk.

## 2. Act quickly to show affected individuals that you are trying to protect them.

In responding to data breaches, time is of the essence. Many have criticized Equifax for waiting until early September to notify affected individuals of a data breach it discovered in July. Most state data breach notification statutes require that a company disclose a data breach "in the most expedient" time possible, without further clarification about what that means. The minimum amount of time specified under state laws that contain specific time periods for notification is generally either 30 or 45 days from discovery of the breach.

In light of these general standards, Equifax's timing for notification to individuals may not have constituted an improper or unlawful delay as a matter of law. After all, it takes some time to investigate what happened, confirm what data was breached, and implement remedial measures. And, as a company responding to a data breach, you do not want to rush to publicize inaccurate facts that you later have to correct. However, as a practical matter, 6 weeks is a lengthy period of time for sensitive personal information to be exposed without notifying affected individuals—and as the response to Equifax shows, many people believe this kind of delay is unreasonable, regardless of the legal standards. Thus, while a company needs time to investigate the incident and communicate accurate facts to those affected, all companies should seek to notify those whose information has been compromised sooner rather than later.

(continued on page 2)



Coblentz Patch Duffy & Bass LLP

## 3. Take actions that demonstrate that you are genuinely attempting to remedy the problem.

Data breaches happen. They will continue to happen. And the public generally understands that not every data breach, especially a hacking attack, can be prevented. However, when a data breach occurs, affected individuals want to know that the company is doing everything in its power to protect them, not itself. Equifax added insult to injury when it offered to enroll affected consumers in free credit monitoring services—something required under at least some state data breach laws—only if consumers agreed to waive certain legal rights against the company. Unsurprisingly, this did not go over well in the court of public opinion. And, while Equifax has since agreed to provide credit monitoring without these legal restrictions, the reputational damage has already been done.

Ultimately, the legal fallout from any data breach will be what it will be based on the circumstances and whether the company had reasonable protections in place. But reputational harm may damage the company as much or more than the legal process. The best thing a company can do in the wake of a breach is to diligently correct its data security weaknesses and work with affected individuals to minimize the scope and harm caused by the breach.

## 4. Consider what sensitive personal data you maintain or need to maintain and how to safeguard it.

It is a rare company that holds no sensitive personal data. While credit reporting companies like Equifax have more sensitive information than most, all companies have some kind of personal data—in the form of customer or employee social security numbers, financial account numbers, or other information—that triggers data breach notification requirements. All companies should, at a minimum, know the types of personal information they maintain, how and where is it stored, who has access, and whether it is sufficiently secured. Companies then need to consider: (1) whether they truly need all the personal information they have and (2) whether such personal information can be separated, encrypted, or otherwise safeguarded to minimize the accessibility of such information or its usefulness if improperly accessed or exposed.

## 5. Consider cybersecurity insurance and other professional services.

While every company will at some point experience a data breach incident, the potential risk largely depends on the type and volume of sensitive personal data a company maintains. For those companies where there is a real possibility of significant financial injury if a data breach were to occur, cybersecurity insurance is something to consider. Many companies elect not to carry cybersecurity insurance because they do not want to pay expensive premiums, they are unsure exactly what the policies will cover, or they are skeptical that they will suffer a significant cybersecurity incident sufficient to justify the cost of insurance. But the Equifax breach reminds us that data breaches will occur—and likely with increasing frequency in coming years. Companies with significant risk should analyze whether cybersecurity insurance makes sense for them.

As the Equifax breach shows, especially in the area of cybersecurity, an ounce of prevention is worth a pound of cure. Companies should work with cybersecurity consultants, attorneys, or other professionals prior to a data breach both to protect against breaches, and to prepare to respond to a breach. Preventative cybersecurity training for employees is key, as human error is responsible for many data breaches. Companies should ensure that their IT systems are reasonably secured, their personnel are reasonably trained, and their data breach response plan is ready to go for when a data breach occurs. And it will.

Scott C. Hall
415 772 5798
shall@coblentzlaw.com
www.coblentzlaw.com

David (Duff) Beach
415 772 5708
dbeach@coblentzlaw.com
www.coblentzlaw.com

Coblentz Patch Duffy & Bass LLP