

**FHH Telecom Law**  
**May 2007**

**FCC Clamps Down**  
**On CPNI Disclosure Practices**

*By Donald J. Evans*  
*evans@fhhlaw.com*  
*703-812-0430*

Driven by the crack of Congressional whips, the FCC has imposed strict new requirements on the disclosure of Customer Proprietary Network Information (CPNI). A year ago, the communications world was shocked – shocked! – to learn that unscrupulous persons were illicitly obtaining information from phone companies about their customers' phone calls with the greatest of ease. The FCC at that time handed out some exemplary fines and required all carriers to file certifications of their compliance with the CPNI protection rules which had been around since 1998. It also opened a rulemaking to consider the imposition of stricter rules to deal with the problem in the face of widespread lackadaisical compliance.

Unlike many such tempests on the Washington weather map, this one refused to peter out. More and more reports surfaced of “pretexting” as a common practice to obtain customer data, despite the non-disclosure rules, and Congress continued to express concern that the FCC was not doing enough to deal with the problem. In response, the FCC recently handed out a spate of hundred thousand dollar fines to carriers who, on spot check, had not filled out and put in a drawer their internal certification of compliance with the CPNI rules.

The Commission also adopted new procedures applicable both to common carriers and VoIP operators to protect such data. Starting in about six months, phone companies must:

- File every March 1 with the FCC a statement of compliance with the CPNI rules;
- Require a password from customers before disclosing call detail information during customer-initiated contacts and when data is accessed by customers on-line;
- Notify customers at their addresses of record whenever there is a change in the customer account information;
- Notify law enforcement within seven days of a breach of CPNI security;
- Require customers to “opt in” to arrangements with joint venturers or independent contractors who use the CPNI for marketing communications-related services.

The FCC did seem to acknowledge that at some point the interposition of these

protections hampers the ability of carriers to address routine customer questions or concerns. Accordingly, the FCC stressed that carriers could address a question about a bill without a password if the customer provides the information about the items in question. Similarly, the carrier can send requested information to the address of record of the customer without needing a password, the theory being that in these circumstances no private information would be disclosed to imposters. And customers who present themselves at store locations can be identified by picture ID without a password. Business customers who have a dedicated account representative are exempt from the new rules on the theory that their privacy is governed by detailed contracts between them and the carrier. (NB – Contracts with business customers must deal with this issue or the exemption does not apply.) Nevertheless, there is no doubt that these new security measures will complicate customer-carrier contacts.

For one thing, customers who do not now have a password will have to have one set up, and their identity must be verified without using “readily available biographical information” such as birth date, address and possibly even that old favorite, mother’s maiden name. (Customers with existing passwords do not need to set up a new one.) The password procedures (including telling the customer what his password is when he has forgotten it) are familiar to users of password-protected sites. To accommodate smaller carriers, the FCC has allowed an additional six months for them to implement password protection for their on-line databases.

Also of particular note is the FCC’s new rule with respect to disclosure of breaches of security. You might imagine that the customer should be informed right away if the carrier inadvertently discloses CPNI. Instead, the FCC requires that *law enforcement* be informed right away so they can seek to apprehend the perpetrator; absent exigent circumstances, however, the customer is *not* to be informed until law enforcement says it’s OK. This curious rule seems to put the cart of catching the criminals before the horse of protecting the privacy rights of the customer.

Finally, the FCC requested further comment as to whether it should require customer data to be encrypted (to prevent hackers from getting the information), whether audit trails should be required as an aid in tracking down breaches, whether password protection should be expanded to non-call detail CPNI, and whether data in carriers’ computers should be systematically destroyed (or otherwise quarantined) after a certain period to reduce the risk of disclosure. Comments on those issues are due in about 30 days, replies 30 days thereafter.