

FCC CPNI Rules

On April 2, 2007, the FCC released a [Report and Order](#) which adopts additional rules to protect customer proprietary network information ("CPNI"). Under the new rules, communications carriers must notify law enforcement of any breaches of CPNI, and they must also file annual CPNI certifications with the FCC. In addition, the FCC's new CPNI regulations cover providers of interconnected Voice over Internet Protocol ("VoIP") services. The new rules will take effect six months after publication in the Federal Register or when approved by the Office of Management and Budget, whichever is later. The FCC also released a [Further Notice of Proposed Rulemaking](#) to consider what further regulations might be necessary to protect CPNI.

The new regulations, following the recent release of several FCC decisions penalizing carriers for apparent CPNI rule violations (see http://www.tkcrowe.com/cpni_enforcement_actions.html), underscore the FCC's heightened focus on the protection of CPNI. All carriers, including facilities-based and resale carriers, wireless providers, MVNOs and prepaid calling card providers, should commence preparations for complying with the new rules.

Rules

CPNI is the individually identifiable information that is created by a customer's relationship with a communications provider, such as data about the frequency, duration and timing of calls, the information on a customer's bill and call-identifying information. Because of the sensitive nature of this information, CPNI is afforded greater protection under Section 222 of the Communications Act of 1934, as amended, than the other two general categories of customer information – aggregate customer information and subscriber list information. In its [Report and Order](#), the FCC stated that it is now adopting additional protections for CPNI because "[t]he carriers' record on protecting CPNI demonstrates that" some carriers "have failed to adequately protect CPNI."

The FCC CPNI rules are summarized below:

- [Carrier Authentication](#). Since the release of call detail information over the telephone presents an immediate risk to privacy, carriers are prohibited from releasing call detail information based on customer-initiated telephone contact, except under three circumstances: (1) when a customer provides a pre-established password; (2) when a customer requests that the information be sent to the customer's address of record; or (3) when a carrier calls the telephone number of record and discloses the information. In addition, carriers must provide mandatory password protection for online account access. Online access based solely on a customer's readily available biographical information is prohibited. However, carriers are not required to reinitialize existing passwords for online customer accounts. At retail locations, carriers may continue to provide account access to customers who present valid photo IDs.

- [Notice of Account Changes](#). Carriers must notify a customer immediately of account activity, such as a change to a password, an online account or an address of record. Notification may be by voicemail, text message or by mail to the customer's address of record.

- [Notice of Unauthorized Disclosure of CPNI](#). If there has been a breach of CPNI, carriers must provide electronic notification of the breach within seven business days to the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI"). (The FCC will provide a link for the reporting of breaches at www.fcc.gov/eb/CPNI/.) In order to allow law enforcement time to conduct an investigation, carriers must wait another seven business days before notifying the affected customers of the breach (unless the USSS and FBI request that the carrier continue to postpone disclosure). However, carriers may notify customers sooner if there is a risk of immediate and irreparable harm. In addition, carriers must keep records of discovered breaches for at least two years.

- [Joint Venture and Independent Contractor Use of CPNI](#). Carriers must obtain opt-in consent from a customer before disclosing a customer's CPNI to a joint venture partner or an independent contractor for the marketing of communications-related services to the customer. Under the current opt-out regime, the burden is on the customer; a carrier may share a customer's CPNI with another entity after providing notice to the customer, so long as the customer does not object. However, since current opt-out notices "are often vague and not comprehensible to an average consumer," the FCC said it is necessary to revise the rules to require express prior customer authorization.

- [Annual CPNI Certification](#). Carriers must file an annual certification with the FCC, explaining any actions that they have taken against data brokers and summarizing all consumer complaints that they have received during the year relating to the unauthorized release of CPNI. This requirement will be in addition to the existing certification procedure, under which carriers must have an officer sign a compliance certificate each year attesting that the officer has personal knowledge that the carrier's procedures are sufficient to ensure compliance with the CPNI rules. Under the current rules, that certification must be made available to the public, but does not have to be filed with the FCC. The new annual certification filing that must be made with the FCC will be due by March 1 of every year, in EB Docket No. 06-36, and cover the previous calendar year. The first filing under the new rules will likely be due on March 1, 2008.

- [Interconnected VoIP Service](#). The CPNI rules will apply to providers of interconnected VoIP service. Interconnected VoIP is telephone service via a broadband connection that utilizes Internet protocol and allows users to receive calls from, and terminate calls to, the public switched telephone network. Owing to the growth in popularity of VoIP services, the FCC noted that if it did not extend the CPNI regulations to interconnected VoIP, "a significant number of American consumers might suffer a loss of privacy and/or safety resulting from unauthorized disclosure of their CPNI."

- [Enforcement Proceedings](#). Carriers must take reasonable measures to discover and protect against unauthorized access to CPNI. If there is a breach, the FCC will infer that the carrier's protection methods were insufficient. As the FCC stated, "We fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information." The FCC will not require carriers to encrypt their customers' CPNI, but it will expect them to do so if that would provide "significant additional protection against the unauthorized access to CPNI" at a reasonable cost. We expect the FCC's Enforcement Bureau to continue to aggressively penalize providers which fail to comply with the existing and new CPNI rules.

- [Business Customers](#). In limited circumstances, carriers may establish by contract authentication procedures for business customers that are different from those in the new rules, so long as those customers have a dedicated account representative and the contracts specifically address the protection of CPNI.