KATZ BANKS KUMIN

Implications of the FCC's Recent Cox Communications Settlement for Cybersecurity Whistleblowers

By Alexis Ronickher
November 17, 2015

On November 6, 2015, for the first time, the Federal Communications Commission (FCC) fined a cable company for failing to adequately protect customer information. Cox Communications agreed to pay $595,000 to resolve the FCC's investigation into an August 2014 breach that compromised the personal information of approximately 60 of its cable customers.

The FCC's enforcement action did not involve a whistleblower; however, it is important for cybersecurity whistleblowers for two reasons. First, it shows that lax cybersecurity and a company's failure to adequately protect customer data do not have to culminate in a mega breach to violate federal law. According to the FCC, the cable provider violated the Communications Act, even though only 60 customers were affected by the cyber breach, because Cox failed to take the necessary actions to prevent unauthorized access to the personally identifiable information of those customers.

In the cybersecurity whistleblower context, companies often attempt to defend against retaliation claims by arguing that the whistleblower could not have reasonably believed that the security problem could have resulted in the company violating any laws, given that there was no serious threat of a significant breach. The Cox settlement counsels against such flippant dismissals of whistleblower concerns. Companies that ignore whistleblowers because they think that the reported problems will not result in a catastrophic data breach and, instead, retaliate against whistleblowers when they continue to raise those concerns cannot avoid liability by arguing that the whistleblowers' belief that there was a legal violation was unreasonable. Given the FCC's enforcement action in this case, it is reasonable for whistleblowers to believe that cybersecurity vulnerabilities that could result in even just a small breach could violate federal law, depending on the circumstance.

Second, the FCC's action against Cox demonstrates that the federal government's focus on cybersecurity is not limited to publicly traded companies. It is true that the Securities and Exchange Commission has been very vocal regarding its interest in regulating cybersecurity in public companies and market participants. And, it is true that this stated interest provides a strong basis for whistleblower protection under the Sarbanes-Oxley Act (SOX) and the Dodd-Frank Act for employees of public companies who blow the whistle on cybersecurity issues. The FCC's action, however, was against Cox Communications, a private company, whose parent company, Cox Enterprises, is also privately held, meaning that both are outside the scope of SOX and Dodd-Frank whistleblower protections. Employees of private companies like Cox, however, who report or oppose violations of federal laws like the Communications Act may be covered by state laws that prohibit companies from terminating an employee for reporting or opposing unlawful conduct. Not all states protect whistleblowers who report violations of federal law, but many do, such as California, the District of Columbia, Illinois, and Massachusetts. In such jurisdictions, employees of private companies who report cybersecurity issues that could reasonably violate federal law are protected from being wrongfully terminated.

As we have pointed out in the past, in our experience, most cybersecurity whistleblowers are looking out for the best interests of the company they are working for. If companies commit to actively addressing the cybersecurity vulnerabilities raised by these conscientious employees (even if those vulnerabilities initially appear minor), they will both have a more robust cybersecurity posture and avoid significant legal liability—both for the underlying federal violation and unlawful retaliation.