Courts and State Legislatures Broaden Claims Available to Cybersecurity Whistleblowers

February 13, 2020

Like the years immediately preceding it, 2019 marked another banner year for cybersecurity whistleblowers. Lawsuits relating to deficient corporate cybersecurity practices survived challenges in securities litigation and under the False Claims Act ("FCA"). The U.S. Department of Justice ("DOJ") settled its first FCA case arising from a cybersecurity vulnerability. And over the course of the year, 31 states enacted legislation addressing cybersecurity issues. These actions have further established the legitimacy of cybersecurity deficiencies as a basis for liability under federal and state law and have further strengthened protections for whistleblowers who report such concerns internally or to regulators.

Several courts issued decisions in 2019 finding that allegedly deficient cybersecurity practices could form the basis for liability under the FCA and the securities laws. A critical link between these two types of cases is that they are both subject to the heightened pleading standard under Federal Rule of Civil Procedure 9(b), because they both fundamentally involve allegations of fraud, which must be pleaded "with particularity." Among other things, this requires specific allegations of scienter, another word for intent or knowledge of wrongdoing. While courts across the country have established different standards for a showing of scienter, the threshold can generally be met through plausible allegations that the defendant had "(1) a motive and opportunity to commit the fraud; or (2) strong circumstantial evidence of conscious misbehavior or recklessness." *Gagnon v. Alkermes PLC*, 368 F. Supp. 3d 750, 772 (S.D.N.Y. 2019) (citation omitted).

Courts Rule in Cybersecurity Cases Tried under Securities Laws

In a January 2019 decision, a federal court in Georgia rejected the majority of Equifax's arguments that its alleged misstatements concerning its cybersecurity practices were not actionable under Section 10(b) of the Securities Exchange Act of 1934 and 17 C.F.R. § 240.10b-5, which prohibit publicly traded companies from making false or misleading statements to investors. *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189 (N.D. Ga. 2019). The investors in that case noted that while Equifax was experiencing a massive data breach – allegedly caused by its own deficient cybersecurity practices – it was simultaneously and emphatically touting the strength of its cybersecurity practices to investors. *Id.* at 1217–32. The court found that not only had the plaintiffs adequately alleged that these statements were false and misleading, they had also sufficiently alleged scienter on the part of Equifax and its CEO, Richard F. Smith. *Id.* at 1233–47. The court did, however, dismiss claims against three other Equifax executives for failure to establish scienter. *Id.* The court later rejected Equifax's effort to seek an interlocutory review. *In re Equifax Inc. Sec. Litig.*, No. 1:17-

CV-3463-TWT, 2019 WL 3449673 (N.D. Ga. July 29, 2019).

In another decision, a California court found that a plaintiff's case could not be dismissed for failure to state a claim because he had sufficiently alleged that public statements made by PayPal concerning a data breach were misleading. *Sgarlata v. PayPal Holdings, Inc.*, 409 F. Supp. 3d 846, 855–56 (N.D. Cal. 2019). The court then found, however, that the plaintiff had failed to allege scienter, and granted PayPal's motion to dismiss. *Id.* at 861. Despite this negative result, both the *Equifax* and *PayPal* decisions demonstrate that cybersecurity vulnerabilities may lead to violations of securities laws – and therefore may also give rise to a viable whistleblower tip to the SEC. For related reasons, were an employee to face retaliation because she opposed cybersecurity vulnerabilities – particularly those that led to misrepresentations to investors – she could find herself with a strong claim under the Sarbanes-Oxley Act anti-retaliation provision and potentially other whistleblower protection laws.

Cybersecurity Deficiencies Lead to Liability under the False Claims Act

In the FCA context, in May 2019, a California court denied a motion to dismiss a lawsuit filed by Brian Markus, Aerojet's Senior Director of Cyber Security, Compliance, and Controls, who discovered that the company was knowingly failing to comply with federal cybersecurity guidelines. *United States v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240 (E.D. Cal. 2019). Among other things, Mr. Markus alleged that Aerojet had failed to fully disclose its noncompliance with Department of Defense rules requiring defense contractors to safeguard certain technical information from cybersecurity threats. The court rejected several Aerojet arguments that its alleged failure to comply with those rules was immaterial and permitted the case to move forward.

Cybersecurity whistleblowers celebrated a blockbuster win in July 2019, when the DOJ settled its first qui tam case arising from a government contractor's cybersecurity vulnerabilities. That case was filed by whistleblower James Gleen, whose 2011 qui tam suit alleged that Cisco Systems, Inc., sold video surveillance products to the federal government containing cybersecurity flaws so significant that they not only compromised the product itself, but potentially compromised any computer or system connected to the product. Cisco paid the government $8.6 million to resolve the claims that its actions violated the FCA. For more about the Cisco case, *see* Alexis Ronickher, *Cisco FCA Deal Shows Viability Of Cybersecurity Qui Tams*, Law360 (Aug. 5, 2019), https://www.law360.com/articles/1184931.

States Enact Legislation Advancing Cybersecurity Regulations

In addition to federal court decisions improving the landscape for cybersecurity whistleblowers under federal law, dozens of states passed laws in 2019 that implicate cybersecurity issues. According to the National Conference of State Legislatures, 31 states enacted cybersecurity-related legislation in 2019. *See* NCSL, *Cybersecurity Legislation 2019* (Jan. 10, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx. Among other advances, New York passed a law requiring businesses to implement reasonable data security to protect the private information of New York residents; Indiana passed a law requiring wastewater treatment plant applicants to include a cybersecurity plan in their applications; Oregon passed a law requiring manufacturers selling connected devices to install reasonable cybersecurity features; several states passed laws that require insurers to develop and maintain information security programs; and several states passed laws that create cybersecurity standards for managing their elections. A number of states also created statewide cybersecurity agencies, which may lead to yet more significant protections in the future.

Increased Protections for Cybersecurity Whistleblowers

Due to the lack of any comprehensive bill protecting whistleblowers from retaliation for reporting cybersecurity vulnerabilities, every law passed to establish legal and binding cybersecurity requirements creates another potential avenue for relief for whistleblowers committed to ensuring that their employers treat customer, client, and third-party data with care. This is because in many of these states, as Alexis Ronickher explains in the Cybersecurity Whistleblower Protection Guide, if an employee is terminated because she opposed violations of these cybersecurity laws, she could have a claim against her employer for wrongful termination in violation of public policy. Likewise, when litigation under federal laws with anti-retaliation provisions leads to court decisions holding that misconduct relating to cybersecurity constitutes a violation of those laws, or to public settlements by government regulators, whistleblowers have a stronger argument that their efforts to ensure compliance with those laws are protected from retaliation. For these reasons, 2019 was another excellent year for cybersecurity whistleblowers and their advocates, who enter 2020 with more and better supported avenues for relief.