Margaret A. Reetz Partner
margaret.reetz@mendes.com
Gregory S. Mantych Associate
Mendes & Mount LLP, New York

Equifax data breach: this one may not go unnoticed

As the dust starts to settle on the Equifax data breach, in which nearly half of the US population's personal data was potentially compromised, Margaret Reetz and Gregory Mantych, of Mendes & Mount LLP, provide their analysis of the breach and the wide-ranging impact.

There are hacking incidents and then there are hacking incidents. The statistics so far:

- Impacted consumers: 145.5 million US; 15.5 million UK; 100,000 Canada.
- Lawsuits: two US states; two US cities; hundreds of class actions filed.
- Congressional hearings: four.
- Management changes: one CEO retired; two technology officers out.
- Regulator investigations: at least two federal; over 38 states.

The personal data of nearly half of the US population was potentially impacted as a result of a breach at the credit reporting company, Equifax. Such numbers are staggering, particularly considering that around a quarter of the population consists of minors, whose sensitive data hopefully would not have been submitted to the credit agencies. Was the handling of data and the response by Equifax a case study in what not to do? With such a large portion of the electorate at risk, and regulators ready to pounce, are lawmakers not far behind? Should the entire mechanism be scrapped in favour of a model not reliant on traditional identifiers?

There will be, and have been, proposals for new regulations but it remains to be seen whether there is the right mix of support and momentum for any one or more measures. While cyber security is not a 'top-of-mind' concern for American consumers, the sheer magnitude of this incident and how the company responded will not soon leave regulators' memories[1].

Initial reports

Equifax, one of the three US credit reporting bureaus, initially announced on 7 September 2017 that it had suffered a cyber security incident impacting approximately 143 million US consumers[2]. This figure had to be revised upward to 145.5 million[3]. Finally, the figure was revised to include consumers outside the US, although Equifax reports that there is no evidence that the attackers accessed databases located outside the US (15.2 million British consumers were impacted, and close to 700,000 of those will receive notifications from Equifax with offers of its own and another third party's risk mitigation tools; 100,000 Canadian consumers likewise were impacted)[4].

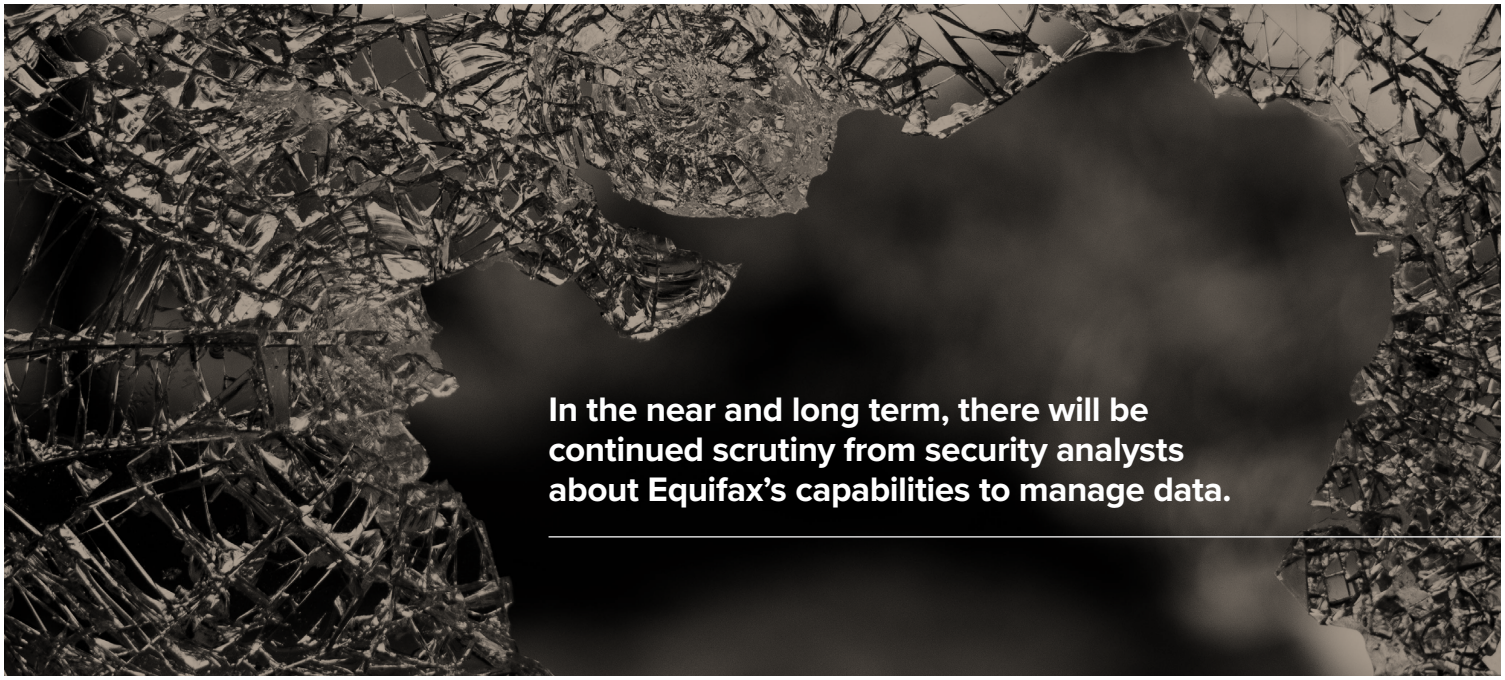
The credit reporting bureaus typically act to collect, compile and report on consumer information in the form of credit reports[5]. Ordinarily, credit reports are used by financial services entities (banks, credit card issuers) to support the issuance of mortgages, auto loans, credit cards and private student loans. They also may be used as a form of background check: rental housing, setting auto and homeowner's insurance policy premiums and even in certain employee hiring situations[6]. Thus, the influence and impact on consumers' lives is enormous. This also explains how it is that one entity would have access to and control over such a large swathe of consumers' sensitive data.

Equifax reported that the data breach resulted when "criminals exploited a US website application vulnerability," Apache Struts CVE-2017-5638[7]. Apache Struts is a piece of computer code used for creating web applications. Equifax reportedly used Apache Struts in whole or in part to create, support and/or operate its Dispute Portal[8]. Apache Struts is an 'open source code,' free and available for anyone to download, install, or integrate into their systems and is used by Fortune 100 to provide web applications in Java, powering front and back-end applications. Like many other pieces of open source code, it comes with no warranties of any kind, including anything to do with security. The flaw in this code reportedly dates back to March 2017[9]. Accordingly, regulators are now arguing that it was incumbent upon Equifax - and any company that uses Apache Struts (and presumably any open source code) - to assess whether it is appropriate and sufficiently secure for the company's purpose, noting that the software should have been updated to secure against known vulnerabilities[10].

For its part, Equifax still has not provided specific evidence regarding the cause of the breach but written statements in support of the former CEO's congressional testimony confirm some of the events. Former CEO Richard Smith has testified that the failure to patch a two month old bug was among the chief failures that caused the breach. Although a patch for the code execution flaw was available during the first week of March 2017, Equifax administrators did not apply it until 29 July, when Equifax first learned of the breach. In fact, an email that directed administrators to patch the critical vulnerability in the open source application framework was not followed[11]. In his testimony, Smith blamed a single unnamed IT employee. Equifax reports that its forensics vendor (Mandiant) has completed its investigation (as of the first week of October 2017) so, for now, this appears to be the extent of Equifax's account[12].

Public relations miscues

The initial response by Equifax was neither reassuring nor orderly. The announcements directed consumers to a link on the Equifax website and then instructed the consumer to enter the last six digits of their Social



In the near and long term, there will be continued scrutiny from security analysts about Equifax's capabilities to manage data.

Security Number. The process did not go well. Once entered, consumers received a notification that their data was potentially compromised and that they should check back with Equifax, without further explanation[13].

Also, there was the delay in divulging the breach. Equifax became aware of the intrusion on 29 July 2017 but it did not issue its press release until 7 September. To add insult to injury for consumers, one remedy offered was to request a credit freeze from the very same, apparently at risk, credit reporting bureaus - at a cost[14]. Some reporting suggests that the rollout was hurried, due to forces outside of the control of Equifax[15].

In the near and long term, there will be continued scrutiny from security analysts about the company's capabilities to manage data. The actual web portal for handling credit report disputes used a platform that commentators say is vulnerable in its own right. Equifax took that down but confidence is not at an all-time high for their ongoing practices and standards[16]. Finally, in what may be an 'irony-deficient' environment, the website banner taglines still read: '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.'

Investigations and litigation

States react first

The states of Massachusetts and New York wasted no time in pursuing actions and remedies on behalf of their constituents. The Massachusetts Attorney General's Office filed suit against Equifax as of 19 September 2017 seeking civil penalties, disgorgement of profits, restitution, costs and attorney's fees, citing that state's Consumer Protection Act and breach notification law[17]. The Massachusetts' Attorney General specifically alleges that Equifax failed to give timely notice. Governor Andrew M Cuomo of New York announced a "new action" to direct the State's Department of Financial Services to issue new regulations requiring credit reporting agencies to register with the Department in accordance with the State's "first-in-the-nation cybersecurity standard[18]." Presumably, the State is looking to make it clear that the New York State Department of Financial Services should have oversight and enforcement for such agencies[19].
In addition, the cities of Chicago and San Francisco have filed their own actions[20].

Congressional hearing and response

To date, there have been four hearings where legislators were unrestrained, animated and almost coarse in their statements and questions to the former CEO of Equifax, Richard Smith (these hearings were held by: the House Energy & Commerce Committee (Digital and Consumer Protection Subcommittee); the House Financial Services Committee; the Senate Banking, Housing, and Urban Affairs Committee; and the Senate Judiciary Committee (Privacy Technology and the Law Subcommittee)). There was no shortage of analogies, outrage and theatrics, resulting in something of a quote-fest:

"Because of this breach, consumers will spend the rest of their lives worrying about credit history. But Equifax will be just fine [and] it could actually come out ahead!" - Sen. Elizabeth Warren, Massachusetts.

"This may be the most harmful attack on a company's personal information the world has ever seen," - Rep. Jeb Hensarling, Texas.

"That looks like we're giving Lindsay Lohan the key to the minibar. I don't pay extra at a restaurant to prevent a waitress from spitting in my food (in reaction to the prospect that Equifax could make money from consumers rushing to get identity theft protection products)," - Sen. John Kennedy, Louisiana.

There are a few bills that have been introduced in the immediate aftermath. Senator Elizabeth Warren of Massachusetts introduced a measure that would force the credit bureaus to eliminate fees for credit freezes and to streamline the entire process. Some commentators feel that the situation adds insult to injury that a consumer is forced to use the very same credit bureaus that have drawn such critical scrutiny to put a 'freeze' on their credit files. The effect of the freeze, also known as a security freeze, restricts access to a consumer's credit report, thus making it difficult for a thief to open up a new unauthorised account in that consumer's name (certain entities may still have access)[21].

Other senators have introduced the draft Data Broker Accountability and Transparency Act to hold the data broker industry accountable for breaches. This Act would allow consumers to correct their information as shown in certain reports and allow consumers to restrict brokers from using, sharing or selling their personal information for marketing purposes. Such brokers would also be subject to enhanced requirements with respect to security, privacy and breach notifications[22].

continued

Regulatory and criminal investigations

The Federal Trade Commission ('FTC') has opened a probe into these events[23]. It also issued a statement: "The FTC typically does not comment on ongoing investigations. However, in light of the intense public interest and the potential impact of this matter, I can confirm that FTC staff is investigating the Equifax data breach[24]."

Three Equifax executives were permitted to sell more than $1.8 million worth of stock in the days following the 29 July discovery of the breach. Reportedly, the executives that sold the stock had not been informed of the breach at the time. The Department of Justice has now opened an investigation into these trades.

The Attorney Generals from 38 states sent a letter to Experian and TransUnion urging them to stop charging fees for credit freezes and fees to lift or temporarily lift credit fees, in light of the Equifax breach. This is also leading these Attorney Generals to draft legislation to ban or restrict fees for credit freezes (seven states already have similar legislation)[25].

Class actions filed

Not surprisingly, hundreds of class action lawsuits have been filed.

The class allegations are as to be expected: "[t]his action arises from one of the largest data security breaches ever to occur in the United States. As a result [...] millions of individuals whose sensitive personal data was made accessible now face substantial risk of further injury from identity theft, credit and reputational harm, false tax claims or even extortion[26]."

Plaintiffs allege that the "website Equifax set up and directed consumers to use to check whether their Confidential Personal Information had been compromised was itself fraught with security risks[27]." The causes of action include alleged violations of the Fair Credit Reporting Act, breach of fiduciary duty, negligence, breach of contract, invasion of privacy and unfair practices violations.

It looks like a consolidated action is likely headed to the Northern District of Georgia[28]. Plaintiffs' counsel have filed motions to transfer to the Federal District Court in Atlanta, to be heard before the Judicial Panel on Multi-District Litigation. Not only does Equifax maintain its headquarters in Atlanta, Georgia but plaintiffs' counsel notes in their motion that two other major data breach matters were handled there i.e. Home Depot and Arby's Restaurant Group.

Conclusion

When the dust settles

Some commentators are less than sanguine about the prospects of significant legislative accomplishments, even following what seems to be the granddaddy of all breaches[29]. There remains a great deal of confusion about the stranglehold that the credit reporting bureaus have over the consumer financial system and the best approach to insure the integrity of the system. Other commentators are looking at the entire infrastructure to see whether technological advances can resolve some basic issues. For instance, some advocates suggest replacing the reliance on the use of social security numbers as an identifier and moving toward biometrics or a blockchain equivalent.

One system touted is in use in Estonia, where the country has created a digital identification system[30]. For the time being, it is more likely that regulators in certain states like Massachusetts, Illinois, New York and California will put a great deal of pressure on all of the credit bureaus to force higher security standards, if not significant improvements to the responses to such incidents. Market forces ultimately may also prove to be a greater influencer in this sector.

1. According to a Pew Research Center study entitled 'Americans and Cybersecurity,' 26 January 2017, roughly half of Americans do not trust the federal government or social media sites to protect their data but, many fail to follow cyber security best practices and most do not worry how to secure online passwords, and even if the victim of a major data breach, they are no more likely to take additional steps to secure their personal information. See http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf
2. www.equifaxsecurity2017.com
3. http://fortune.com/2017/10/02/equifax-credit-breach-total/
4. http://www.independent.co.uk/news/business/news/equifax-cyber-attack-millions-client-records-compromised-credit-reporting-agency-uk-sensitive-a7993946.html; http://thehill.com/policy/cybersecurity/354749-equifax-says-nearly-700000-uk-consumers-impacted-by-breach
5. http://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf; the three largest nationwide consumer reporting agencies (NCRAs) - Equifax Information Services LLC (Equifax), TransUnion LLC (TransUnion), and Experian Information Solutions Inc. (Experian)
6. Ibid.
7. Commonwealth of Massachusetts v. Equifax, Inc., Case No. 1784-CV-03009 (Superior Court of Massachusetts, 19 September 2017).
8. Ibid. at 7.
9. http://www.zdnet.com/article/equifax-confirms-apache-struts-flaw-it-failed-to-patch-was-to-blame-for-data-breach/
10. Ibid.
11. https://arstechnica.com/information-technology/2017/10/a-series-of-delays-and-major-errors-led-to-massive-equifax-breach/
12. https://www.equifaxsecurity2017.com/frequently-asked-questions/
13. https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/after-data-breach-equifax-asks-consumers-for-social-security-numbers-to-see-if-theyve-been-affected/?utm_term=.5fc6c7c9fe56
14. https://krebsonsecurity.com/2017/09/heres-what-to-ask-the-former-equifax-ceo/
15. Ibid.
16. https://www.wired.com/story/equifax-breach-no-excuse/
17. G.L. c. 93A; G.L. c.93H; Commonwealth of Massachusetts v. Equifax, Inc., Case No. 1784-CV-03009 (Superior Court of Massachusetts).
18. See, 'Governor Cuomo Announces New Actions to Protect New Yorkers' Personal Information in Wake of Equifax Security Breach,' www.governor.ny.gov/news, September 18, 2017, Press Room. The attack may be linked to nation-state actors. See, https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros
19. N.Y. Fin. Serv. L § 102.
20. http://chicago.cbslocal.com/2017/09/28/chicago-lawsuit-equifax-data-breach/; the city's consumer fraud ordinance was updated in 2012 to allow for penalties as high as $10,000 dollars per victim per day, https://techcrunch.com/2017/09/27/san-francisco-sues-equifax-on-behalf-of-15-million-californians-affected-by-the-breach/
21. https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs
22. https://iapp.org/news/a/senators-introduce-legislation-following-equifax-breach/
23. https://www.engadget.com/2017/09/18/equifax-stock-sales-doj-investigation-insider-trading/
24. http://www.reuters.com/article/equifax-cyber-ftc/u-s-ftc-opens-probe-into-massive-equifax-hack-idUSFWN1LV0KN
25. http://www.illinoisattorneygeneral.gov/pressroom/2017_10/20171010b.html
26. Morris v. Equifax Inc. and Equifax Information Services LLC, Case No 3:17-cv-05815-MEJ (Oct. 10, 2017, U.S.D.C. No. Dist. Calif.), p. 3.
27. Ibid. at 4.
28. http://www.nationallawjournal.com/id=1202797902499/Lawyers-Begin-Move-to-Corral-Equifax-Class-Suits-Into-MDLslreturn=20170911104815; The consolidated cases are In re Equifax Inc. Data Breach Litigation, 2800, U.S. Judicial Panel on Multi-district Litigation.
29. http://www.pbs.org/newshour/rundown/equifax-breach-congress-unlikely-pass-new-rules-protect-consumer-data/
30. http://www.zdnet.com/article/data-breaches-highlight-how-social-security-number-has-to-be-phased-out-for-blockchain-biometrics/