Written Statement

Of

Thomas J. Navin
Chief, Wireline Competition Bureau
Federal Communications Commission

On

H.R. 5126, the Truth in Caller ID Act of 2006

Before the
Subcommittee on Telecommunications and the Internet
Committee on Energy and Commerce
U.S. House of Representatives

May 18, 2006

Good morning Chairman Upton, Ranking Member Markey and members of the Subcommittee. Thank you for the opportunity to speak about the problem of caller identification or "caller ID" spoofing.

As you know, caller ID services let customers identify who is calling them 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 way 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 concerned about how this practice may affect the public safety and law enforcement communities in particular.

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 FCC 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. Among other things, SS7 conveys information 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. In one particularly harmful way, caller ID spoofing threatens our public safety. Spoofers can fabricate emergency calls and cause local law enforcement and public safety agencies to deploy their resources needlessly. The Newark Star-Ledger reported that police in New Brunswick, New Jersey shut down one city neighborhood for hours, evacuating buildings and closing streets as a SWAT team surrounded an apartment house. Police had received a call from a girl saying she had been handcuffed and raped in the apartment, when the call was a hoax. Caller ID had been spoofed to make the call appear to come from the apartment. Hoaxes like these divert our local public safety resources away from where they are so desperately needed – responding to real emergencies and real threats to our homeland security.

My colleagues in the Commission's Enforcement Bureau are actively pursuing the issue of caller ID spoofing. They have issued letters of inquiry or subpoenas to several entities who are apparently engaged in marketing and selling caller ID spoofing services to customers. The Enforcement Bureau continues to gather and analyze information about these companies' practices, their networks, their businesses, their customers, and other germane information, as

well as analyze enforcement options, some of which may be limited as to entities that are not regulated by the Commission.

In addition, the Enforcement Bureau has met with carriers, assembled internal technical experts to address the problem, and begun coordinating with the Federal Trade Commission regarding its efforts to address this problem.

Finally, I note that the Committee is considering imposing restrictions on voice over Internet protocol, or VoIP providers that facilitate caller ID spoofing. As you know, there are many varieties of VoIP, and the definition of VoIP in this bill, as well as other proposed legislation, could be interpreted to exclude many of them from the reach of the Commission. As the House of Representatives considers legislation affecting VoIP, it should be aware that a restrictive definition of VoIP here or in other legislation might establish a statutory precedent that would restrict the Commission's authority to protect life and property in both the public safety and law enforcement contexts.

In conclusion, the intentional manipulation of caller ID information, especially for the purposes of fraud or deception, is a troubling development in the telecommunications industry. As chief of the Wireline Competition Bureau at the FCC, I share your concern about this practice. I look forward to working with this Committee, other Members of Congress, Chairman Martin and the Commission to ensure the public maintains its confidence in the telecommunications industry. Thank you for the opportunity to speak with you today.