Written Statement

Of

Kris Anne Monteith
Chief, Enforcement Bureau
Federal Communications Commission

On

Caller ID Spoofing

Before the
Committee on Commerce, Science, and Transportation
United States Senate

June 21, 2007

Good morning Chairman Inouye, Vice Chairman Stevens and members of the Committee. Thank you for the opportunity to speak about the problem of caller identification (caller ID) spoofing.

As you know, caller ID services let customers identify who is calling them before they answer a call by displaying the caller's telephone number or other information – such as a name or business name – on the customer's equipment before the customer picks up the phone. "Caller ID spoofing" refers to a practice in which the caller ID information transmitted with a telephone call is manipulated in a manner that misleads the call recipient about the identity of the caller. The use of Internet technology to make phone calls has apparently made caller ID spoofing even easier. The Commission is deeply concerned about reports that caller ID information is being manipulated for fraudulent or other deceptive purposes and the impact of those practices on the public trust and confidence in the telecommunications industry. We are particularly concerned about how this practice may affect consumers as well as public safety and law enforcement communities.

In my testimony, I will first provide a brief technical background on caller ID spoofing. Then, I will describe the Commission's rules addressing caller ID services and the steps the Commission is taking to make sure that providers are fully meeting their obligations under the Communications Act and the Commission's rules and orders.

As a technical matter, caller ID spoofing happens by manipulating the data elements that travel with a phone call. Phone calls on the public switched telephone network, or PSTN, are routed to their destinations by means of a specialized protocol called the Signaling System 7, or SS7. SS7 conveys information associated with a call

such as the telephone number of the caller. The SS7 information for a call is provided by the carrier that the caller uses to place the call. Caller ID then displays that caller's number to the called party. Caller ID spoofing is accomplished by manipulating the SS7 information associated with the call.

The Commission addressed caller ID on the PSTN in 1995 with rule 64.1601, which generally requires all carriers using SS7 to transmit the calling party number associated with an interstate call to interconnecting carriers. The same Commission rule also requires telemarketers to transmit accurate caller ID information.

The development of Internet and IP technologies has made caller ID spoofing easier than it used to be. Now, entities using IP technology can generate false calling party information and pass it into the PSTN via SS7. Caller ID spoofing can potentially threaten our public safety. For example, spoofers can fabricate emergency calls and cause local law enforcement and public safety agencies to deploy their resources needlessly. Caller ID spoofing can potentially threaten consumers. For example, spoofing can be used by the unscrupulous to defraud consumers by making calls appear as if they are from legitimate businesses or government offices.

The Commission's Enforcement Bureau (Bureau) has been investigating the issue of caller ID spoofing since the summer of 2005 when information regarding junk fax spoofing came to our attention. To date, the Bureau has initiated investigations of thirteen companies engaged in the marketing and selling of caller ID spoofing services to customers. One investigation resulted in a citation against a telemarketer, Intelligent Alternatives, for rule violations, including violations of the caller ID rules under section 64.1601. We have sent formal letters of inquiry and, at the same time, served subpoenas

to compel responses to our inquiries. In some cases, we have issued subsequent letters of inquiry to uncover additional evidence of possible violations of the Communications Act.

Our investigations have revealed that the companies engaged in this practice are of varying degrees of sophistication that employ disparate methods and technologies to provide service to different types of customers. Some of the companies, for example, claim they are providing spoofing services only to customers such as law enforcement officials or private investigators, or to others engaged in the furtherance of debt collection and other similar objectives. The companies also allow customers varying amounts of flexibility over the spoofing: some companies claim they do not allow customers the ability to customize the false number to be displayed on the called party's caller ID while others do provide that functionality. This last characteristic is particularly important when determining whether spoofers permit their customers to use "911" as a spoofed number or whether the customers can spoof the numbers of first-responders and other emergency services providers. We are continuing to seek relevant information to assist us in fully understanding these issues and whether violations of the Communications Act or our rules have occurred.

We also have held meetings with numerous industry representatives, including wireline, wireless, and voice over Internet protocol (VoIP)-based companies, to determine the impact of caller ID spoofing on their consumers and networks. And, we have coordinated with state agencies, the Federal Trade Commission and other interested organizations, such as the National Emergency Number Association, regarding their efforts to address and identify solutions to this problem. The Enforcement Bureau is committed to continuing to gather and analyze information about these companies'

practices, their networks, their businesses, their customers, and other germane information.

In addition to our enforcement efforts, the Commission has taken affirmative steps to prevent those engaged in caller ID spoofing for deceptive reasons from successfully accessing the personal information of telecommunications customers. In a recent Order tightening the Commission's Customer Proprietary Network Information or CPNI rules, the Commission determined that a carrier providing call history information over the phone to a customer must call the customer at the account's telephone number of record to provide such information rather than rely on caller ID as an authentication method, thereby eliminating one of the major tools of pretexters.

As the Commission indicated in its testimony before the House of Representatives Energy and Commerce Subcommittee on Telecommunications and the Internet last year, the Commission may not have sufficient authority to fully address this issue; some of these entities do not appear to be directly regulated by the Commission, an assertion made by some targets of our investigations. Thus, legislation that clarifies the Commission's authority in this area would be helpful.

In conclusion, the intentional manipulation of caller ID information, especially for the purpose of fraud or deception, is a troubling development in the telecommunications industry. The Commission looks forward to working with this Committee, and other Members of Congress, to ensure the public maintains its confidence in the telecommunications industry. Thank you for the opportunity to speak with you today.