Mendoza Law, LLC

1000 University Ave., W. Suite 222
Saint Paul, MN 55104
651-330-8062 (Main)
www.mendozalawoffice.com

Anthony S. Mendoza, Esq.
Direct Dial: 651-340-8884
tony@mendozalawoffice.com

FCC DELVES INTO CYBERSECURITY

The FCC has become one of a long list of federal agencies that consider cybersecurity enforcement to be part of their jurisdiction. In July 2015, the FCC fined TerraCom, Inc. and YourTel America, Inc. $3.5 million for failing to password protect information gathered from low income customers under the FCC's Lifeline telephone assistance program. To evaluate eligibility for the Lifeline program, TerraCom and YourTel collected sensitive personal information from customers. Customers submitted this information to the companies via electronic forms and scanned images of sensitive personal documentation. A third party vendor used by the companies failed to use password protection of the personal data stored while it was conducting a server upgrade. The personal information of 300,000 customers was accessible over the public internet. The data base was breached in 2013.

In November 2015, the FCC fined Cox Communications $595,000 after an 18 year old hacker based in the U.K. named "Evil Jordie" (who has subsequently been arrested) used a pretexting scheme, posing as a member of Cox's IT department, to convince a Cox CSR and a Cox contractor to enter their account IDs and passwords into a fake Cox website. The hacker was then able to use those credentials to access Cox's databases containing personal and sensitive information about Cox subscribers. The hacker posted some of this subscriber information on social media sites, changed the passwords of Cox customers, and shared some of the information with another hacker. Cox learned of the breach on August 12, 2014. Cox contacted the FBI on August 18, 2014. Cox did not disclose the breach through the FCC's data breach reporting portal. Cox notified all but two affected customers on September 16, 2014.

The Enforcement Bureau investigation focused on whether Cox violated 47 U.S.C. section 222 and FCC rules issued thereunder, otherwise known as the FCC's Consumer Proprietary Network Information (CPNI) rules. Specifically, the Bureau investigated whether Cox:

- Failed to properly protect the confidentiality of Cox customers' CPNI;
- Failed to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI;
- Failed to provide timely notifications to law enforcement;
- Failed to monitor breached data online;
- Failed to notify all affected customers of the breaches.

In addition to the fines, in both cases, the parties entered into similar consent decrees. Cox agreed to:

- Appoint a senior Compliance Officer;
- Develop a consumer privacy law Compliance Plan, which must include:

    - Develop a comprehensive risk assessment using the NIST Cybersecurity Framework;
    - Develop an Information Security Program, including: (i) Administrative, technical, and physical safeguards; (ii) Reasonable measures to protect CPNI collected or maintained by third parties; (iii) Policies and procedures to identify the nature and extent of CPNI collected and maintained by Cox and third parties related to Cox, minimize the number of employees who have access to such information, minimize the amount and type of CPNI collected, and collect CPNI in a secure manner; (iv) Periodic reviews and evaluation of the Program; (v) Monitoring of critical points for security events; (vi) Conducting annual audits of selected call centers and customers service processes; (vii) Conducting annual penetration testing; and (viii) Developing an internal threat detection program.
- All off-network access by third parties must be authenticated through a site-to-site VPN.
- Conduct a formal assessment into multi-factor authentication and migrate all third parties to multifactor authentication.
- Develop an Incident Response Plan.
- Review its breach notification procedures.

Cox further agreed to the following remediation measures:

- Offer complimentary credit monitoring to customers whose data has been compromised.
- Monitor known websites for breach activity to identify data belonging to customers affected by the breach;
- Notify all customers Cox learns were affected by the breach.
- Send a copy of the Consent Decree to all employees.
- Establish new operating procedures the aid compliance with the Consent Decree.
- Develop or revise a privacy law Cox compliance manual and distribute the manual to all employees.
- Review, revise, and implement new privacy law training for all employees to ensure future compliance with Consent Decree. Training must be done annually.
- Not allow any employee or third party who has not been trained to the new compliance manual to interact with any Cox customer until such training has been completed.
- Report any noncompliance events within 15 days after discovery.
- File periodic compliance reports for 3 years.

On April 1, 2016, the FCC also opened a Broadband Privacy docket (WC Docket No. 16-106). In the *Notice of Proposed Rulemaking*, the FCC seeks comment on whether to create a broadened definition of CPNI derived from broadband services. CPNI is a term that has generally applied to telephone services, but with the FCC's recent reclassification of broadband as a Title II

telecommunications service in its so-called Net Neutrality Order, the FCC seeks to include CPNI that broadband carriers obtain from customers. The types of information the FCC proposes to include in the definition include: e-mail addresses, phone numbers, MAC addresses, IP addresses, internet browsing history, service plan information, and certain information about customer premises equipment (CPE). One of the more controversial aspects of the FCC's proposed rules is the inconsistent treatment of internet service providers, such as cable and telephone companies, and content providers such as Google and Facebook. As proposed, the FCC rules would apply only to ISPs, and not to content providers.

The proposed rules would:

- Allow the use of CPNI for the purpose of marketing a companies' own broadband services, but such companies would be required to allow customers to opt-out of such use. Customers would have to opt-in to any other use of their CPNI.
- Require companies to notify customers at the point of sale and on-line about the terms of their privacy policies.
- Require companies to perform risk assessments, conduct training, appoint a compliance officer, utilize robust authentication procedures, and hold accountable third parties with whom a company shares their CPNI.

The initial comment period on the FCC's Broadband Privacy rules has expired. Reply comments are due July 6, 2016.