Cybersecurity Law Report
An Acuris company

cslawreport.com

September 11, 2019

DATA BREACH LITIGATION

Lessons From Equifax on How to Mitigate Post-Breach Legal Liability

By Avi Gesser, Patrick Blakemore and Peter Bozzo, *Davis Polk*

On July 22, 2019, the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB) and 50 state and territorial attorneys general settled their claims against Equifax Inc. related to a massive 2017 breach of Equifax data. That settlement also resolves hundreds of civil consumer-fraud class actions brought against Equifax, but it does not address a securities-fraud class action that Equifax's shareholders brought against the company in the wake of the breach, which could still result in significant recovery for Equifax shareholders.

The Equifax settlement and the progress of the securities-fraud class action are instructive as to how civil and regulatory liability will play out for companies imperiled by large cyber events. Aside from loss of consumer and employee confidence, reputational damage and other losses resulting directly from a successful cyber attack, there are three large buckets of legal liability that companies face: (1) federal and state regulators, (2) classes of consumers and (3) classes of shareholders (for public companies).

See also "Reducing Risk in the Dawn of Equifax and Other Cyber-Related Securities Fraud Class Actions" (Feb. 13, 2019).

Regulatory Liability

The SEC, FTC, CFTC and state attorneys general all have a potential role in imposing civil penalties or other forms of liability in the aftermath of a cyber event.

SEC

The SEC can bring actions against public companies for failing to disclose in their quarterly filings that a material breach has occurred or providing materially misleading statements about a company's cybersecurity policies. The SEC pursued this course when Yahoo! Inc. failed to disclose a data breach for over two years, resulting in Yahoo!'s agreement to pay a $35-million civil penalty.

The SEC can also bring actions against certain regulated entities for failure to take reasonable steps to secure customers' personal information, including actions to enforce the "Safeguards Rule," 17 C.F.R. § 248.30(a), which requires registered broker-dealers and investment advisers to adopt written policies and procedures for protecting customer data. The SEC extracted a $1-million penalty from Voya Financial Advisors Inc. after the company suffered a cyber intrusion due to, among other things, Voya's failure to adopt reasonable written policies that complied with the Safeguards Rule.

See "SEC Risk Alert Highlights Policy Design and Implementation Failures and Roadmaps Future Enforcement" (Apr. 24, 2019).

FTC

The FTC, CFTC and state attorneys general can also pursue claims against companies that fail to take reasonable steps to protect customer data. For instance, Section 5 of the FTC Act prohibits certain unfair or deceptive commercial acts or practices, and the FTC has used this authority – as it did in Equifax's case – to impose liability on companies both for failing to adopt adequate security measures and for misrepresenting (or failing to disclose) weaknesses in those security measures.

See CSLR's three-part series on lessons from the FTC's 2018 Privacy and Data Security Update: "Enforcement Takeaways" (Apr. 24, 2019); "Financial Privacy, COPPA and International Enforcement" (May 1, 2019); and "Hearings, Reports and 2019 Predictions" (May 8, 2019).

CFTC

Similarly, the Commodity Exchange Act gives the CFTC the ability to bring enforcement actions for fraudulent or manipulative conduct in condition with interstate commodities markets.

State AGs

Relying on breach-notification laws enacted in all 50 states and the District of Columbia, state attorneys general may additionally bring claims against companies that fail to provide sufficient notice of breaches to consumers or directly to the attorney general's office. Many of those state statutes also require companies to take reasonable measures to protect personal information and allow the state attorney general to bring actions for violations.

See "The Growing Role of State AGs in Privacy Enforcement" (Nov. 28, 2018).

Consumer Class Actions

Following a major data breach, consumers often file class actions against the breached company, typically bringing claims for negligence and violation of state consumer protection laws (as well as, in some cases, claims for unjust enrichment, breach of contract/implied contract, or negligent misrepresentation). Immediately after the Equifax breach was announced, consumers filed complaints against the company alleging that it had willfully, recklessly or negligently failed to maintain adequate technological and cybersecurity safeguards to protect users' data from unauthorized access. Yahoo!, Target and Home Depot were subject to similar suits after data breaches exposed personal information held by those entities.

Shareholder Class Actions

For public companies, shareholders may bring actions to recover losses in the value of their shares following disclosure of a breach. These actions often depend on attributing the stock price decline to a company's fraudulent statements touting the quality of its cybersecurity programs – statements that, in the wake of a breach, were arguably revealed to be false or misleading. In addition to the Equifax litigation, Yahoo!, PayPal, Chegg and Marriott have all faced securities fraud class actions following breaches at those companies.

Shareholders may also bring derivative cases in the name of the company against the directors for mismanagement in failing to prevent cyber events or adopt adequate safeguards for mitigating and responding to them. For instance, following the Yahoo! breach, plaintiffs in shareholder derivative suits alleged that the company's officers and directors had failed to protect users' data, notify users of the breach and remediate the breaches – even as they sold some of their own Yahoo! shares. Those suits resulted in a $29-million settlement, the first significant recovery in a cyber-related derivative lawsuit following disappointing outcomes for plaintiffs' attorneys in cyber-related derivative suits brought against Wyndham and Home Depot.

Which of these three buckets of legal liability will end up posing the most serious threat to companies that have experienced a large data breach remains unclear, but all three are coming quickly in the wake of public breach disclosures.

Just a week after the Equifax settlement, Capital One announced a breach that affected approximately 106 million credit card applicants – including 140,000 customers whose Social Security numbers were stolen and 80,000 customers whose bank account numbers were compromised. Capital One already faces at least three consumer class action lawsuits arising from the breach and several state regulatory inquiries. Securities class actions will likely follow, considering that Capital One's stock price dropped significantly on the day the breach was announced, erasing over $1 billion in market capitalization. Indeed, plaintiffs' law firms are actively recruiting investors in Capital One to serve as lead plaintiffs in future securities lawsuits based on the decline in Capital One's share price following disclosure of the breach.

Equifax's Regulatory Settlement

Federal and state regulators are under increasing pressure to impose meaningful penalties on companies that have experienced data breaches and have not implemented adequate data safeguards. The regulatory portion of the Equifax settlement included $275 million in civil penalties imposed by the Consumer Financial Protection Bureau and state/territorial attorneys general, or approximately $1.87 on a per-consumer basis.

See "Learning From the Equifax Settlement" (Jul. 31, 2019).

Equifax's Consumer Class Action Settlement

To settle the consumer class actions and regulatory claims against it, Equifax agreed to pay $380.5 million (and potentially up to $505.5 million) into a fund that will, among other things, cover credit-monitoring services for affected consumers and compensate them for out-of-pocket expenses "fairly traceable" to the breach. With the personal information of as many as 147 million people affected by the breach, the total amount of the fund – even if fully funded with $505.5 million – corresponds to about $3.44 per consumer. Critics described the settlement figure as "grievously low," "too little, too late" and insufficient to actually deter misconduct or negligence by companies susceptible to data breaches.

Reasons for Small Settlements

Small settlements in consumer cases are largely due to the high bars for recovery. Plaintiffs

typically must prove that they suffered actual harm as a result of the data breach. But it is often difficult to know whether a particular consumer's data has been accessed or used, and even if that could be established, damages are hard to quantify if credit companies promise to make consumers whole for any losses and provide free credit and identity theft monitoring. Indeed, many large-scale consumer class actions arising from data breaches have been dismissed on the grounds that plaintiffs cannot even establish standing to bring the case because they cannot show that they have suffered any harm. Several courts have found that, where consumers could not point to specific, concrete injuries (such as fraudulent charges) resulting from a data breach, their injuries were hypothetical future harms insufficient to confer standing.

See also "The New Normal: Easier Data Breach Standing Is Here to Stay" (Feb. 6, 2019).

CCPA's Attempt to Address Deficient Monetary Recoveries

California has attempted to address the deficiencies and incentive structures that result in low recoveries in cyber-related consumer cases through the California Consumer Privacy Act (CCPA) of 2018. The statute permits certain users whose personal information is subject to unauthorized access to recover between $100 and $750 per breach (or actual damages, whichever is higher) if the breach results from a "business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." This statute – and comparable laws being proposed in other states – creates the possibility for more potent consumer class actions going forward.

In CCPA private suits, it may be difficult for businesses that experience a breach to prove that their security procedures were adequate, and the cases may involve extensive and perhaps embarrassing discovery into a company's cybersecurity practices. These factors, combined with the threat of significant statutory fines, may create more serious civil exposure for companies that have experienced large breaches.

See CSLR's two-part series on CCPA priorities: "Turning Legislation Prep Into a Program Shift" (Jun. 5, 2019); "Tackling Data Subject Rights Requests and Vendors" (Jun. 12, 2019); and its two-part series on preparing for the CCPA: "Securing Buy-In and Setting the Scope" (Feb. 27, 2019); and "Best Practices and Understanding Enforcement" (Mar. 6, 2019).

Equifax's Securities Fraud Litigation

The securities-fraud suit pending against Equifax presents another avenue for significant liability. In securities class actions (unlike consumer class actions), the plaintiffs are the company's shareholders, and the measure of damages is the loss in value of the company's stock resulting from its alleged misrepresentations or omissions. In Equifax's case, the date when the breach was announced saw Equifax's stock price close at $142.72. Eight days later, that value had declined to $92.98, a decrease of approximately 36 percent. Three months after the announcement, it had climbed back only to $116.83, reflecting an approximately $3-billion loss in market capitalization from the date when the breach became public.

Over the past few months, the securities-fraud case against Equifax has moved steadily forward. Plaintiffs filed suit on September 8, 2017, just one day after Equifax announced the breach. The court denied the defendants' motion to dismiss in relevant part on January 28, 2019, permitting the plaintiffs' claims against Equifax to proceed. The court held that plaintiffs had sufficiently alleged that Equifax made misleading statements about the quality of its cybersecurity protections and its compliance with data protection laws. Although the federal securities laws pose a heightened bar for pleading scienter, the court concluded that plaintiffs had cleared this bar by pointing to evidence that Equifax knew – based on pre-breach audit reports, investigations and warnings from employees – about the inadequacy of its security systems at the time it made statements touting them. Finally, the court concluded that plaintiffs had adequately alleged loss causation by pointing to a potential causal connection between revelations about Equifax's cybersecurity failings and the decline in its stock price.

In July 2019, the court denied Equifax's request to file an interlocutory appeal of the order on the motion to dismiss. Plaintiffs have also filed a motion for class certification, which defendants have opposed – in part on the ground that plaintiffs' damages methodology will overcompensate the plaintiff class by permitting them to recover for stock declines that resulted from the fact of the breach itself (as opposed to any alleged misrepresentations or omissions about Equifax's data security). The motion remains pending, and discovery is proceeding in the case.

Mitigating Cybersecurity Risk

The Equifax settlement and the pending class action securities case provide several important data points for companies trying to assess their cyber risks and how best to reduce those risks. Companies should review the settlement, as well as the measures imposed on other companies as part of cybersecurity resolutions, and see (1) how they compare, (2) whether there is significant risk that their cybersecurity will be viewed as inadequate or their statements about their cybersecurity will be viewed as inaccurate and (3) what steps they can take to reduce such risks.

Guidance on Achieving Reasonable Security From Equifax

The Equifax settlement provides insight into what regulators view as reasonable cybersecurity measures. As such, it provides some guidance for companies on how to (1) establish reasonable cybersecurity techniques to reduce the risks of civil and regulatory liability and (2) avoid regulatory and shareholder civil risk arising from public claims that the company's cybersecurity is "reasonable," "effective" or reflects "best practices," if such statements do not match how courts or regulators would view the company's data protection measures.

The settlement requires Equifax to:

- identify an employee who will be responsible for the company's information security initiative;

- annually review internal and external security risks and implement any measures necessary to mitigate or eliminate them;
- evaluate and test the efficacy of its security measures;
- adopt (and enforce) written policies or guidelines aimed at implementing an enhanced information security program;
- offer regular training programs on cybersecurity issues, including at least annual training on security awareness for all employees;
- keep the board of directors (or a relevant subcommittee) updated about the company's information security program; and
- ensure that third parties with access to Equifax data are employing sufficient cybersecurity measures.

Top Ten Data Protection Measures

Ten examples of specific steps companies are taking to implement the kinds of requirements set forth in the Equifax settlement and reduce their cyber risk include the following:

1. mapping where personal information and sensitive data are collected and stored in the company, and knowing what is connected to the network;
2. encrypting sensitive data on the network and on portable devices such as laptops;
3. implementing multi-factor authentication for remote logins to their networks, and discontinuing access through webmail programs;
4. granting employees access only to the parts of the network that they need to do their work;
5. limiting the number of individuals with administrative computer privileges, as well as the length of time privileged access is granted;
6. ensuring prompt adoption of software patches and updates;
7. conducting regular penetration testing and vulnerability assessments;
8. monitoring computer networks for suspicious behavior and unauthorized activity by employees; and
9. Maintaining an updated incident response plan, and conducting annual tabletop exercises to the plan; and
10. Having a data minimization policy that allows for the identification and deletion of old sensitive data that is no longer needed for business, legal or regulatory purposes.

Avi Gesser is a partner in Davis Polk's litigation department, representing clients in a wide range of cybersecurity issues and counseling companies that have experienced cyber events.

Patrick Blakemore is an associate in Davis Polk's litigation department.

Peter Bozzo is an associate in Davis Polk's litigation department.