



The Financial Center
666 Walnut Street, Suite 2500
Des Moines, IA 50309
Telephone: (515) 288-2500
Facsimile: (515) 243-0654

CLIENT UPDATE

December 8, 2007

The FCC's revised rules governing carrier use and protection of customer proprietary network information (**CPNI**) are now in effect.

Among other requirements, the new rules require telecommunications carriers to file a CPNI compliance certification with the Commission on an annual basis. The compliance certification must include a statement explaining how the carrier's policies and procedures ensure that it is in compliance with the CPNI rules.

The initial certification filing is due **March 1, 2008** and must include the required data pertaining to the previous calendar year. The certification must be signed by an officer of the carrier and will be filed as a public record in Enforcement Bureau Docket No. 06-36.

In advance of the filing deadline, all carriers should review their own CPNI protection programs to ensure that they are in compliance with the FCC's CPNI rules, including the most recent revisions. A carrier should review its CPNI protection program on an annual basis with respect to the following:

- Identify a "compliance officer" who understands the carrier's obligations under the CPNI rules and has personal knowledge of the carrier's operating procedures for the protection of CPNI.
- Identify circumstances under which the carrier uses, discloses or grants third parties access to customer CPNI.
- Identify the operating procedures that the carrier has in place for the protection of CPNI, including:
 - measures taken to discover and protect against attempts to gain unauthorized access to CPNI;

- reasonable customer authentication procedures for the release of CPNI (call detail and non-call detail) based on customer-initiated telephone contact, online account access or an in-store visit;
 - reasonable procedures for notifying customers of account changes;
 - legally valid forms and methods for notifying customer and obtaining customer CPNI approval (opt-in or opt-out) for use or disclosure of CPNI when such approval is required;
 - system for clearly establishing status of a customer's CPNI approval prior to the use or disclosure of CPNI;
 - procedures for training personnel as to when they are or are not authorized to use or disclose CPNI, including specific disciplinary process;
 - supervisory review process for use of CPNI for outbound marketing;
 - procedures for safeguarding the handling and sharing of CPNI with affiliates or third parties; and
 - procedures for notifying customers and law enforcement of CPNI security breaches.
- Identify any legal or law enforcement actions the carrier has taken against pre-texters.
 - Establish public file with copies of CPNI rules and appropriate CPNI-related certifications, notices and procedures. *(Note: any form containing non-public, personally identifiable customer information should not be included in the public file).*

Under the Communications Act and FCC regulations, all telecommunications carriers have the duty to implement operating procedures to protect the privacy of CPNI. If you have questions concerning CPNI compliance, please contact John Pietila at 515-288-2500 or JohnPietila@DavisBrownLaw.com.