THOMSON REUTERS

Westlaw®

Equifax: Why this data breach is different from all the others

By Shari Claire Lewis, Esq., and Amanda R. Gurman, Esq., *Rivkin Radler LLP*

NOVEMBER 2017

As the world is now well aware, on Sept. 7, Equifax announced that it had experienced a "cybersecurity incident" that compromised the personal and financial information (including name, address, birth date, driver's license number and Social Security number) of over 143 million U.S. consumers.

Equifax has reported that the breach first occurred in mid-May 2017 and continued through July. While the breach was discovered July 29, Equifax did not announce it to the public until six weeks later.[1]

In just a month, this breach proved to be unique not just in scope but also with respect to its potential impact on how business is conducted.

The breach shined a bright light on the data practices of the largely unregulated credit monitoring industry as well as general risks inherent in the pervasive collection of personal information. It affected many individuals who had never directly contacted Equifax or voluntarily used its services.

This breach was unlike many prior cybersecurity incidents in which customers voluntarily provided companies with personal information and thus had some control over whether to accept the risk of disclosure.

Consumers and businesses placed their trust in Equifax to secure their most important personal and financial information. A breach of this trust hits particularly hard with consumers, leaving many wondering, if a company of this nature cannot keep their information secure, who can?

No doubt this breach will expose Equifax to many of the same claims that others have faced in the past, but it remains unique in many respects.

With the benefit of hindsight, Equifax is being criticized for both its failure to implement appropriate cybersecurity measures to protect against breach in the first instance and the adequacy of its breach response procedures.

Both of these deficiencies have already led to allegations against Equifax and may result in potential liability in the form of civil suits, enforcement proceedings, regulatory investigations and criminal investigations.

One aspect of Equifax's performance that has been called into question is whether and to what extent the breach was preventable.

The vulnerability that hackers exploited to access Equifax's information was in the Apache Struts web-application software. After Equifax announced the cybersecurity incident and identified this software as the source of the breach, the Apache Software Foundation released a statement indicating that Equifax received notice of the vulnerability that caused the breach, as well as instructions to fix the vulnerability, in March 2017.[2]

While the breach was discovered July 29, Equifax did not announce it to the public until six weeks later.

Equifax apparently chose not to or failed to implement the remediation. As a result, the vulnerability persisted and was ultimately exploited in May.

Unfortunately, Equifax is not exceptional in its failure to take necessary steps to prevent exploitation of known vulnerabilities.

For example, in May the WannaCry ransomware attack exploited a Windows vulnerability for which Microsoft had previously provided a patch.

In the MongoDB ransom event, hackers were able to attack thousands of unsecured servers in two different waves months apart. The second wave occurred because companies failed to take necessary security measures after the first one.

Many consider the Equifax data breach to be the straw that breaks the camel's back, demonstrating the need for regulation and/or industry standards across all data collectors.

While regulation remains an unknown, Equifax's failure to take necessary security measures has and will provide the basis for numerous claims against the company.

Indeed, at least 23 proposed consumer class-action lawsuits have been reportedly filed against Equifax around the country.[3] These lawsuits allege, among other things, security negligence by Equifax and undue delay in alerting the public.

The suits are predicated on the theory that Equifax's cybersecurity was inadequate, that the company knew or should have known of this inadequacy, and that it failed to take action to correct the inadequacy to the detriment of consumers.

The complaints hinge on the fact that Apache notified Equifax of the software vulnerability and provided a solution that Equifax failed to promptly implement.

It remains to be seen what financial liability Equifax will ultimately face as a result of these suits. In the past, consumer class-action settlements of this nature have not netted consumers large sums of money, as it can be difficult for many consumers to establish financial losses as a result of a breach.

Many people suffer no direct financial harm from the disclosure of their personal or financial information, as it is either not used or remediation is quickly provided. As a result, past settlements have provided nonmonetary remedies, such as free credit monitoring and cash reimbursement for those who suffered actual out-of-pocket losses, with no compensation being paid for merely having the information disclosed to the public.[4]

> The breach shined a bright light on the data practices of the largely unregulated credit monitoring industry.

However, courts are now trending toward treating data theft (and the corresponding threat of future identity theft) as a sufficient harm permitting consumers to maintain a claim.

With the filing of these suits and this trend, Equifax faces the risk that it will have to pay more than mere actual out-of-pocket costs to the consumers whose information was disclosed.

In addition to the consumer class actions, Equifax is facing at least one proposed securities fraud class-action lawsuit.[5] This suit alleges violations of the Securities Exchange Act of 1934 based on Equifax's purported materially false and misleading statements to the public.

In this regard, the false and/or misleading statements focus on Equifax's disclosure that the company maintained adequate measures to protect its data system when, in fact, it did not.

The proposed class-action complaint alleges damages based on the 17 percent drop in Equifax's share price as a result of the breach disclosure.

Unlike many of its predecessors, Equifax's data breach was exceptional because it experienced a fairly significant decrease in its stock price (likely a reflection of the fact that Equifax's business model depends on maintaining the confidentiality of consumer's personal information). This provided fodder for hungry plaintiffs' lawyers who have been eagerly awaiting a large enough stock drop to bring such a suit.

Given that there have been few securities class action lawsuits arising out of cybersecurity breaches, it is difficult to tell how Equifax will fare in defending such a suit.

However, the massive stock price drop combined with the suspiciously timed sale of shares by Equifax's officers certainly puts Equifax at a disadvantage.

While Equifax's allegedly lax cybersecurity measures certainly present liability issues, what is more interesting are the threats posed by its conduct after the breach. The company's six-week delay in disclosing the breach not only left its customers exposed; it also exposed it and its officers and directors to potential liability.

First, the delay in disclosure likely violates several state disclosure laws. Indeed, individual states have enacted their own laws dictating disclosure requirements after a breach.

While each state has slightly different requirements, what is fairly uniform is the requirement that a breach be disclosed in "the most expedient manner possible and without unreasonable delay."[6] This time frame is often not defined, but several states have specified that disclosure must take place no later than 45 days after the date that the breach was discovered.[7]

Violation of these state statutes could subject Equifax to fines and penalties.

Importantly, the penalties do not necessarily require that any financial harm was suffered by consumers and can provide for certain fixed amounts (for example, $5,000) to be imposed for each violation or for each day that Equifax delayed in disclosing the breach.[8]

Attorneys general from Illinois, Massachusetts, New York and Pennsylvania have already contacted Equifax in response to the breach, and Massachusetts Attorney General Maura Healey filed suit against the company Sept. 19.

Equifax's disclosure delay also subjects the directors and officers to potential individual liability. As has now become public knowledge, several Equifax officers sold a large portion of their company shares during the period between when the breach was discovered and when it was disclosed.

Indeed, Chief Financial Officer John Gamble on Sept. 1 sold shares worth $946,374, and Joseph Loughran, the president of the company's U.S. Information Solutions division, exercised options to dispose of stock worth $584,099. Similarly, Rodolfo Ploder, president of Workforce Solutions at Equifax, sold $250,458 of stock Aug. 2.[9]

While there is presently no evidence that these individuals had knowledge of the data breach when they sold their

shares (and Equifax has denied they did), the fact that the shares were sold during this time has raised red flags with federal regulators.

Both the Securities and Exchange Commission and the Justice Department have commenced investigations into possible insider trading by these individuals, at a minimum subjecting them to costs in defending themselves and potentially exposing them to criminal penalties.

Irrespective of whether these individuals will ultimately be deemed liability, Equifax's delay in disclosing the breach has put them in the crosshairs and will likely subject the company to criticism regarding its post-breach response.

These individuals may also face potential exposure in the form of derivative lawsuits. Specifically, it is often the case that when a company is sued for violations of securities laws (as Equifax has been here), a derivative suit will follow.

These suits typically allege that the directors and officers are individually liable for the damages suffered by the company due to breaches of their fiduciary duties. Here, Equifax faces potential exposure in light of the numerous lawsuits that have been filed as a result of the data breach.

Equifax's disclosure delay subjects the company's directors and officers to potential individual liability.

In addition, the investigations by the SEC and Justice Department provide further fodder for shareholders to argue the directors and officers breached their fiduciary obligations to the company.

While it is impossible to know whether derivative suits will be filed, such suits were filed after the data breaches experienced by Wyndham Worldwide Corp., Home Depot Inc., Wendy's Co. and Target Corp. Thus, with the additional negative facts present with respect to the Equifax breach, such a suit is certainly a possibility.

Equifax is also facing myriad governmental and regulatory investigations and enforcement actions. Aside from investigations by state attorneys general, the SEC and the Justice Department, the company is currently the subject of investigations by the House Financial Services Committee, the House Energy and Commerce Committee, the Federal Trade Commission, and the FBI.

At this time, there is little information regarding the status of these probes. What is evident, though, is that the breach has garnered the attention of numerous investigating bodies and may prompt federal regulatory changes.

Of particular concern for Equifax may be the FTC's authority to pursue action pursuant to Section 5 of the Fair Trade Commission Act, which bars unfair or deceptive acts or practices.

Notably, Section 5 describes an unfair practice as one that causes or is likely to cause harm to consumers, cannot be reasonably avoided by consumers, and is not outweighed by the countervailing benefits to the consumer.

Given consumers' lack of meaningful choice in Equifax's collection of personal data, the FTC's Bureau of Consumer Protection is expected to become involved in this matter, and through it, to become even more involved in consumer data protection in general.

In addition to its many legal concerns, Equifax is facing massive criticism for its breach response. As part of its supposed remediation efforts, the company offered consumers free credit monitoring.[10]

However, there was substantial push-back to this remedy, as Equifax limited the time frame to only one year and then required consumers to enter personally identifiable information into its website to sign up.

On top of that, consumers who signed up for the free monitoring had to agree to waive the right to sue. These limitations prompted severe criticism.

In response, Equifax clarified its terms of service to say that enrolling in its complimentary monitoring service would not waive the right to bring legal action in response to the breach.[11] Equifax has also agreed to waive the fee to set up a security freeze until Nov. 21, 2017.

However, questions remain as to whether a fee will thereafter be charged to "thaw" the freeze; how Equifax will assign PINs for this purpose; and who will bear the cost to initiate and thaw credit freezes with the other two major credit reporting agencies, Experian and TransUnion, where such a freeze would also be applied.

Overall, Equifax's conduct leaves many wondering if Equifax was prepared, in any manner, for a data breach. Most notably, the breach is likely to have a significant impact on the way Equifax and the other credit monitors conduct their business.

The breach has placed a sharp focus on the lack of regulation and oversight on this industry, which collects and holds massive quantities of personal information. It does so not at the request of the individuals but on behalf of businesses that use the information to inform their decisions regarding individual consumers.

While this deficiency is being investigated and discussed, it remains to be seen what, if any, regulatory changes will result from the Equifax data breach. At a minimum, the issue is being discussed on a much larger scale than ever, which may result in positive changes.

The Equifax breach nevertheless leaves us with many unanswered questions about what the future will hold in this area. Will companies be more likely to experience a share price decrease as a result of a cybersecurity incident? Will such

decreases be met with more frequent and more successful securities and derivative suits? Will regulators more harshly prosecute companies who experience breaches? Will we see wide-scale regulatory reform on cybersecurity?

It certainly appears that the Equifax data breach has prompted a ground swell for greater privacy protection in the United States through regulation, oversight and recourse. One thing is certain: Equifax will not escape this breach unscathed.

NOTES

[1] *See Equifax Announces Security Incident Involving Consumer Information,* EQUIFAX (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

[2] *See Apache Struts Statement on Equifax Security Breach,* APACHE SOFTWARE FOUNDATION BLOG (Sept. 9, 2017), http://bit.ly/2wh7QJM.

[3] It is difficult to determine precisely how many lawsuits have been filed against Equifax, and more may be filed in the future, but sources report anywhere from 23 to 50 purported class-action suits have been commenced. *See* Kevin McCoy, *Equifax Hit With at Least 23 Class-Action Lawsuits Over Massive Cyberbreach,* USA TODAY (Sept. 11, 2017), https://usat.ly/2gYs8FL; Anna Bahney, *Will Equifax Be Held Accountable?,* CNN MONEY (Sept. 15, 2017), http://cnnmon.ie/2f0zXqn.

[4] *In re Heartland Payment Sys. Inc. Customer Data Sec. Breach Litig.,* No. 09-md-02046 (S.D. Tex. 2012); *In re Target Corp. Customer Data Sec. Breach Litig.,* No. 14-md-02522 (D. Minn. 2015); *In re The Home Depot Inc. Customer Data Sec. Breach Litig.,* No. 14-md-02583 (N.D. Ga. 2016).

[5] *Kuhns v. Equifax Inc.,* No. 17-cv-3463, *complaint filed,* 2017 WL 4053019 (N.D. Ga. Sept. 8, 2017).

[6] A comprehensive list of each individual disclosure law can be found at the National Conference of State Legislatures' website. *Security Breach Notification Laws,* Nat'l Conference of State Legislatures (Apr. 12, 2017), http://bit.ly/1ao7NAi.

[7] *See* FLA. STAT. ANN. § 501.171; VT. STAT. ANN. Tit. 9 § 2430 et seq.; WASH. REV. CODE § 19.255.010 et seq.; WIS. STAT. § 134.98.

[8] FLA. STAT. ANN. § 501.171(9)(a); HAW. REV. STAT. § 487N-3(a); OR. REV. STAT. § 646A.600.

[9] The disclosure of the stock sales came from Equifax's regulatory filings. *See* Anders Melin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed,* BLOOMBERG (Sept. 7, 2017), https://bloom.bg/2wMQecQ.

[10] *See* note 1.

[11] *See* Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes, EQUIFAX (Sept. 17, 2017), http://bit.ly/2xG5p8R.

This article first appeared in the November 2017, edition of Westlaw Journal White Collar Crime.

ABOUT THE AUTHORS

Shari Claire Lewis (L) is a New York-based partner in **Rivkin Radler LLP**'s privacy, data and cyberlaw practice group; complex torts and product liability group; and professional liability group. She has focused her practice on the intersection of law and technology, often advising and representing clients on 21st-century technology challenges they face. She can be reached at shari.lewis@rivkin.com. **Amanda R. Gurman** (R), an associate in the firm's professional liability practice group, defends attorneys, insurance agents and brokers, accountants, and various other professionals in civil litigation. She can be reached at amanda.gurman@rivkin.com.