October 30, 2014

The Federal Communications Commission (FCC) has taken its first big step into the regulation of data security by fining two affiliated telecommunications carriers a total of $10 million for failing to protect personal information, such as Social Security Numbers and drivers licenses, of some 300,000 consumers. The FCC's action drew sharp dissents from the two Republican Commissioners who argued that the FCC exceeded its authority and imposed penalties without first providing fair notice that these actions were unlawful under the Federal Communications Act. As a result of the FCC's actions, at least for telecommunications carriers, it is now explicitly a violation of the Federal Communications Act to:

- Fail to properly protect consumers "proprietary information" even when stored on a third-party's servers;
- Represent to consumers that the company will take appropriate steps to protect data and not provide the promised protections; and
- Fail to provide notification to all potentially affected consumers of a breach.

The FCC's actions have implications not only for telecommunications carriers, but also potentially for vendors that the carriers use to obtain or store proprietary information about their customers or applicants for service.

The FCC's order

The two carriers in this action provide subsidized telephone service to eligible low income consumers. Applicants for the subsidized services must (a) demonstrate need and (b) submit a Social Security Number, a driver's license, tax returns, statements regarding government benefits or other documents establishing income level. The two carriers retained a third party vendor to provide various services, including software and electronic storage on dedicated data servers (belonging to yet another service provider) to house the collected information. According to the Order, the data was stored in clear, readable text and in electronic format accessible via the Internet using simple searches. In 2013, an investigative reporter discovered that this information was being stored on an unprotected Internet site and accessed "at least 128,066 confidential records and documents" and then alerted the company.

Statutory violations

Section 222(a) of the Communications Act

The FCC found that the two carriers violated section 222(a) of the Communications Act, which requires carriers to protect "propriety information" of its "customers." Section 222(a) imposes a duty on telecommunications carriers to protect the confidentiality of "proprietary information" of "customers." This section is part of Act's customer proprietary network information ("CPNI") provisions. The FCC had not previously defined the term "proprietary information" outside the context of network-related information. In this order, the FCC interprets "proprietary information" (PI), to include "private information that a customers have an interest in protecting from public exposure," such a trade secrets, privileged information and personally identifiable information. Additionally, the FCC found that the duty to protect PI applies to applicants for service, as well as "customers" and is triggered when "the carrier accepts confidential private information" as part of application process.

The Order, however, was not clear in the degree of data protection that would be necessary to satisfy Section 222(a). In this particular case, the companies' security measures "lacked even the most basic features to protect PI." The PI, which was hosted

on a third-party vendor's server, was "widely available on public websites online through a simple Google search." The companies' use of random URLs without password protection or encryption, was insufficient. The FCC imposed a fine of $8.5 million for apparently violating section 222(a).

Section 201(b) of the Communications Act

Section 201(b) of the Act bars telecommunications carriers from engaging in any "unjust or unreasonable" practice. The FCC has never before applied this section to data security practices, yet found here that the failure to protect and secure PI constitutes an unjust and unreasonable practice. The FCC cited two reasons for this finding: (1) the companies failed to employ even the most basic and readily available technologies and security features; and (2) the companies' data practices created an unreasonable risk of authorized access. For example, the companies use URLs with the consumers' names in plain text, according to the Order. An investigative reporter was able to access and download approximately 128,066 proprietary records. Recognizing that this was the first case in which 201(b) was applied to data security practices, the FCC did not impose a fine with respect to this violation but warned carriers that the "Commission is committed to aggressive enforcement of unlawful practices to cyber security and data protection."

The FCC also found that the companies' privacy policies and statements on their websites misleadingly claimed they would protect the security of customer specific information from unauthorized access. The FCC found that this representation was "false, deceptive and misleading." Citing a joint FCC/FTC policy statement that "indicated" that marketing practices found deceptive or unfair under the FTC Act would also constitute an unjust or unreasonable practice under 201(b), and imposed a fine of $1.5 million.

Finally, the FCC found that failure to notify all potentially affected consumers of a security breach constitutes an unjust or unreasonable practice. The companies claimed that they had notified 35,129 of the more than 300,000 consumers whose data was exposed, consistent with the requirements of state breach notification laws. Find that all of the records stored on the servers were "at risk," the FCC concluded the companies should have notified all of the 300,000 customers. The FCC stated it would review notifications on a case by case basis but it expected carriers to "act in an abundance of caution—even to the extent of being overly inclusive" when notifying consumers.

Implications

As stated above, this first meaningful foray into data protection and privacy by the FCC carries some wide ranging implications. First, it means another regulator besides the FTC has gotten involved in privacy and security on behalf of consumers. Second, the FCC has stated its intent to pursue aggressive enforcement in this area. Carriers and, indirectly entities that provide data collection and storage for carriers, have been warned. Third, a finding by the FCC that a privacy or security practice is unjust or unreasonable could permit a private action in federal court for damages (including attorney's fees) under sections 206 and 207 of the Communications Act. Here, the FCC seemed to think persons might suffer compensable damages stating that "affected consumers face years of hassle and significant expense of credit monitoring to prevent permanent financial harm." Fourth, companies responsible for personal information must consider whether and how those obligations related to protecting that information could be flowed down through all levels of service providers.

Finally, the FCC found that failure to notify all potentially affected consumers of a security breach constitutes an unjust or unreasonable practice. The companies claimed that they had notified 35,129 of the more than 300,000 consumers whose data was exposed, consistent with the requirements of state breach notification laws. Finding that all of the records stored on the servers were "at risk," the FCC concluded the companies should have notified all of the 300,000 customers. The FCC stated it would review notifications on a case by case basis but it expected carriers to "act in an abundance of caution—even to the extent of being overly inclusive" when notifying consumers.

Key Contacts

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090