akerman

Practice Update

FCC Settles Data Breach Investigation with Cox Communications

November 20, 2015

By Scott M. Kessler

Recently, the Enforcement Bureau of the Federal Communications Commission (FCC) entered into a settlement with Cox Communications (Cox) resolving an investigation into whether the cable operator failed to properly protect its customers' personally identifiable information (PII) when its electronic data systems were breached in 2014. Cox is the third-largest cable television provider and the seventh-largest telephone carrier in the United States with over six million subscribers. This settlement presents the FCC's first privacy and data security enforcement action with a cable operator, echoing steps the FCC has recently taken against telecommunications providers to regulate and enforce privacy and cybersecurity breaches.

The Breach

Cox's electronic data systems were breached in August 2014 by a hacker using the alias "Evil Jordie," a member of the band of teenage cybercriminals known as the Lizard Squad. Evil Jordie simply called Cox and posed as a member of Cox's information technology department. He convinced both a Cox customer service representative and a Cox contractor to provide him with their account IDs and passwords and enter them into a "phishing" website.

Related People

Scott M. Kessler

Related Work

Data Privacy and Security
Litigation

Related Offices

New York

“With those credentials, the hacker gained unauthorized access to Cox customers’ personally identifiable information, which included names, addresses, email addresses, secret questions/answers, PINs, and in some cases partial social security and driver’s license numbers of Cox’s cable customers, as well as Customer Proprietary Network Information (CPNI) of the company’s telephone customers,” the FCC said. “The hacker then posted some customers’ information on social media sites, changed some customers’ account passwords, and shared the compromised account credentials with another alleged member of the Lizard Squad.”

Enforcement of the Communications Act

The Communications Act (47 U.S.C. § 151 et seq.) requires that a cable operator shall not disclose PII of any subscriber without the prior consent, in written or electronic form, of the subscriber. In addition, the Communications Act requires cable operators to take all such actions as are necessary to prevent unauthorized access to PII by a person other than the subscriber of cable operator. Under 47 U.S.C. § 522(5), the term “cable operator” means any person or group of persons (A) who provides cable service over a cable system and directly or through one or more affiliates owns a significant interest in such cable system, or (B) who otherwise controls or is responsible for, through any arrangement, the management and operation of such a cable system.

The FCC’s investigation found shortcomings in Cox’s readily available measures for all of its employees or contractors that might have prevented the use of compromised credentials by the hacker. The Enforcement Bureau also determined that Cox failed to report this breach to the FCC’s data breach portal, as required by law.

The Settlement

Cox agreed to pay a civil penalty of $595,000, and the FCC required the carrier to identify all affected customers, notify these customers of the breach, and to provide the customers with one year of free credit monitoring

As part of the settlement, Cox has agreed to adopt a comprehensive compliance plan, which includes establishing an information security program. The mandates of this plan include annual system audits, internal threat monitoring, penetration testing, and additional breach notification systems and processes to protect customers' PII. Further, the Enforcement Bureau of the FCC will monitor Cox's compliance with the consent decree for seven years.

This action should be taken as a signal that the FCC, along with the FTC and SEC, intend to monitor and police data breaches more vigilantly and fine carriers that fail to diligently safeguard its customers' PII. Companies that provide communication services, such as cable, wireless, and DSL companies, must take customer email account security seriously and should consider offering a two-step authentication so that if customer account credentials get phished, lost or stolen, the attackers still need that second authentication factor to access any personal information.
