WILMERHALE

FCC Releases New Rules for Safeguarding Customer Proprietary Network Information in Response to Pretexting

2007-04-09

After a 13-month proceeding and heated debate on several issues, the FCC finally released an order on April 2, 2007, modifying the customer proprietary network information (CPNI) rules that apply to telephone service providers. Like other recent federal and state initiatives designed to strengthen protections against theft of customers' personally identifiable information, this order resulted from concerns that arose from several scandals brought to the Commission's attention in 2005. The particular abuse at issue in the telephone industry, known as "pretexting," involved the activity of "data brokers," who have been able to obtain and sell call records by pretending to be (or be authorized by) the telephone customer. The amended rules tighten disclosure safeguards by imposing password requirements for obtaining access to call records, requiring disclosure of such unauthorized access (and advance notification to law enforcement), and imposing greater restrictions on sharing CPNI with joint venture partners and independent contractors. The order also modifies carriers' annual certification obligations, and applies the CPNI rules to interconnected VoIP providers for the first time. The rules will take effect in six months, subject to approval from the Office of Management and Budget.

The FCC also issued an accompanying Further Notice of Proposed Rulemaking, which seeks comment on additional proposals. These include extension of password protections to other CPNI situations; requirements for encryption, audit trails and physical safeguards for transfer of CPNI between carriers and third parties (including affiliates); limits on data retention; and proposals for securing the privacy of CPNI stored on mobile equipment. Comments are due within 30 days of the order's publication in the Federal Register.

Perhaps most importantly, the order imposes a general duty on carriers to take "every reasonable precaution" to prevent unauthorized disclosure of CPNI, and it creates a presumption of a violation of that duty in any case of unauthorized disclosure of information. Although the FCC has not yet determined whether to require the specific safeguards described above, it has warned against the failure to adopt such safeguards or other measures reasonably designed to prevent pretexting. Since the FCC has previously established that carriers are directly responsible for the actions of their agents in safeguarding CPNI, this duty means that carriers now need to take particular care to ensure that any contracts with third parties upon whom they rely in providing their services include obligations to comply with the limitations set forth in the FCC's newly revised CPNI rules.

The changes to the CPNI rules include the following:

New CPNI Disclosure Safeguards

- **Access to call records:** To protect against pretexting, carriers may not release call detail information during a customer-initiated call unless the customer provides a password. In creating this password, a carrier may not use information from the customer's life history (e.g., SSN, mother's maiden name, home address or DOB); it can, however, use a "shared secret" method of one or more question/answer combinations to deal with lost or forgotten passwords. Otherwise, if a carrier chooses to release call detail information, it can only do so by (1) sending the call records to the address of record (postal or electronic), (2) calling the customer back at the telephone number of record, or (3) providing the call records at a store location upon proof of valid photo ID matching the customer's account information.

- **Online account access to any CPNI:** Online access to account information, including call detail information, now requires that authentication be permitted only through the use of the same kinds of non-life-history-related passwords.
- **Customer notification of account changes:** To alert customers to possible theft of CPNI, carriers must provide notification whenever a password, backup authentication data, online account or address of record is created or changed. Notification may be accomplished by voicemail, text message or regular mail, but must be sent to the telephone number or address of record and must not reveal the changed information.
- **Business customer exception:** Carriers and businesses may negotiate other authentication regimes, provided that (1) the customer has a dedicated account representative and (2) the negotiated service contract specifically addresses CPNI.

Notification of Breaches

- **"Breach" defined:** A breach occurs when a person without authorization or one who is exceeding authorization has intentionally gained access to, used or disclosed CPNI.
- **Notification to USSS and FBI:** Carriers must notify the US Secret Service and FBI as soon as practicable after reasonable determination of a breach, and in no event later than seven business days. The FCC will maintain a link on its website to a central reporting facility at http://www.fcc.gov/eb/CPNI.
- **Notification to customers and public:** The Commission has also now established a mandate for notifying customers of a breach, but (over strong dissents) has conditioned that process on the views of law enforcement authorities as to its effect on their investigation. No customer notification (or other public disclosure) may occur until seven business days after the USSS and FBI are informed, unless a carrier believes there is an extraordinarily urgent need to notify customers sooner. Carriers must cooperate with the relevant investigating agency prior to making any such early notification. Such an agency may thereafter direct the company to withhold notice to customers for 30 days (or longer, as reasonably necessary in the judgment of the agency).
- **Recordkeeping:** Carriers must keep records of all breaches, notifications to the USSS and FBI, and notifications to customers, for at least two years. The records must include (if available) dates of discovery and notification, a detailed description of the CPNI at issue and the circumstances of the breach.

Other Changes

- **Opt-in consent for joint ventures and independent contractors:** Over the strenuous objections of many carriers, disclosure of CPNI to joint venture partners or independent contractors for marketing purposes is now subject to opt-in approval from customers.
- **Filing of annual CPNI certification:** A carrier's annual CPNI certification must now be filed with the Commission by March 1 for data pertaining to each previous calendar year. The certification must include (1) an officer's statement of personal knowledge that the company's procedures ensure compliance with the rules; (2) a statement accompanying the certificate explaining how the company's procedures ensure compliance with the rules;

(3) an explanation of any actions taken against data brokers; and (4) a summary of all customer complaints concerning unauthorized release of CPNI. To avoid providing a roadmap for pretexters, carriers may file both redacted and non-redacted versions of these filings, with only specific data about the company's actual security procedures and actual complaints redacted.

- **Interconnected VoIP:** The CPNI rules now apply to providers of interconnected VoIP service. Although the FCC asked (in passing) for comment on this issue in its notice, much of the recent debate has involved the content of the rules, not their reach. In the order, the FCC explained that while it has not decided (yet) whether interconnected VoIP services are "telecommunications services" or "information services" under the Communications Act, the Commission's Title I ancillary jurisdiction allows it to impose the CPNI rules on interconnected VoIP providers. In the wake of recent similar developments pertaining to the Communications Assistance for Law Enforcement Act (CALEA), universal service, and 911 requirements, VoIP providers are likely to see the application of the CPNI rules as yet another move in the wrong direction—imposing "legacy" telecom rules on this new generation of voice service.

For more information on this and other communications and e-commerce matters, please contact the authors listed above.