wiley

NEWSLETTER

Another Federal Regulator Enters the Fray on Privacy and Data Security

November 2014

On October 24, 2014, the Federal Communications Commission (FCC or Commission) confirmed that an additional cop is on the beat when it comes to privacy and data security. The FCC released a Notice of Apparent Liability for Forfeiture (NAL) proposing a fine of $10 million to two communications companies for violations of the Communications Act (the Act) based on the carriers' alleged inadequate data security measures. *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, FCC 14-173 (released Oct. 24, 2014).

The NAL alleges that the carriers, TerraCom, Inc. and YourTel America, Inc. (collectively, the Companies) stored proprietary information (PI) collected from consumers used to verify eligibility for the Commission's Lifeline program in an easily accessible format on the Internet and then failed to notify affected consumers after learning that the information was publicly accessible.

The NAL alleges four violations. First, it alleges that the carriers' failure to protect the confidentiality of the PI violates Section 222(a), which protects Customer Proprietary Network Information (CPNI). Second, it alleges that the carriers' failure to employ reasonable data security practices constitutes an "unjust and unreasonable practice" in violation of Section 201(b). Third, it alleges that the carriers' lax data security practices were contrary to the representations in their privacy policies, which, according to the NAL, also violates Section 201(b). Finally, the NAL alleges that the carriers' failure to notify affected customers also constitutes an "unjust and unreasonable practice" in violation of Section 201(b).

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Henry Gola
Partner
202.719.7561
hgola@wiley.law

This NAL signals a more aggressive FCC approach to data security, and drew dissents from the two Commissioners. Commissioner Pai objected on due process grounds, noting that the Commission has not put the private sector on notice that the failure to protect PI may violate the Communications Act. Among the NAL's flaws, "[t]he Commission never identifies in the entire Notice of Apparent Liability a single rule that has been violated." Commissioner Pai explained that "the Commission asserts that these companies violated novel legal interpretations and never-adopted rules. And it seeks to impose a substantial financial penalty. In so doing, the Commission runs afoul of the fair warning rule. I cannot support such 'sentence first, verdict afterward' decision-making." Commissioner O'Rielly was "not convinced that the FCC has authority to act" in this case. He explained that Section 222 was "never intended to address the security of data on the Internet." He described this NAL as part of a "disturbing trend at the Commission where, in the absence of clear statutory authority, the Commission suddenly imbues an innocuous provision of the Act with tremendous significance in order to meet its policy outcome."

Factual Background

The Companies provide telecommunications services as part of the FCC's Lifeline program. In order to obtain Lifeline services from the Companies, customers electronically submit an application with information and supporting documents to verify their eligibility, such as their name and address, date of birth, Social Security Number, driver's license, Social Security benefit statements, and paycheck stubs. The Companies retained CallCenters India, Inc. d/b/a/ Vcare Corporation (Vcare) to provide electronic storage for the collected documents and applications. According to the NAL, the Companies "stored the PI-containing documents in clear, readable text in an electronic format accessible via the Internet." In addition, the Companies assigned the PI "random URLs" but did not use encryption.

A Scripps Howard News Service (Scripps) investigative reporter discovered the unprotected Internet site, and between March 24, 2013 and April 25, 2013, Scripps accessed more than 128,000 confidential records and documents submitted by Lifeline applicants, including by "conducting a simple Google search." Scripps then notified the Companies on April 26, 2013 that it had accessed their servers and retrieved the PI information and documentation. Four days later, the Companies sent Scripps a "cease and desist" letter alleging that its reporters were "hackers" who had illegally accessed the Vcare servers.

The Companies subsequently contacted the FCC's Enforcement Bureau (EB) about the data breach. The EB issued a Letter of Inquiry (LOI) on June 17, 2013, to which the Companies responded on July 17, 2013.

The NAL Charges the Companies with Violations of Sections 222(a) and 201(b) of the Communications Act

The First Violation. The NAL states that Section 222(a) "imposes a duty on every telecommunications carrier 'to protect the confidentiality of proprietary information of, and relating to . . . customers." Citing "clear" Congressional intent, the NAL interprets PI in Section 222(a) "as clearly encompassing private information that customers have an interest in protecting from public exposure." The NAL also finds it "clear that the scope of [PI] protected by Section 222(a) is broader than the statutorily defined term 'customer proprietary network information' (CPNI)." In addition, the NAL finds that PI as used in Section 222(a) encompasses confidential

information such as personally identifiable information (PII). In defining PII, the NAL cites the definition put forth by the National Institute of Standards and Technology (NIST), which is "(1) any information that can be used to distinguish or trace an individual's identity, such as by name, security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." The NAL finds that the eligibility information submitted by Lifeline customers fits within the FCC's definition of PI.

The NAL rejects the Companies' argument that Section 222(a) applies only to "customers" and that applicants for Lifeline who did not subscribe to the Companies' service were not "customers."

According to the NAL, "[t]he evidence shows that the Companies' security measures lacked even the most basic features to protect consumers' PI." The NAL states that the Companies "knew or should have known that the use of random URLs without more (*e.g.*, encryption) to protect applicant records provided inadequate security and left the documents vulnerable to exposure via search engines," which "is the practical equivalent of having provided no security at all." Because the Companies did not employ appropriate security measures and "exposed their customers to potentially substantial injury," the NAL finds that the Companies violated Section 222(a).

The Second Violation. For the same data security practices, the NAL also finds that the Companies violated Section 201(b), which states that "[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communications service [by wire and radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful." The NAL states that "the lack of encryption clearly evidences the unjust and unreasonable nature of the companies' data security practices." In addition, the NAL finds that the Companies' use of random URLs to protect customer PI "created an unreasonable risk of unauthorized access." The NAL points out that customer data was accessed in foreign countries that "are often identified as hot spots for identity theft." The NAL finds the "lack or near lack of any data security and magnitude of potential harm" as "unjust and unreasonable" in violation of Section 201(b). The Commission notes that, because it had not previously found inadequate data security measures to violate Section 201(b), it does not propose a forfeiture for this violation.

The Third Violation. With regard to the third violation, the NAL finds that the Companies' privacy policies were "false, deceptive, and misleading to consumers" in violation of Section 201(b) of the Act. The Companies' privacy policy stated that they:

Ha[d] implemented technology and security features to safeguard the privacy of your customer specific information from unauthorized access or improper use and will continue to enhance [their] security measures as technology becomes available. Unfortunately, there is no such thing as foolproof security on the Internet, and therefore, [the Companies] make[] no guaranties with regard to the sufficiency of our security measures.

The NAL finds that the Companies "employed virtually no technology or security features" for customer PI and "did not implement or otherwise 'enhance' . . . security measures and technologies until they were informed of a data security breach." In finding a violation of the Communications Act based on the privacy policies, the NAL cites two NALs issued in 2011 which found that deceptive marketing of prepaid calling cards constituted an unjust and unreasonable practice in violation of Section 201(b). In addition, the NAL states that "[t]he FCC has indicated that a marketing act or practice by a carrier that would constitute an unfair or deceptive act or practice under the FTC Act likewise constitutes an unjust and unreasonable act under Section 201(b) of the Communications Act."

The Fourth Violation. The NAL finds that the Companies notified only a portion of the affected customers. According to the NAL, "notification of anything less than all potentially affected consumers [is] unjust and unreasonable in violation of Section 201(b)." The Commission warns that it:

Expect[s] carriers to act in an abundance of caution—even to the extent of being overly inclusive—in their practices with respect to notifying consumers of security breaches. We will review a carrier's notification practices on a case-by-case basis to determine whether it acted justly towards consumers and in a reasonable manner under the factual circumstances of a given case (*i.e.*, taking into account the sensitivity of the consumer information, the scale and scope of a breach, the clarity and means of notification, among other things).

Proposed Forfeiture. The NAL states that "the protection of consumer PI is a fundamental obligation of all telecommunications carriers" and that, "[g]iven the increasing concern about the security of personal data, [the FCC] must take aggressive, substantial steps to ensure that carriers implement necessary and adequate measures to protect consumers' PI."

The NAL notes that neither the forfeiture guidelines nor case law establishes a base forfeiture for Section 222 (a) violations. Instead, the Commission looks to Forfeiture Orders that establish a base forfeiture between $20,000 and $29,000 for failure to file annual CPNI compliance certifications. Though "the Companies' actions were much more egregious than the actions of the carriers in the CPNI cases," the NAL establishes a base forfeiture of $29,000. According to the NAL, the Companies stored PI of approximately 305,065 customers on unsecured servers, and "each document containing PI that the Companies failed to protect constitutes a separate violation for which a forfeiture may be assessed." Further, "[e]ach unprotected document constitutes a continuing violation that occurred on each of the 81 days that elapsed between February 4, 2013, and the date that the Companies remedied the failure on April 26, 2013." Multiplying $29,000 by 305,065 separate violations would result in a proposed forfeiture of $8.85 billion. Instead, the Commission proposes a forfeiture for the Section 222(a) violations of $8.5 million.

The NAL also proposes a forfeiture for just one of the three alleged Section 201(b) violations. For the Companies' "false and misleading privacy policies," the NAL proposes a forfeiture of $1.5 million. However, because "this is the first time we declare a carrier's practices unjust and unreasonable under Section 201(b)

for failures related to data security and notice to consumers in connection with a security breach," the NAL declines to propose forfeitures for those alleged offenses. Still, the NAL warns that "carriers are now on notice that in the future" the FCC "fully intends to assess forfeitures" for these violations of Section 201(b).

Together, the proposed forfeitures total $10 million.

The FCC's Expanding Interest in Data Security

This action is another signal of increasingly aggressive federal oversight of security and privacy practices. The NAL is similar to the Federal Trade Commission's (FTC) suit against Wyndham Worldwide Corp. (Wyndham) for violation of Section 5(a) of the FTC Act prohibiting "unfair or deceptive acts or practices." There, the FTC alleged that Wyndham did not comply with its disseminated privacy policies, and also claimed Wyndham failed to use "reasonable and appropriate" safeguards to protect personal information it collected and maintained, which the FTC claimed was an "unfair" business practice. In April 2014, the United States District Court for the District of New Jersey affirmed the FTC's jurisdiction after Wyndham moved to dismiss the FTC's unfair and deceptive practices claims.

The NAL demonstrates the FCC's expanding interest in technical data security standards as the "the Commission's first data security case and largest privacy action in the Commission's history." It is likely that an emboldened FCC Enforcement Bureau will look to take additional action in the data security area. The FCC is now another source of potential guidance—and liability—when it comes to data security.