THOMSON REUTERS

Westlaw®

Why the Equifax breach could be the tipping point

By Sean L. Harrington, *Concord Law School*

NOVEMBER 2017

> A memo to a higher office
> Open letter to the powers that be
> To a god, a king, a head of state
> A captain of industry
> To the movers and the shakers ...
> Can't everybody see?[1]

On Sept. 7, Equifax, one of the three primary consumer credit reporting agencies, announced one of the largest cybersecurity data breaches in history — a breach the company claims it discovered in July. The breach compromised the personal information of 143 million people — nearly half the U.S. population.

Equifax is in the business of collecting, processing and selling data. It describes itself as follows:

> Equifax is a global information solutions company that uses trusted unique data, innovative analytics, technology and industry expertise to power organizations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions. The company organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers.[2]

That "trusted unique data," which was exposed, includes names, Social Security numbers, birth dates, mailing addresses, driver's license numbers and, for some affected people, credit card numbers.

There may be some irony in the company's use of the word "trusted." One commentator may have phrased it best, noting, "Equifax sits at the intersection of cybersecurity and the personal information system."[3] Arguably, this characterization means Equifax had a greater duty to secure the data than any or most of the business partners that supplied it.

As of this writing, Equifax is being investigated by the Federal Trade Commission, New York's financial regulator, several state attorneys general, the U.K. Financial Conduct Authority and various congressional subcommittees. Several class-action suits were filed within days after the breach was announced.

Consumers and commentators alike have speculated as to what obligations Equifax had to protect this data. The consensus seems to be that its actions were likely negligent, and perhaps grossly negligent.

Specifically, there has been much criticism of the fact that the education credentials of Equifax's chief information security officer are a bachelor's degree in music composition and a Master of Fine Arts (also in music).

Making matters worse, three Equifax executives sold shares in August, shortly after the breach was allegedly discovered, but before it was publicly disclosed. Those sales are the subject of a criminal investigation by the Justice Department.[4]

Equifax's CEO, chief information officer and chief information security officer have left the company in the wake of the scandal. Equifax shares have plunged by as much as 35 percent as a direct and proximate result of the breach and the company's response to it.

The scope of this analysis, however, is limited to Equifax's obligations prior to the breach and, based on facts known at the time of this writing, the liabilities the company may have incurred.

It does not address collateral matters, such as the securities trading of Equifax insiders, the qualifications of Equifax executives, the controversy regarding the arbitration clause in Equifax's initial credit monitoring offer, or the propriety of the providers that Equifax uses for its website services.

EQUIFAX'S LEGAL OBLIGATIONS

Regarding the safeguarding of data, Equifax has several different legal duties. These include the officers' and directors' duty of loyalty, the duty of good faith and various fiduciary duties. These duties are owed to shareholders, customers and employees. They are also owed to those with whom the company has a special relationship, such as one that may be created by statute (for example, the Fair Credit Reporting Act).

The fact that the breach primarily affects consumers (who are not in privity of contract with Equifax) creates difficult questions about the scope of the duty and legal standing.

In basic negligence terms, those whose data was held by Equifax were certainly within the "zone of danger" to whom a duty was owed without regard to the existence of a contractual relationship.

The breach in question, Equifax claimed, was attributable to an Apache Struts flaw that was rated as a 10.0 ("critical") in the National Institute of Standards and Technology vulnerability database, and for which a patch was issued on or before March 6. The vulnerability was widely disclosed March 13, when the NIST and the U.S. Computer Readiness Team issued "high vulnerability" warnings.

The time between the issuance of the patch and the purported discovery of the breach was 145 days. Consequently, there has been outrage that the massive breach was easily avoidable by timely patching, and the Apache Software Foundation issued a statement that the "the Equifax data compromise was due to their failure to install the security updates provided in a timely manner."[5]

> There has been outrage that the massive breach was easily avoidable by timely patching.

The average time to patch for organizations is 55 days, according to the Symantec Internet Threat Report. Symantec also found that it takes only an average of six days for exploit code to become available to the public.[6]

Edgescan found that the average time to fix is 62 days for critical application vulnerabilities and 12 days for critical network vulnerabilities.[7]

But these findings should be construed in context: Time to patch varies based not only on the severity of the vulnerability but also on several other factors as well. These include the criticality of the data, the industry, the maturity of an organization's security posture, and the potential for impact (such as patient — or customer — harm, harm to brand image and monetary penalties).

For example, a large, well-funded bank would ordinarily patch a critical vulnerability within a few days. Therefore, the efficacy and reasonableness of Equifax's data security controls must take into account the size, maturity and wherewithal of the organization; the regulatory requirements to which the organization is subject; the classification of data in need of protection; and the potential impact if the data is compromised.

Reportedly, a researcher discovered critical vulnerabilities in December 2016, allowing the researcher to "access the personal data of every American, including Social Security numbers, full names, birthdates, and city and state of residence."[8]

The researcher also claimed to have been able to take control of several Equifax servers and found several servers susceptible to well-known, critical vulnerabilities. If true, this would indicate that Equifax did not have an effective vulnerability management program in place and apparently did not conduct routine penetration tests on its publicly facing servers. This would fall well below the accepted standard of care for an organization of this size and resources.

Although the standard to which Equifax may be held regarding the efficacy and reasonableness of its controls may vary depending on the forum of review and jurisdiction, commercial reasonableness as articulated in *FTC v. Wyndham Worldwide Corp*.[9] may be the best standard to use for purposes of this analysis.

Several factors indicate that Equifax's information security program was immature and lacked sufficient oversight by its board. These include the sensitivity and volume of the data at risk, the potential for future harm, the status of Equifax as one of the big three credit reporting agencies, the monetary resources that Equifax presumably had available, and the facts that have been publicly disclosed as of the date of this writing.

As a result, Equifax appears to have lacked a robust risk management program and/or an effective vulnerability management program that included threat intelligence gathering, vulnerability scanning and timely patching.

EQUIFAX'S POSSIBLE LOSSES AND LIABILITIES

The possible losses and liabilities fall into the following categories: civil liability; fines and corrective action programs imposed by regulators; criminal liability; harm to reputation, goodwill and competitive advantage; loss of market capitalization (shareholder value); and the cost of remediation.

Civil suit liabilities

Absent evidence that the misappropriated data was used, for example, to drain a victim's bank account, data breach lawsuits are typically based on a theory of "future harm." In these suits, the plaintiff alleges that the defendant wrongfully created a risk of harm rather than actual harm.

Lawsuits may also be allowed pursuant to a state or federal statutory cause of action. Earlier this year, in *In re Horizon Healthcare Services Inc. Data Breach Litigation,*[10] the first

— and, thus far, only — federal circuit court of appeals to consider the issue found that a violation of the Fair Credit Reporting Act conferred standing by providing a private cause of action.

The court concluded the gravamen of the act is to prevent the compromise of personal information and said the imminent risk of future harm is inherent in data breaches.

Horizon Healthcare was decided after, and in contemplation of, two prior Supreme Court decisions that set a high bar for legal standing involving harm from a data breach.

In *Spokeo Inc. v. Robins*[11] the high court remanded the case because the plaintiffs focused solely on "particularization" and not the "concreteness" of their injury.

And in *Clapper v. Amnesty International*[12] the court rejected the plaintiffs' argument that standing existed merely because the plaintiffs expended money and time in an effort to prevent misappropriation of their data.

But perhaps this time is different. Because of the magnitude of the breach and the completeness of the data (making it seemingly a virtual certainty that the data will be misused), the Federal Trade Commission has exhorted consumers to check their credit reports, order a credit freeze, request fraud alerts, and file taxes early to prevent a criminal from filing them and intercepting a tax refund.

Because of the magnitude of the breach and the completeness of the data, the Federal Trade Commission has exhorted consumers to check their credit reports.

With artful pleading and guidance from the Supreme Court, consumers might have enough to satisfy the high standing standard.

Regulatory enforcement actions

Although consumers often do not have standing to sue based on a mere risk of harm, regulated companies have enforceable legal obligations regarding the security of the data entrusted to them. Regulatory enforcement actions can result in civil penalties, injunctive relief and corrective action programs.

Here, at least three regulators appear to have some overlapping authority over Equifax's information security program: the Securities and Exchange Commission, the Federal Trade Commission and the Consumer Financial Protection Bureau.[13]

All three agencies have jurisdiction to investigate the adequacy of cybersecurity controls, and they have already done so in enforcement actions against other companies. In September, both the FTC and CFPB announced investigations into the Equifax breach.

When publicly announced and substantial fines make headlines, often the most enduring and costly consequences are the corrective actions that companies must immediately undertake under the regulator's oversight.

For example, the health care industry learned long ago that corrective action programs imposed by the Department of Health and Human Services' Office for Civil Rights can last for years and cost many times more than accompanying fines.

Similarly, banks have for some time been subject to "matters requiring attention," a form of supervisory remediation imposed by the Office of the Comptroller of the Currency.

Although the FTC's interest in cybersecurity enforcement is relatively recent, and the CFPB itself is a relatively new agency, the CFPB did recently obtain a consent order against Dwolla Inc., an online payment service, for misleading consumers about its information security practices.[14]

Dwolla was required, among other things, to cease misrepresenting its information security practices, develop an information-security training and awareness program, pay a $100,000 fine, and retain an outside firm to conduct data-security audits annually for five years. Equifax's exposure in this regard could be substantial.

Criminal liability

Although it has been widely reported that one U.S. senator said about Equifax, "Somebody needs to go to jail," this statement was in reference to the insider trading allegations.

Charges pursuant to the "responsible corporate officer" doctrine can be brought only where authorized by law, such as via the federal Food, Drug and Cosmetic Act. And because there are not yet any allegations of mail fraud or wire fraud (that Equifax affirmatively deceived the public), the likelihood that any criminal liability will arise from this breach appears to be small.

One often overlooked piece of legislation is the Sarbanes-Oxley Act of 2002, which, among other things, imposes criminal penalties and requires signed reports from CEOs and chief financial officers detailing "all significant deficiencies in the design and operation of internal controls."

A false certification by the CEO and CFO under Section 906 may lead to the disgorgement of bonuses and other incentive-based compensation received in the prior 12 months, a fine of up to $5 million, and a term of imprisonment of up to 20 years.

It would not be unreasonable for the SEC to ask the following questions: How bad was Equifax's information security program at the time of the breach relative to industry standard best practices? How poorly was the information security program overseen by its senior leadership team? If the program was substandard and overseen so poorly that it constituted a significant deficiency or material weakness, should that have been disclosed to the SEC by the CFO and CEO?

Harm to reputation, goodwill and competitive advantage

Although other companies' reputations have largely recovered after data breaches, Equifax has been conspicuously ostracized because of the size of the breach, the potential harm and the perceived degree of negligence that made the breach possible.

In the first of what may be several business impacts, the Internal Revenue Service reportedly moved to suspend a contract under which Equifax would verify the identity of taxpayers.

To the extent that companies already have business dealings or would have such dealings with Equifax in the future, it is likely that they would demand adequate assurances from Equifax regarding the progress of its remediation, such as a Service Organization Control 2 Type II certification of examination.

A firm of Equifax's size and stature should already have been able to provide business partners with a SOC2 report, which is a generally accepted, industry standard means of declaring cybersecurity readiness.

Loss of market capitalization

After the breach, Equifax's common shares plunged from over $140 to less than $95. These losses were aggravated by public perception regarding Equifax's response to the breach, including the terms of its credit monitoring program and the intermittent unavailability of its website in the days immediately following the breach.

Moreover, investment may be hurt by recurring news that the breach affected more consumers than originally disclosed, and most recently, discovery that a key component of Equifax's website was redirecting users to a fake Adobe Flash download prompt that installs malware.

Although these losses have already led to a shareholder derivative suit,[15] one need only look to Target and TJX stock prices to realize that the investing public has a short memory regarding data breaches.

Whether Equifax's market capitalization rebounds depends on its ability to ride out the storm, provide adequate assurances to its customers as to its data security posture, and satisfy regulators' demands.

If Equifax has cyberinsurance coverage, some — but certainly not all — of these costs may be covered.

Remediation

The task of recovering from a breach of this size is considerable. It involves the orchestration of internal and external forensics experts, corporate and outside counsel, corporate communications (public relations), and what is left of the senior leadership team.

It would be impracticable to put a figure on the costs, but Equifax reportedly retained the forensic and incident response services of Mandiant, a seasoned and venerable firm.

Equifax also reportedly retained the white-shoe law firm WilmerHale, and possibly other high-priced firms, to assist with its internal investigations, media relations and breach notification obligations.

And there is invariably a substantial internal reallocation of information technology and information security resources in response to a breach, including diverting resources from other planned capital expenditure projects, augmenting information security staff (who command high salaries due to the shortage of experienced applicants) and outsourcing services to handle consumer inquiries.

CONCLUSION

The ultimate consequences of the Equifax breach, whether measured in terms of its effects on consumers, the impact on market capitalization, or the outcome of lawsuits and state and federal regulators' enforcement actions, have yet to be fully realized.

Breaches of this magnitude have become so common that they have given rise to a burgeoning cyberinsurance industry, an information security skills shortage, congressional and public attention, a focus on the national security implications of data security, and a nascent law practice specialization.

Indeed, as a result of this particular breach, passage of federal legislation on data breach notification is more likely than ever.

A trite adage in the information security industry is that there are two kinds of companies: those who have been hacked, and those who don't know they've been hacked.

Organizations that adopt industry-standard controls frameworks, risk management programs, layered defenses and incident response programs will limit their liabilities and be judged much more kindly after a hack than those that do not.

Those that do not will eventually be exposed by hackers or insiders, and any negligence on the part of the organization will also come to light, attracting the ire of regulators, shareholders and customers.

NOTES

[1] Rush, *Second Nature, on* Hold Your Fire (Mercury Records 1987).

[2] *Company Profile,* Equifax, http://bit.ly/2zJeDl2.

[3] Brenda R. Sharton & David S. Kantrowitz, *Equifax and Why It's So Hard to Sue a Company for Losing Your Personal Information,* Harvard Bus. Rev. (Sept. 22, 2017), http://bit.ly/2wV4Gf8.

[4] Tom Schoenberg & Anders Melin, *Equifax Stock Sales Said to Be Focus of U.S. Criminal Probe,* St. Louis Post-Dispatch (Sept. 18, 2017), http://bit.ly/2imeZEs.

[5] The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for Apache Struts Export, Apache Software Found.: Apache Software Found. Blog (Sept. 14, 2017), http://bit.ly/2fonFJ9

[6] *2017 Internet Security Threat Report,* Symantec, http://symc.ly/1Xsm4zz.

[7] Edgescan, Edgescan 2016 Vulnerability Statistics Report (2016), http://bit.ly/2nEU2sX.

[8] Lorenzo Franceschi-Bicchierai, *Equifax Was Warned,* Motherboard (Oct. 26, 2017, 11:19 AM), http://bit.ly/2yPij4B.

[9] *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015) (where the FTC alleged that Wyndham did not use encryption, firewalls and other commercially reasonable methods for protecting consumer data).

[10] 846 F.3d 625 (3d Cir. 2017).

[11] 136 S. Ct. 1540 (2016).

[12] 133 S. Ct. 1138 (2013).

[13] The FBI likely has an investigation underway regarding the perpetrators of the breach, but this is not in the context of regulatory oversight of Equifax.

[14] *In the Matter of Dwolla Inc.,* File No. 2016-CFPB-0007 (F.T.C. Mar. 2, 2016).

[15] Press Release, Levi & Korsinsky, Levi & Korsinsky LLP Announces Notice of Filing Securities Class Action Against Equifax Inc. and Certain Executive Officers and/or Directors, Yahoo Fin. (Sept. 11, 2017), https://yhoo.it/2yO3LPl.

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

ABOUT THE AUTHOR

Sean L. Harrington is a cybersecurity and privacy practitioner, digital forensics examiner in private practice, and adjunct professor of law at **Concord Law School**. He is admitted to the state bars of California and Wisconsin, is licensed by the Texas Private Security Bureau, and is a fellow of the Cybersecurity Institute. He is also a volunteer investigator with Minnesota's 4th Judicial District Ethics Committee and a council member of the Computer & Technology Law Section of the Minnesota State Bar Association. In addition, he has held several leadership posts with the Minnesota chapter of the High Technology Crime Investigation Association, Financial Services Roundtable, Financial Services Sector Coordinating Council and other associations. Harrington holds the CIPP/US, CISSP, CHFI, CSOXP, MCSE and CCFP certifications.