

## FCC Adopts Rules Implementing the Truth in Caller ID Act

By K.C. Halm and Rob Morgan

June 27, 2011

The Federal Communications Commission (FCC) issued a Report and Order (Order) on June 22, 2011, implementing the Truth in Caller ID Act (the Act). Enacted on December 22, 2010, the Act is aimed at prohibiting the use of caller ID “spoofing,” which entails the practice of modifying caller ID information by making a call appear to come from a phone number different from the originating phone number for ill intent.

Specifically, the Act prohibits the use of caller ID “spoofing” to facilitate schemes that defraud consumers and threaten public safety through the manipulation of caller ID information. The Act forbids the practice of caller ID spoofing, in connection with any telecommunications service or IP-enabled voice service, which causes any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value. Violations of this rule may be penalized through fines up to \$10,000 for each violation, or three times that amount for each day of a continuing violation. Penalties for any continuing violation are capped at \$1 million for any single act, or failure to act.

### FCC regulations mirror statute by prohibiting caller ID spoofing with malicious intent

The FCC’s primary rule in this proceeding builds upon its current rules governing interstate caller ID and other calling party number (CPN) services. The new caller ID rule closely mirrors the language of the Act, stating that “no person or entity in the United States shall, with intent to defraud, cause harm, or wrongfully obtain anything of value, knowingly cause, directly or indirectly, any caller identification service to transmit or display misleading or inaccurate caller identification information.” The new rule addresses both the transmission and display of misleading or inaccurate information to make clear that, even if a carrier or interconnected VoIP provider transmits accurate caller identification information, it would be a violation for a person or entity to knowingly cause, directly or indirectly, a device that displays caller identification information to display inaccurate or misleading information with the intent to defraud, cause harm, or wrongfully obtain something of value.

### Key factor is malicious intent

The key factor in the new rule prohibiting caller ID spoofing is malicious intent. Telecommunications carriers, or interconnected VoIP providers, that transmit incorrect caller ID information *without* the requisite intent to defraud, cause harm, or wrongfully obtain anything of value will not be found to have violated the rules. By closely following the statutory language, the FCC ensured that its rules did not expand the activities proscribed by the Act, or the number of entities within its scope.

The key factor in determining whether illegal spoofing occurred under the Act and the new rules is intent to cause harm. Absent such intent, no violation will be found. Thus, as the FCC recognized, there may be valid reasons for manipulating caller ID information, such as for domestic violence centers that wish to mask their identity, or for doctors responding to after-hours messages from patients. In addition, carriers may also manipulate caller ID to test equipment to emulate the customer experience, or to investigate fraudulent use of the network. Each of these practices would *not* fall within the scope of the prohibition of the FCC’s new rule.

### Exceptions are limited

As provided for in the Act, authorized activities of law enforcement agencies, states or their political subdivisions, and United States intelligence agencies are exempted from limits on spoofing, as are

persons or entities authorized under a court order to engage in caller ID manipulation.

The FCC declined to adopt any exceptions based on status, such as for VoIP service providers, because it considers the requisite intent-to-do-harm standard as being sufficiently clear. For example, one carrier requested specific exemptions for the manipulation of caller ID to investigate fraud, for telemarketing, customer service, or for simply transmitting Caller ID data received from a customer or another carrier. The FCC rejected that proposal. In deciding such exemptions are unnecessary, the FCC agreed with the Department of Justice, which expressed concern that such exemptions for VoIP and other service providers could “create dangerous loopholes ... that could be exploited by criminals.”

Consistent with the Act, the Order clearly states that blocking one’s own phone number, or displaying a company’s main number instead of the direct number of an individual, are permitted activities under the implementing rules. The Order indicates that the FCC is concerned, however, with the practice of unmasking blocked numbers, which the FCC characterized as “effectively stripping out the privacy indicator chosen by the calling party.” Despite its concern, the FCC concluded that the record is “not sufficiently robust” to support amending the rules to prohibit unmasking blocked numbers.

The FCC declined to extend this new rule to the practice of modifying CPN data in order to mask the jurisdictional nature of a call, a practice closely related to the intercarrier compensation phantom traffic issue, as some commenters had requested.

### **Penalties**

The Order amends section 1.80(b) of the FCC’s rules to provide for the maximum fines allowed under the Act, which as noted above, can be up to \$10,000 for each violation, or three times that amount for each day of a continuing violation. The amount of fines levied will be determined using the balancing factors found in 47 U.S.C. § 503(b)(2)(E): “the nature, circumstances, extent, and gravity of the violation, and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require.”

The Order can be found [here](#); and the Truth in Caller ID Act can be found [here](#).

If you have any comments or would like more information, please contact your Davis Wright Tremaine contact, or the authors.

This advisory is a publication of Davis Wright Tremaine LLP. Our purpose in publishing this advisory is to inform our clients and friends of recent legal developments. It is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations.