BROOKS PIERCE

FCC Fines Cable Operator Following Data Breach

Digital Media and Data Privacy Law Blog

By J. Benjamin Davis on 11.17.2015
Posted in Data Breach, FCC Matters

The FCC has been flexing its muscles in 2015 when it comes to enforcing data security requirements. In April, it reached a $25 million settlement with AT&T Services, Inc. for failing to safeguard customers' personal information. In July, it reached a $3.5 million settlement with TerraCom, Inc. and YourTel America, Inc. to resolve similar claims. Earlier this month, the FCC announced it had reached a $595,000 settlement with Cox Communications, Inc. ("Cox") to resolve the Enforcement Bureau's investigation into whether Cox failed to properly protect its customers' personal information when its data systems were breached in an August 2014 incident. This marks the FCC's first data security enforcement action against a cable operator.

The August 2014 security breach that drew the Bureau's attention involved a member of the Lizard Squad hacking group. In a classic "pretexting" attack, the hacker convinced a Cox customer service representative and a Cox contractor over the phone that he was with Cox's IT department. He then sent them a link to a malicious website that mimicked the look of Cox's corporate intranet site, where they entered their Cox IDs and passwords. Using this information, the hacker gained unauthorized access to former and current Cox customers' personally identifiable information, including names, addresses, email addresses, and PINs, as well as partial Social Security numbers and partial driver's license numbers.

The hacker then proceeded to post some customers' information on social media sites, change some customers' account passwords, and share other data to fellow Lizard Squad members. According to the FCC's consent decree, a total of 61 Cox customers had their data exposed. The resulting FCC fine comes out to almost $10,000 per customer---why so steep? (The $25 million fine the FCC imposed on AT&T came out to roughly $90 per affected customer.)

One reason is that, while Cox promptly reported the incident to the FBI, it never reported the breach to the FCC's data breach portal. The FCC's regulations implementing Section 222 of the Communications Act require that breaches be reported to the portal within seven business days; the FCC shares information collected from the portal with the FBI and U.S. Secret Service to facilitate any breach related investigation.

In addition, while the FCC acknowledged that Cox had some defenses in place, it noted that those defenses (as well as related training) were inadequate. "At the time of the breach, Cox employed multifactor authentication for some employees and third party contractors with access to Cox

electronic data systems, but not for the compromised employee or contractor," the FCC noted in the consent decree. "Cox's internal policies and training programs expressly prohibited Cox employees and third party contractors from disclosing access credentials to anyone and warned against pretexting attacks." (This last part would seem to help Cox's case, but the success of the pretexting attack in the face of such warnings and prohibitions likely gave the FCC the impression that Cox's training and testing programs were not reasonably robust.)

In addition to paying the fine, Cox agreed to identify and notify all affected customers of the breach and provide them with a year of free credit monitoring. Cox also agreed to, among other things:

- Develop and implement a compliance plan;
- Designate a senior corporate manager to serve as a Compliance Officer, who will work with a Chief Privacy Officer (who must be a certified privacy professional), and a Chief Information Security Officer to develop, implement and administer the compliance plan;
- Conduct a comprehensive privacy risk assessment;
- Review and revise its written information security program;
- Maintain policies and procedures for third-party vendor oversight, including multifactor authentication;
- Use multifactor authentication across the company for employees with access to confidential customer information;
- Implement a more robust data breach response plan (including annual test exercises) and subject the plan to third-party review;
- Review and revise its compliance manual; and
- Ensure privacy and security awareness training is provided to employees and third-party vendors.

The FCC will monitor Cox's compliance with the consent decree for the next **seven years**.

With this third data privacy enforcement action of 2015, the FCC is sending a clear signal that it intends to aggressively enforce the Communications Act's requirements that customer information be protected (and that security breaches be promptly reported to the FCC). While Cox's information security program may have enabled it to limit the incident to a relatively small number of customers, the fact remains that the breach exposed a number of shortcomings. Cox's customer service representative and third party vendor fell for a classic "pretexting" scam, Cox failed to enact multifactor authentication across the enterprise (which would have helped prevent the hacker's attack from succeeding), and Cox never reported the breach to the FCC's data

security portal. Unfortunately for Cox, those factors helped make this an “easy” case for the FCC, as well as a cautionary tale for others in the industry.