Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Rules and Regulations Implementing the	)	WC Docket No. 11-39
Truth in Caller ID Act of 2009	)	

COMMENTS OF THE UNITED STATES DEPARTMENT OF JUSTICE

Jason M. Weinstein
Deputy Assistant Attorney General
Criminal Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530
(202) 616-3928

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Rules and Regulations Implementing the	)	WC Docket No. 11-39
Truth in Caller ID Act of 2009	)	

The United States Department of Justice respectfully submits these comments in response to the Notice of Proposed Rulemaking released on March 9, 2011 (the "NPRM"), in the above-captioned docket.

I. Overview of the Department of Justice's Comments

The Department of Justice believes that caller ID spoofing poses a significant threat to public safety that can be substantially mitigated through the imposition of narrowly tailored regulations upon the caller ID spoofing industry. The Department further believes that the Commission is empowered to enact such regulations, and should exercise its authority to prevent criminals from using caller ID spoofing to harm, harass, and defraud the public.

In the comments below, the Department urges the Commission to adopt a broader rulemaking approach that includes regulations designed to curtail the widespread abuse of caller ID spoofing by criminals. The Department's comments also include a detailed discussion of the Commission's authority to regulate caller ID spoofing providers, and address other questions raised in the NPRM.

II. Introduction

On December 22, 2010, the President signed Public Law No. 111-331, the Truth in Caller ID Act of 2009, which prohibits the transmission of false caller ID information in connection

with a scheme to defraud, cause harm, or wrongfully obtain anything of value. On March 9, 2011, the Federal Communications Commission ("FCC" or "Commission") issued a Notice of Proposed Rulemaking inviting comment on a series of regulations proposed by the Commission that would implement the prohibitions within Section 2 of the Act.

The proposed regulations address caller ID spoofing, i.e., altering the telephone number displayed to the recipient of a telephone call to a number different than the caller's actual telephone number.[1] Although caller ID spoofing once required special equipment or a relatively high degree of technical sophistication, there are now widely available services that make caller ID spoofing as simple and inexpensive as placing a call with a traditional telephone calling card.

As the Department pointed out in its January 26, 2011 letter to the Commission, which the Department incorporates herein by reference, the widespread availability of caller ID spoofing services is a significant facilitator of criminal activity and a substantial threat to public safety.[2] Numerous examples from around the country demonstrate these concerns, including the incidents described below:

- Spoofed caller ID services have enabled a particularly insidious form of fraud known as "swatting." Swatting refers to the practice of placing false emergency calls to law enforcement for the purpose of eliciting a response from the Special Weapons and Tactics ("SWAT") team, usually as a means of revenge. In one of the largest swatting cases to date, Stuart Rosoff and a number of co-conspirators pled guilty to participating in a swatting conspiracy that targeted more than 100 victims. Using a spoofing service, Rosoff and his co-conspirators were able to place calls to the police that appeared to

[1] The notion of spoofing does not include caller ID *blocking* – i.e., preventing any caller ID from being displayed, a capability that telecommunications carriers generally are required to support. *See* 47 C.F.R. § 64.1601(b) (2010). Nor should spoofing be understood to include transmitting a number related to a private branch exchange (PBX) or the main telephone number of a business's network in place of an extension.

[2] *In the Matter of Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Letter from Lanny A. Breuer, Assistant Attorney General, Department of Justice, to Marlene H. Dortch, Secretary, FCC, at 1 (Jan. 26, 2011) ("*DOJ Letter*").

originate from the home telephone of their chosen victim. In these calls, one of the conspirators would identify himself to police as a member of the targeted family. The imposter would then tell police that he had shot and killed several members of the family and was holding the remaining family members hostage. Believing the emergency to be real, law enforcement would respond on an emergency basis, leading to dangerous confrontations between heavily armed police officers and the innocent victims of the "swatting" incident. At least two injuries resulted.

- Caller ID spoofing services are often used in connection with stalking and harassment. For example, in 2008, Danielle Zimmer and Carmen Veneziale pled guilty to harassment and making terrorist threats. Zimmer and Veneziale used a spoofing service to place 13 different calls to the cell phones of Zimmer's co-workers. The calls were placed in the middle of the night and, as a result of a spoofing service, appeared to originate from the victim's home telephone number. During the calls, Veneziale would inform the victims that he had broken into their homes and was watching them.

- Caller ID spoofing services are also widely used by identity thieves. In one long-running scam, members of the public are called from a spoofed telephone number associated with the local court. Call recipients are told they missed their scheduled jury duty and are threatened with prosecution. The victims are then ordered to provide personally identifying information, including their Social Security number.

- Identity thieves also use caller ID spoofing services to access cell phone voicemail. When a call appears to originate from a user's cell phone, most cellular providers do not require a password in order to access the user's voicemail account. As a result, identity thieves are able to access most cell phone voicemail systems simply by spoofing the victim's cell phone number. According to news reports, more than 50 voicemail accounts – including several belonging to celebrities – were accessed in this manner in a 2006 incident.

Widespread availability of caller ID spoofing services also enables criminals to more effectively hide their activities from law enforcement and significantly complicates evidence collection by law enforcement.

III. The Views of the Department

In its January 26, 2011 letter to the Commission, the Department urged the FCC to adopt regulations that would deter criminals from using caller ID spoofing services to further their criminal activity.[3] The Department's letter pointed out that caller ID spoofing services are

[3] *Id.* at 3-4.

widely used by criminals to facilitate illegal activity.[4] The letter also discussed the legislative history of the Truth in Caller ID Act, including a floor statement by Chairman Richard Boucher, whose subcommittee reported the House companion bill, urging the Commission to consider imposing regulations upon caller ID spoofing providers.[5] Finally, the Department's letter proposed two regulatory goals that would deter criminals from using spoofed caller ID to further their crimes: 1) requiring spoofing providers to make a good faith effort to verify that a user has the authority to use the substituted number; and 2) the adoption of standards that would permit call recipients to determine whether caller ID information has been altered and allow law enforcement to trace such calls to the true originating telephone number with appropriate authority.[6]

The first of these goals could be accomplished in any number of ways. Caller ID spoofing services could maintain a pool of alternate numbers that customers could use to place spoofed calls. Alternatively, caller ID spoofing services could be required to verify that the substitute number belongs to the user by placing a one-time verification call to that number. In this way, if a doctor wished to display an office number on patients' phones rather than the number of the cell phone from which the call actually originated, the doctor need only set up an account with a spoofing provider and register the office phone. A one-time verification call would assure that the doctor does indeed have use of and control over that number, and any future calls could then appropriately spoof the office number.

The second of these goals could also be accomplished in a number of ways. The Department does not have a particular technical solution to propose but would rely on the

[4] *Id.* at 1.

[5] *Id.* at 3.

[6] *Id.* at 4.

Commission's expertise to solve this problem. Perhaps a flag could be set within the signaling protocols that would indicate that that the caller ID information being transmitted represents a substituted or modified number.

The Department is not wedded to any particular approach so long as it is successful in reducing the ability of criminals to spoof caller ID in such a way that it displays telephone numbers that are not under their control, or fools victims, telephone companies, and law enforcement into believing that the information displayed in the caller ID is genuine.

A. The Commission Can and Should Regulate Caller ID Spoofing Providers

In the Department's view, the Commission enjoys broad authority to regulate caller ID spoofing providers, authority that was only bolstered with the passage of the Truth in Caller ID Act. By utilizing this authority to impose narrowly tailored regulation upon caller ID spoofing providers, the Commission can take a significant step toward ending the rampant abuse of caller ID spoofing by criminals.

1. Caller ID Spoofing Facilitates Criminal Activity

As the real-world examples highlighted in the introduction to the Department's comments make clear, caller ID spoofing services facilitate a broad range of criminal activity. Unfortunately, the incidents described above are not isolated events. Although reliable data on the use of caller ID spoofing by criminals is not readily available, a review of recent media coverage for stories involving caller ID spoofing provides some perspective on the scope of the problem. In the month of February 2011 alone, more than a dozen media outlets from around the country filed stories involving the abuse of caller ID spoofing by criminals. These reports involved 14 unrelated incidents, which took place in Alabama (3), California, Iowa, Massachusetts, Michigan (2), Minnesota, Oregon, Pennsylvania, Tennessee, Vermont and

Washington.[7] Although these media reports offer only a sampling of the actual number of criminal schemes that rely on spoofed caller ID, they make clear that the use of caller ID spoofing to facilitate criminal activity has become commonplace. This conclusion is consistent with the Department's own experience, which includes a rapidly increasing number of investigations involving criminals who have used caller ID spoofing services to commit their crimes.

2. The Commission has the Authority to Regulate Caller ID Spoofing Providers

In the Department's view, the Commission's authority to regulate the caller ID spoofing industry is derived from at least two sources: (1) the Truth in Caller ID Act itself, which authorizes the Commission to "prescribe regulations to implement" the Act (47 U.S.C. §

[7] *FNB Bank Officials Warn Customers of Potential Phone Scam*, The Daily Sentinel (February 2, 2011), http://thedailysentinel.com/news/article_d4971758-2f2c-11e0-bbc8-001cc4c002e0.html; *BBB Warns Residents of Caller ID Spoofing from Cardholder Services*, Sand Mountain Reporter (February 11, 2011), http://www.sandmountainreporter.com/news/local/article_629ad6a6-3627-11e0-beef-001cc4c03286.html; *Prank Calls Put Homewood Residents on Alert*, CBS 42 News (February 22, 2011), http://www.cbs42.com/content/ localnews/story/Prank-calls-put-Homewood-residents-on-alert/VeWxAjTnSke2UbcJ0cN4iA.cspx; *Woman Arrested For Allegedly Impersonating FBI*, San Jose Mercury News (February 10, 2011), http://www.mercurynews.com/news/ci_17355104; *Officials Warn of Fake Health Inspectors in Iowa*, Des Moines Register (February 24, 2011), http://webcache.googleusercontent.com/search?q=cache:H4Bfr-JnFFEJ:www.desmoinesregister.com/print/article/20110224/NEWS01/110224009/Officials-warn-fake-health-inspectors-Iowa+Officials+Warn+of+Fake+Health+Inspectors+in+Iowa,+Des+Moines+Register&cd=2&hl=en&ct=clnk&gl=us&source=www.google.com; *Pranksters Target People with Phony Caller ID*, CBS Boston (February 4, 2011), http://boston.cbslocal.com/2011/02/04/pranksters-target-people-with-phony-caller-id/; *Spoofing Scam*, Battle Creek Enquirer (February 11, 2011), http://cc.bingj.com/cache.aspx?q=Spoofing+Scam%2c+Battle+Creek+Enquirer%2c+February+11%2c+2011&d=4996185315476176&mkt=en-US&setlang=en-US&w=5daa5dfe,516e019e; *Three Teens Charged for Threatening Phone Calls*, Petoskey News (February 15, 2011), http://articles.petoskeynews.com/2011-02-16/teens_28549124; *Fake Officers Scam Woman Out of $6K*, KPTV Fox 12 (February 4, 2011), http://www.kptv.com/news/26755904/detail.html; *Man Doesn't Fall For Scammers Trap*, PhillyBurbs.com (February 20, 2011), http://cc.bingj.com/cache.aspx?q=man+doesn+t+fall+for+scammers+trap+phillyburbs&d=4762436017325466&mkt=en-US&setlang=en-US&w=16a1c723,f40abe97; *Spoofing Misused in Scam*, Shelbyville Times-Gazette (February 3, 2011), http://www.t-g.com/story/1700197.html; *Troopers Warn of Phone Scammers Posing As State Police*, WCAX (February 17, 2011), http://www.wcax.com/Global/story.asp?S=14047095; *Scammers from Oregon Fail To Defraud Woman*, The Seattle Times (February 5, 2011), http://seattletimes.nwsource.com/html/localnews/2014139445_scam06m.html

227(e)(3)); and (2) the Communications Act of 1934, which grants the Commission authority over interstate caller ID service and authorizes the Commission to issue "such rules and regulations . . . as may be necessary in the execution of its functions" (47 U.S.C. § 154(i)). We address each of these sources of authority in turn.

i. The Truth in Caller ID Act

The Truth in Caller ID Act makes it unlawful for any person within the United States, in connection with any telecommunications service or IP-enabled voice service, to "cause 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," unless such transmission is exempted from that prohibition by the Commission. 47 U.S.C. § 227(e)(1).

Section 227(e)(3) is, on its face, a plenary grant of authority to "prescribe regulations to implement" that prohibition. Congress prescribed the contents of the regulations in only two respects: the regulations shall contain "appropriate" exceptions (*id.* at § 227(e)(3)(B)(I)), and they shall contain a specific exception for law enforcement agencies and court orders (*id.* at § 227(e)(3)(B)(ii)). Apart from those two directives, the Commission's authority to adopt rules that "implement" the prohibition is unqualified and unrestricted. The regulatory measures suggested by the Department in its January 26, 2011 letter, such as imposing a verification requirement upon the spoofing industry,[8] are well within the scope of that general authority.

Caller ID spoofing services lie at the heart of the conduct prohibited by Section 227(e)(1). When a calling party wishes to transmit misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain something of value, a

[8] *DOJ Letter* at 3-4.

caller ID spoofing service provides him with the means to do so. Even where the provider is not aware that its service is being used for illicit means, the service remains instrumental to the unlawful conduct of the calling party.

Moreover, spoofing services are themselves subject to the statutory prohibition in Section 227(e)(1), because they are "persons" (*see* 47 U.S.C. § 153(32)) who "cause [the] caller identification service" (*see id.* § 227(e)(8)(B)) to transmit the misleading or inaccurate caller ID information to the called party. If the spoofing service provider does so with the requisite scienter, the provider itself is violating the Act. By requiring spoofing providers to implement measures to deter criminals from abusing their services, the Commission will help ensure that caller ID spoofing services do not themselves run afoul of section 227(e)(1), while preserving the legitimate role of those services in the marketplace.

As a result, this is not a case in which the Commission is being asked to regulate a service that is beyond the ambit of the underlying statutory provisions administered by the Commission. Whether or not caller ID spoofing service providers come within other areas of the Commission's regulatory jurisdiction (and as explained below, at least some of them clearly do), they are providing the very service with which the Truth in Caller ID Act is concerned.

Moreover, the Commission cannot adequately implement the underlying prohibition in Section 227(e)(1) if it categorically excludes caller ID spoofing services from the scope of its regulations under Section 227(e)(3). As explained in the Department's January 26, 2011 letter, persons who cause the transmission of false or misleading caller ID information with "the intent to defraud, cause harm, or wrongfully obtain anything of value," are pursuing ends that are themselves unlawful.[9] If they are prepared (as they must be) to risk the criminal and civil

[9] *Id.* at 3.

sanctions that attend the underlying unlawful conduct, the prospect of liability for violating Section 227(e)(1) is unlikely to alter their course of action. By contrast, modest efforts by the caller ID spoofing services to prevent criminals from abusing their services – such as those suggested in the January 26th letter or others the Commission may devise – have the potential to stop much of the targeted misconduct in its tracks.

Taken together, these considerations place the Department's concerns well within the reach of the Commission's rulemaking authority under Section 227(e)(3). The touchstone of that authority is the Commission's power and responsibility to "implement" the prohibition in Section 227(e)(1). Requiring the caller ID spoofing providers to take basic measures to prevent criminals from abusing their services implements that prohibition in a particularly effective manner, by exposing and thwarting violations before they can actually be carried out. It does so by regulating the service that is used to commit the violation. And without some such measure, there is a very real risk the prohibition may fail to be effectively implemented at all.

Congress could, of course, have imposed obligations on caller ID spoofing services by statute. But given the general grant of rulemaking authority in Section 227(e)(3), the bare fact that Congress did not impose such obligations itself does not imply that the Commission lacks the authority to do so. Indeed, the legislative history reflects a recognition that regulation of caller ID spoofing services by the Commission may be necessary in order to implement the Act. As noted earlier, Representative Boucher, a sponsor of the companion House bill and chairman of the House committee that reported out that bill, understood the Act as vesting the Commission with authority to regulate caller ID spoofing services. Representative Boucher stated explicitly in a floor statement that his committee expected that "pursuant to new subsection 227(e)(3) . . . the Commission will consider imposing obligations on entities that provide caller ID spoofing

services to the public." 156 Cong. Rec. H8378 (daily ed. Dec. 15, 2010). The suggestions outlined in the Department's January 26, 2011 letter are fully consistent with that expectation.

ii. The Communications Act of 1934

The specific grant of rulemaking authority in the Truth in Caller ID Act is supplemented by the preexisting grants of authority in the Communication Act of 1934. As the Supreme Court has explained, "[w]hen Congress enacted the Communications Act of 1934, it granted the FCC broad authority to regulate interstate telephone communications." *Global Crossing Telecommunications, Inc. v. Metrophones Telecommunications, Inc.*, 550 U.S. 45, 48 (2007). The D.C. Circuit recently reemphasized this point in *Comcast Corp. v. FCC*, 600 F.3d 642, 646 (D.C. Cir. 2010) ("Through the Communications Act of 1934, as amended over the decades, Congress has given the Commission express and expansive authority to regulate common carrier services, including landline telephony . . . ."). At bottom, caller ID spoofing services manipulate a key feature of common carrier services, the caller ID system, which has been subject to Commission regulation since 1994. *See* 47 C.F.R. § 64.1600 *et seq.* (2010). In discussing these regulations, the Commission has emphasized that "federal policies to govern the passage of Calling Party Number (CPN) over interstate facilities" are necessary because "their absence impedes the development of potentially valuable CPN based interstate services." 60 Fed. Reg. 24,489, 24,489 (Jun. 5, 1995).

In many cases, caller ID spoofing is provided by prepaid calling card services.[10] For example, the popular SpoofCard service operates as follows: a customer purchases minutes from SpoofCard and is provided a PIN number. The customer can then call a toll-free or local access number, enter his or her PIN, and provide the requested call information – the phone number to

[10] In explaining how third-party caller ID spoofing providers function in the NPRM, the Commission described the prepaid calling card business model. *See NPRM* at 4131.

be called and the number to be "spoofed." SpoofCard then completes the call, using the spoofed number in place of the caller's correct caller ID. In other words, as SpoofCard itself advertises, it is functionally indistinguishable from ordinary prepaid calling card services.[11] Many of SpoofCard's competitors, including Itellas Communications, Telespoof, and PhoneGangster, appear to function in a similar fashion.

The Commission has previously ruled that prepaid calling card services are "telecommunications services" subject to common carrier regulation under Title II of the Communications Act. *See In the Matter of Regulation of Prepaid Calling Card Services*, WC Docket No. 05-68, Declaratory Ruling and Report and Order, 21 F.C.C. Rcd. 7290, 7293 (2006) ("In conjunction with the Commission's prior rulings regarding basic prepaid calling cards and prepaid cards with advertising, all prepaid calling card providers will now be treated as telecommunications service providers."), vacated in part by *Qwest Services Corp. v. FCC,* 509 F.3d 531 (D.C. Cir. 2007); *see also AT&T Corp. Petition for Declaratory Ruling Regarding Enhanced Prepaid Calling Card Services*, WC Docket No. 03-133, Order and Notice of Proposed Rulemaking, 20 F.C.C. Rcd. 4826 (2005). Among other Title II obligations, the Commission has imposed its existing caller ID regulations, 47 C.F.R. § 64.1600 *et seq.*, on prepaid calling card services and mandated that prepaid calling card providers "pass the [caller ID information] of the calling party (i.e., the number associated with the telephone used by the cardholder) . . .". 21 F.C.C. Rcd. at 7302 (emphasis added). Because prepaid calling card services that provide caller ID spoofing are already subject to the Commission's existing caller

[11] *See* SpoofCard, *SpoofCard Frequently Asked Questions*, available at http://www.officialspoofcard.com/faqs.php ("SpoofCard works just like a regular calling card but also has advanced features, like a web control panel, Caller ID spoofing, call recording and a voice changer! SpoofCard works from any phone in the US and Canada through it's [sic] dedicated toll free number.").

ID regulations, and because the Truth in Caller ID Act itself is codified as part of Title II, the Commission has ample authority to impose requirements on such providers.

Caller ID spoofing services are also provided by some interconnected VoIP providers. Although the Commission has not classified interconnected VoIP service as a telecommunications service for the general purposes of Title II, it has previously used its ancillary authority under 47 U.S.C. § 154(i) to extend many common carrier obligations to VoIP providers. *See, e.g.*, *Nuvio Corp. v. FCC*, 473 F.3d 302 (D.C. Cir. 2006) (upholding FCC regulations imposing E911 requirements on VoIP providers); *In The Matter of Telephone Number Requirements for IP-Enabled Services Providers*, WC Docket No. 07-243, Report and Order, Declaratory Ruling, Order on Remand and Notice of Proposed Rulemaking, 22 FCC Rcd. 19531 (2007) (extending local number portability requirements to VoIP providers).[12] Here, the Commission's ancillary authority under Section 154(i), in conjunction with the provisions of the Truth in Caller ID Act, is sufficient to empower the Commission to regulate such providers.

As the D.C. Circuit has explained, the Commission may invoke its ancillary authority when (1) the subject of the regulation comes within the Commission's general jurisdictional grant in Title I over interstate and foreign communication by wire or radio, and (2) the regulations are "reasonably ancillary . . . to the effective performance of its statutorily mandated responsibilities." *Comcast Corp.*, 600 F.3d at 646. The first of these requirements is obviously met here, and the second requirement is satisfied as well, because regulation of caller ID spoofing is "reasonably ancillary" to the effective performance of the Commission's "statutorily mandated responsibilities" in at least two areas.

[12] To the extent that VoIP providers are already subject to the Commission's existing caller ID regulations, the Commission would seem to have similar authority over VoIP-based caller ID spoofing services.

First, regulation of caller ID spoofing services is reasonably ancillary to the effective performance of the Commission's responsibilities under the Truth in Caller ID Act. As discussed above and in our earlier letter, unless the Commission implements reasonable rules to govern the activities of caller ID spoofing services, it will be difficult for the Commission – or for the Department of Justice, which is responsible for criminal prosecutions under the Act – to vindicate the Congressional mandate in the Truth in Caller ID Act. Second, such regulation is also reasonably ancillary to the "effective performance" of the Commission's existing caller ID regulations, 47 C.F.R. § 64.1600 *et seq.*, which are ultimately rooted in statutory responsibilities. Those regulations, as explained, were intended to preserve "potentially valuable CPN based interstate services." 60 Fed. Reg. at 24,489. Clearly, unlawful caller ID spoofing undercuts the reliability, and thus the value, of the caller ID system.

As the Senate Committee Report accompanying the bill discussed, today caller ID spoofing services "can be accessed easily by criminals, identity thieves, or others who wish to harm or deceive someone." S. Rep. No. 111-96, at 2 (2010). The House Committee Report on the companion bill noted as well that "[s]poofing threatens a number of business applications, including credit card verification and automatic call routing, because these systems rely on the telephone number as one piece of a verification and authentication process." H.R. Rep. 111-461, at 3 (2010). Moreover, as the Department's January 26, 2011 letter noted, the widespread availability of unregulated caller ID spoofing services enables criminals to easily shield their activity from law enforcement.[13] Because the imposition of increased civil and criminal liability alone may not be sufficient to limit illegal uses of spoofing services, modest regulation of caller ID spoofing services along the lines suggested in the Department's letter would be "reasonably

[13] *DOJ Letter* at 2.

ancillary . . . to the effective performance" of the Commission's responsibilities under the Truth in Caller ID Act and the existing caller ID regulations.

B. Responses to Other Issues Raised in the NPRM

In addition to the question of whether the Commission can and should regulate spoofing providers, the NPRM sought comment on a variety of other topics related to the proposed regulations. While the Department may address those issues in its reply comments – once the public has had the opportunity to offer its views and respond to the proposals set forth in the Department's January 26, 2011 letter to the Commission – the Department addresses in these Comments two issues raised in the NPRM.

1. Clarification of "Defraud"

In the NPRM, the Commission sought comment on whether it should enact regulations clarifying the meaning of the word "defraud" used within Section 2 of the Truth in Caller ID Act.[14] The Department's view is that no additional clarification of this commonly used statutory term is necessary.

The term "defraud" is routinely used by Congress without further explication in statutes that, like the Truth in Caller ID Act, create criminal penalties. For example, the Computer Fraud and Abuse Act prohibits accessing a protected computer "knowingly and with intent to defraud." *See* 18 U.S.C. § 1030(a)(4), (6). Similar phrasing is used in 18 USC § 1029, in which the term "defraud" appears ten different times. *See* 18 USC § 1029(a)(1)-(8), (10), (e)(3). Many other criminal statutes contain similar language. *See, e.g.*, 18 U.S.C. § 286, 18 U.S.C. § 371, 18 U.S.C. § 500, 18 U.S.C § 1002, and 51 U.S.C. § 5603. Yet, in none of these statutes did Congress attempt to define the term "defraud." The Commission should follow Congress's lead,

[14] *NPRM* at 4134.

and abstain from offering a Commission-crafted definition of the term "defraud" that could unnecessarily limit the scope of the Truth in Caller ID Act and create conflicts with other statutes that use the same term.

2. Exemptions for Spoofing Activity Undertaken Pursuant to Court Order or by Law Enforcement

In its January 26, 2011 letter, the Department offered the Commission suggested language to comply with the Congressional directive that the Commission implement an exception to the provisions of the Truth in Caller ID Act for spoofing activity undertaken pursuant to a court order or by law enforcement.[15] Section 64.1604(b) of the Commission's Proposed Rules includes language that is functionally equivalent to that suggested by the Department.[16] The proposed language is acceptable to the Department, and should be included within the final regulations issued by the Commission.

IV. Conclusion

The Department of Justice urges the Commission to consider a broader rulemaking approach under the Truth in Caller ID Act that includes imposing modest regulations upon the caller ID spoofing industry. The Commission has the authority to require the industry to implement basic verification procedures or other technological solutions that will deter criminals from using these spoofing services to facilitate their illegal acts. The Truth in Caller ID Act provides the Commission with an ideal platform to enact such regulations, one the Department

[15] *DOJ Letter* at 4.

[16] *NPRM* at 4137, 4147.

hopes the Commission will use to protect the public from the growing threat posed by criminals who use caller ID spoofing services to facilitate their crimes.

Dated: April 18, 2011

Respectfully submitted,

The United States Department of Justice

/s/ Jason M. Weinstein

Jason M. Weinstein
Deputy Assistant Attorney General
Criminal Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530
(202) 616-3928