Before the
Federal Communications Commission
Washington, D.C. 20554

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

REPORT AND ORDER

Adopted: June 20, 2011 **Released: June 22, 2011**

By the Commission:

TABLE OF CONTENTS

Para.

I. INTRODUCTION

1. In this Order, we adopt rules to implement the Truth in Caller ID Act of 2009 (Truth in Caller ID Act, or Act).[1] Caller ID services typically identify the telephone numbers and sometimes the names associated with incoming calls, thus allowing consumers to decide whether or how to answer a phone call based on who appears to be calling. However, caller ID information can be altered or manipulated ("spoofed"). Increasingly, bad actors are spoofing caller ID information in order to facilitate a wide variety of malicious schemes, from identity theft to "swatting" (the practice of placing false emergency calls to law enforcement in order to elicit a response from a Special Weapons and Tactics (SWAT) team).

2. In response to the increasing use of caller ID spoofing to facilitate schemes that defraud consumers and threaten public safety, Congress passed the Truth in Caller ID Act. The Truth in Caller ID Act, and our implementing rules, prohibit any person or entity from knowingly spoofing caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value. The Commission can—and will—seek substantial penalties from those who violate the Act and the rules we adopt today.

II. BACKGROUND

3. Caller ID services became possible in the early 1980s when local exchange carriers (LECs) began adopting Signaling System Seven (SS7) signaling techniques, which carriers use to route and manage telephone calls.[2] SS7 techniques place signaling information on a separate transmission channel from the telephone call (*i.e.*, "out-of-band" instead of "in-band" signaling). Separating the signaling information from the voice traffic, along with other features of SS7, enables providers to transmit caller ID information across multiple carriers.[3]

4. In the mid-1990s, the Commission adopted rules governing interstate caller ID and other calling party number (CPN) services offered by telecommunications providers (CPN rules).[4] The CPN rules

[1] The President signed the Truth in Caller ID Act into law on December 22, 2010. Truth in Caller ID Act of 2009, Pub. L. No. 111-331, codified at 47 U.S.C. § 227(e). The Act directs the Federal Communications Commission (Commission) to issue implementing rules within six months of the law's enactment. 47 C.F.R. § 227(e)(3). On March 9, 2011, we issued a Notice of Proposed Rulemaking proposing rules to implement the Act. *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Notice of Proposed Rulemaking, 26 FCC Rcd 4128 (2011) (*Caller ID Act NPRM*). Comments on the *Caller ID Act NPRM* were due April 18, 2011 and Reply Comments were due May 3, 2011. Appendix B of this Order contains a list of commenters and reply commenters and the abbreviations we use when referring to the comments they filed in this proceeding. The Act also requires the Commission, by the same date, to submit a report to Congress on "whether additional legislation is necessary to prohibit the provision of inaccurate caller identification information in technologies that are successor or replacement technologies to telecommunications services or IP-enabled voice services." 47 U.S.C. § 227(e)(4).

[2] *See Rules and Policies Regarding Calling Number Identification Service – Caller ID*, CC Docket No. 91-281, Memorandum Opinion and Order on Reconsideration, Second Report and Order and Third Notice of Proposed Rulemaking, 10 FCC Rcd 11700, 11704–05, paras. 7–11 (1995) (*Second Caller ID Order*); *see also Rules and Policies Regarding Calling Number Identification Service – Caller ID*, CC Docket No. 91-281, Notice of Proposed Rulemaking, 6 FCC Rcd 6752, para. 2 (1991) (*Caller ID NPRM*).

[3] *See Caller ID NPRM*, 6 FCC Rcd at 6752, paras. 1–2. Early subscribers to caller ID services typically paid a monthly fee for caller ID service and usually had to purchase a separate device that received and displayed caller ID information. *Id.* Today, caller ID is provided as a standard feature of many telephone services.

[4] *See Rules and Policies Regarding Calling Number Identification Service – Caller ID*, CC Docket No. 91-281, Report and Order and Further Notice of Proposed Rulemaking, 9 FCC Rcd 1764 (1994) (*First Caller ID Order*); *Second Caller ID Order*, 10 FCC Rcd 11700.

generally require common carriers that use SS7 signaling techniques to route and manage telephone calls to transport the CPN on interstate calls to interconnecting carriers.[5] Terminating carriers can, but are not required to, display calling party numbers to their subscribers.

5. SS7 signaling techniques do not transmit the name of the calling party along with the number, but many caller ID services are able to display both the phone number of the calling party and the name associated with the calling party. The providers of caller ID services identify the name of the subscriber associated with the calling party by sending a query to a centralized calling name (''CNAM'') database or directory that associates telephone numbers with names. There are multiple CNAM databases used by providers of caller ID services.[6]

6. Under the Commission's rules, a calling party can request that his or her calling number and name not be revealed by dialing *67 (or 1167 for rotary phones) before dialing the phone number.[7] Carriers using SS7, or offering or subscribing to any service based on SS7 call set-up functionality, are required to recognize and honor calling parties' privacy requests.[8] As a result, on a call-by-call basis, most callers have the ability to block a call recipient from seeing the calling party's telephone number or name.[9] This basic framework reflects the Commission's balancing of the benefits of caller ID with the privacy issues raised by this and other CPN services.[10]

7. When the Commission first adopted its rules relating to CPN, the use of caller ID services was a new phenomenon. Over time, however, caller ID and other CPN services have become commonplace. Consumers have come to rely on caller ID services to display the phone number and sometimes name associated with an incoming call, and consumers use that information to decide whether or how to answer a phone call.[11] With the proliferation of caller ID services, caller ID spoofing has also become more commonplace. In the past, caller ID spoofing required special equipment or a relatively high degree of

[5] 47 C.F.R. § 64.1601. Earlier this year, the Commission issued an NPRM proposing revisions to section 64.1601 of our rules to require that the calling party number be provided by the originating service provider and to prohibit stripping or altering of this call signaling information. The proposed requirement would apply to interstate and intrastate traffic transmitted by telecommunications providers and entities providing interconnected voice over Internet protocol (VoIP) services. *See Connect America Fund; A National Broadband Plan for Our Future; Establishing Just and Reasonable Rates for Local Exchange Carriers; High-Cost Universal Service Support; Developing a Unified Intercarrier Compensation Regime; Federal-State Joint Board on Universal Service; Lifeline and Link-Up*, WC Docket Nos. 10-90, 07-135, 05-337, 03-109, CC Docket Nos. 01-92, 96-45, GN Docket No. 09-51, Notice of Proposed Rulemaking and Further Notice of Proposed Rulemaking, 26 FCC Rcd 4554 (2011).

[6] *See* TSN Comments at 3–4; Horowitz Comments at 1.

[7] 47 C.F.R. § 64.1601(b).

[8] *Id. See also* TNS Comments at 4.

[9] The Commission's rules exempt certain types of calls, including calls from payphones and from most Private Branch Exchanges, from the requirements to transmit CPN and to recognize and honor calling parties' privacy requests. *See* 47 C.F.R. § 64.1601(d).

[10] The Commission's rules concerning the delivery of CPN also address the transmission and use of automatic number identification (ANI) information, which is information about the phone number used for charging purposes, and may or may not be the same as the CPN. *See* 47 C.F.R. § 64.1602. When the Commission adopted its rules, it found that ANI blocking was not technologically feasible, and that use of ANI did not raise the same privacy concerns as the use of CPN services. Therefore, instead of requiring that ANI blocking be made available to subscribers, the Commission required carriers offering ANI services to limit the permissible uses of ANI. *See First Caller ID Order*, 9 FCC Rcd at 1772–74, paras. 51–58.

[11] *See* Copilevitz Comments at 1; Horowitz Comments at 1; Minnesota AG Comments at 1; TNS Comments at 2; Verizon Reply at 1.

technical sophistication.[12] Now anyone can inexpensively spoof their caller ID by using the services of a third-party spoofing provider.[13]

8. The ease with which callers can spoof their caller ID information is a function of the widespread availability of VoIP technology and the growth of third-party caller ID spoofing services.[14] Callers using some interconnected VoIP services can easily alter their caller ID by making a call appear to come from any phone number.[15] Callers who subscribe to legacy telephone services (and interconnected VoIP services) also can easily spoof their caller ID by purchasing caller ID spoofing services from third parties. Caller ID spoofing services are openly advertised on the Internet, and callers can purchase prepaid cards in retail stores and use them for caller ID spoofing services.[16] There are also companies that offer "caller identification management services" to business customers that enable those business customers to transmit modified CPNs.[17] Because the terminating provider often has no direct relationship with the person placing a call, that provider often has no way to determine the accuracy of the caller ID information it receives and provides to its subscribers.[18]

9. As Congress recognized, and as the record demonstrates, not all instances of caller identification manipulation are harmful, and some may be beneficial.[19] Commenters offered a variety of legitimate reasons for altering caller ID information. For example, as discussed in the *Caller ID Act NPRM*, because many phones are set to refuse calls where the caller ID information is not provided, domestic violence shelters often need to transmit caller ID to complete a call but may have important reasons for not revealing the actual number of the shelter.[20] Likewise, doctors responding to after-hours messages from their patients or other medical providers may want to use their cell phones to return the

[12] *See* DOJ Comments at 2; *see also* InCharge Comments at 1–2.

[13] *See* DOJ Comments at 2; Itellas Comments at 12; NNEDV Comments at 1, 5–13 (describing websites operated by caller ID spoofing providers).

[14] *See Truth in Caller ID Act, Report of the Committee on Commerce, Science, and Transportation on S. 30*, S. REP. NO. 111-96, at 1–2 (2009) (Senate Commerce Committee Report); *see also* NNEDV Comments at 1; InCharge Comments at 1.

[15] *See* Senate Commerce Committee Report at 2; InCharge Comments at 1–2. As discussed *infra* at paras. 27–28, in adopting rules implementing the Act, we use the term "interconnected VoIP services" to be consistent with our existing rules and the direction in the Act. Congress used the term "IP-enabled voice services."

[16] *See* Itellas Comments at 1–2 (describing how consumers can purchase and use Itellas' spoofing services); TelTech Comments at 5–6, 9 (describing how consumers can purchase and use TelTech's spoofing services, including through the purchase of prepaid cards available at retail locations); NNEDV Comments at 5–13 (describing websites operated by caller ID spoofing providers).

[17] *See, e.g.*, NobelBiz Comments at 1; InContact Comments at 1–2; *see also* ATA Comments at 2–3 (explaining that its members operate inbound and outbound "contact centers" and that some "manipulate Caller ID for legitimate business reasons").

[18] *See* AT&T Comments at 5; ATIS Comments at 5; USTelecom Comments at 4; VON Comments at 9.

[19] Senate Commerce Committee Report at 2 (stating that "it is important to recognize that there are some more benign uses of this technology"); *see also* ATA Comments at 3 (explaining that some ATA members manipulate caller ID for legitimate reasons and without the requisite intent to invoke the statute); AT&T Comments at 8–9; Horowitz Comments at 1; inContact Comments at 7; Inter-Agency Comments at 1; NNEDV Comments at 3.

[20] *Caller ID Act NPRM*, 26 FCC Rcd at 4132, para. 7. For example, a domestic violence victim may need to call an abuser from a program or shelter office as part of a court order to discuss custody issues, and use spoofing to ensure the abuser will pick up the call and not determine the victim's location. Alternatively, domestic violence assistance programs may need to call phone lines that are not "safe"—such as lines monitored by an abusive partner—in order to check-in with a program participant, or respond to a victim call, without alerting the abuser. NNEDV Comments at 3. *See also* Senate Commerce Committee Report at 2 (discussing the use of caller ID spoofing by domestic violence shelters).

calls, but choose to transmit their office number rather than their cell phone number as the calling number.[21] The Commission's own rules require telemarketers to transmit caller identification information, but allow for the substitution of the name and customer service number of the seller on whose behalf the telemarketer is calling, as long as the telephone number provided is one a consumer can use to make a do-not-call request during regular business hours.[22] Carriers may also manipulate caller ID to test equipment to emulate the customer experience or to investigate fraudulent use of the network.[23]

10. While caller ID manipulation may sometimes be in the public interest, it is a practice ripe for abuse.[24] Numerous well-publicized examples of caller ID spoofing led to Congressional concern about the misuse of caller ID systems.[25] The comments received by the Commission underscore the alarming use of caller ID spoofing for malicious purposes.[26] In its comments, the United States Department of Justice (DOJ) describes various scenarios in which bad actors use caller ID spoofing to carry out their schemes.[27] For example, DOJ describes the "particularly insidious form of fraud known as 'swatting.'" As DOJ explained, "[s]watting 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."[28] DOJ also describes the use of caller ID spoofing in connection with stalking and harassment; to carry out identity theft schemes; and to gain unauthorized access to cell phone voicemail.[29] Third-party spoofing providers do not dispute that caller ID is used for nefarious purposes. Indeed, Teltech Systems and Itellas, two providers of caller ID spoofing services that filed comments in response to the *Caller ID Act NPRM*, both acknowledge that they respond to numerous law enforcement requests for information.[30] The record indicates that the incidence of malicious spoofing is increasing.[31]

---

[21] *See* PRC Reply at 3; DOJ Reply at 4–5.

[22] *See* 47 C.F.R. § 64.1601(e). Similarly, the FTC's Telemarketing Sales Rule requires a telemarketer to transmit its own caller identification information or that of the entities on whose behalf the telemarketer is working. 16 C.F.R. § 310.4(a)(7). See *infra* para. 36 for a more extensive discussion of the benefits of requiring telemarketers to transmit caller ID information.

[23] AT&T Comments at 8.

[24] *See* Minnesota AG Comments at 1 ("'[S]poofing' of Caller ID services is a substantial problem for Minnesota consumers and their ability to protect themselves against criminal activity conducted by telephone."); DOJ Comments at 2 ("[T]he widespread availability of caller ID spoofing services is a significant facilitator of criminal activity and a substantial threat to public safety."); and DOJ Reply at 2 ("The comments filed in response to the NPRM make abundantly clear that criminals are routinely using caller ID spoofing to further their criminal activity.").

[25] *See* Senate Commerce Committee Report at 1–2.

[26] *See, e.g.*, DOJ Comments at 2–4; Minnesota AG Comments at 1–2; NNEDV Comments at 5–7; PRC Reply at 1. Caller ID spoofing is not only a problem for the person at whom the spoofing is directed, it can also be an expensive and difficult to solve problem for entities whose numbers are being spoofed. *See* JSM Comments at 1 (describing the challenges faced by a paging system that had one of its unassigned telephone numbers spoofed hundreds of thousands of times).

[27] *See* DOJ Comments at 2–3.

[28] *Id.* at 2.

[29] *Id.* at 3.

[30] Itellas Comments at 4–5; TelTech Comments at 8–9.

[31] *See* AT&T Comments at 1 (AT&T has received an increasing number of customer inquiries and complaints regarding spoofing); DOJ Comments at 6 (explaining that DOJ's experience includes a rapidly increasing number of investigations involving criminals who have used caller ID spoofing services to commit their crimes); Minnesota AG Comments at 1 (asserting that Caller ID spoofing is a substantial problem that must be addressed through

(continued....)

11. In order to address the growing problem of caller ID spoofing done for fraudulent or harmful purposes, Congress enacted the Truth in Caller ID Act. The 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."[32] The Act directs the Commission to issue implementing regulations within six months, provides for additional civil penalties for violations of the Act, and establishes a two-year statute of limitations.[33] On March 9, 2011, the Commission issued the *Caller ID Act NPRM* seeking comment on proposed rules to implement the Truth in Caller ID Act.[34]

III. IMPLEMENTATION OF THE TRUTH IN CALLER ID ACT

12. Having considered the record in this proceeding, we adopt rules to carry out the Commission's statutory obligation to implement the Truth in Caller ID Act.[35] The rules we adopt include only modest changes to the rules the Commission proposed in the *Caller ID Act NPRM*.

13. In amending the Commission's CPN rules, we adopt rules that prohibit any person or entity in the United States, acting with the intent to defraud, cause harm, or wrongfully obtain anything of value, from knowingly causing, directly or indirectly, any caller identification service to transmit or display misleading or inaccurate caller identification information.[36] The revisions to our CPN rules are modeled on the Act's prohibition against knowingly engaging in caller ID spoofing with fraudulent or harmful intent. The rules include exemptions based on conduct the Act identifies as exempt from its prohibitions. The revised rules also include new definitions, including several modeled after definitions in the Act. As proposed in the *Caller ID Act NPRM*, the revised rules also specify that blocking or attempting to block one's own caller ID is not a violation of the new rules, while clarifying that telemarketers are not relieved of their obligation to transmit caller identification information.

(...continued from previous page)
comprehensive regulation of the industry); InCharge Comments at 4 (asserting that caller ID spoofing is a serious problem today that is certain to grow in frequency and severity).

[32] 47 U.S.C. § 227(e)(1).

[33] *Id.* § 227(e)(3), (e)(5)(A)(i), and (e)(5)(A)(iv). The Act also provides for criminal penalties for anyone who is convicted of willfully and knowingly violating the Act, and gives the States authority to bring civil actions in federal district court to enforce the Act on behalf of their residents. *Id.* § 227(e)(5)(B) and (e)(6).

[34] *See Caller ID Act NPRM*, 26 FCC Rcd 4128.

[35] Final rules can be found in Appendix A.

[36] *See* 47 C.F.R. § 64.1604(a) in Appendix A. Commenters were generally supportive of the Commission's proposal to prohibit caller ID spoofing done with malicious intent. *See* ATIS Comments at 1 (supporting the government's efforts to prohibit the transmission of misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value); AT&T Comments at 3 (fully supporting the Commission's anti-spoofing regulations); inContact Comments at 1 (supporting the Commission's goal of protecting consumers from harmful caller ID spoofing); NECA *et al.* Comments at 2 (generally supporting the Commission's proposed rules); VON Comments at 3 (generally supporting the Commission's proposed rules); TNS Comments at 2 (supporting government efforts to prohibit calling parties from defrauding called parties through spoofing); Google Reply at 1–2 (generally supporting the Commission's proposed rules); NobelBiz Reply at 1 (generally supporting the Commission's proposed approach); NCTA Reply at 2 (supporting the Commission's proposed rules).

A. Prohibited Practice

14. The principal implementing rule we adopt provides 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 wording of the prohibition in our rules generally tracks the wording of the prohibition in the Act, and is unchanged from the rule the Commission proposed in the *Caller ID Act NPRM*.

15. The Act specifies that the prohibited conduct is "in connection with any telecommunications or IP-enabled voice service." Because we define the terms "caller identification service" and "caller identification information" to encompass the use of telecommunications services and "interconnected VoIP services," we do not need to specify in the rule that the prohibition encompasses calls made using telecommunications services and IP-enabled voice services, as specified in the Act.[37]

16. We also note that the Act is directed at "any person," but does not define the term "person." In order to make clear that the rules are not limited to natural persons and to be consistent with the Commission's current rules concerning the delivery of CPN,[38] our amendments to the CPN rules use the phrase any "person or entity."[39] The only commenter that addressed the use of the phrase "person or entity" in the proposed rules supported the Commission's clarification that the rule applies to both natural persons and other entities.[40]

17. In the *Caller ID Act NPRM*, the Commission asked about the placement of the term "knowingly" in the proposed rules.[41] As with the proposed rules, the rules we adopt today provide that in order to violate the rules, the person or entity "knowingly" causing transmission or display of inaccurate or misleading caller identification must be the same person or entity that is acting with intent to defraud, cause harm, or wrongfully obtain anything of value. The Truth in Caller ID Act is aimed at prohibiting the use of caller ID spoofing for ill intent. Therefore, we believe that an entity subject to liability for violating the Act must knowingly spoof caller identification information and do so with intent to defraud, cause harm, or wrongfully obtain something of value.

18. Most commenters agreed with the Commission's proposal to clarify that the word "knowingly" modifies the action of the person or entity engaged in malicious caller ID spoofing because this is the most logical reading of placement of the word in the Truth in Caller ID Act.[42] However, in its reply

---

[37] As discussed below, in our rules we use the term "interconnected VoIP service," whereas the Act uses the term "IP-enabled voice service." We do this because the Act defines "IP-enabled voice service" as having "the meaning given that term by Section 9.3 of the Commission's regulations (47 C.F.R. 9.3), as those regulations may be amended by the Commission from time to time." 47 U.S.C. § 227(e)(8)(C). Section 9.3 of the Commission's regulations defines "interconnected VoIP service" not "IP-enabled voice service." *See infra* paras. 27–28.

[38] *See* 47 C.F.R. § 64.1601(e).

[39] By contrast, the amendments to the Commission's forfeiture rules use the term "person" in order to be consistent with use of the term "person" in the forfeiture rules. In both cases, we intend for the entities covered to be those within the scope of the definition of "person" in the Communications Act. *See* 47 U.S.C. § 153(32) ("The term 'person' includes an individual, partnership, association, joint-stock company, trust or corporation.").

[40] VON Comments at 3–4 (agreeing that expanding compliance obligations to individuals and entities "achieves Congress' underlying goal - to stop malicious, fraudulent and harmful actions of the Caller ID spoofer").

[41] *Caller ID Act NPRM*, 26 FCC Rcd at 4133, para. 13.

[42] *See, e.g.*, TNS Comments at 5 (agreeing that the rule should be focused on whether the caller has knowingly manipulated caller ID information in order to defraud, cause harm or wrongfully obtain anything of value); VON Comments at 4–5; Google Reply at 3 (stating that "the draft regulations correctly focus on persons that *knowingly*

(continued....)

comments, the Privacy Rights Clearinghouse (PRC) recommends that the Commission change the placement of the word "knowingly" so that it modifies the actions of the caller identification service or modify the rule so that spoofing services are prohibited from knowingly transmitting misleading or inaccurate caller identification information for a party violating the Act.[43] PRC argues that requiring that the same person or entity knowingly cause the transmission or display of misleading or inaccurate caller identification information and have the requisite intent to "defraud, cause harm, or wrongfully obtain anything of value" imposes an unnecessary hurdle to enforcement efforts.[44]

19. We disagree with PRC's arguments. Based on our reading of the statute, it is not enough that a person or entity intend to defraud, cause harm, or wrongfully obtain anything of value to violate the Truth in Caller ID Act. Rather, the person or entity intending to defraud, cause harm or wrongfully obtain anything of value must facilitate the scheme through the manipulation or alteration of caller identification information. Moreover, adopting a rule in which "knowingly" modifies the action of the caller identification service would not impose liability on caller ID spoofing services for knowingly manipulating caller identification information absent intent to defraud, cause harm, or wrongfully obtain anything of value. Nor would it ease the burden on law enforcement of proving a violation of the Act. Instead, it would require law enforcers to show that the provider of the caller ID service—usually a terminating carrier or VoIP provider—knew that the incoming caller identification information was manipulated or altered. As the Commission noted in the *Caller ID Act NPRM*, "in many instances the caller identification service has no way of knowing whether or not the caller identification information it has receives has been manipulated."[45] We do not believe Congress intended to impose liability on caller ID spoofers acting with malicious intent only upon proof that the provider of the call recipient's caller ID service knew that the caller identification information was manipulated or altered. That would be a perverse result, wholly inconsistent with the intent of the Act and its legislative history.[46]

20. As for PRC's suggestion that we modify the rule to hold spoofing providers liable for transmitting inaccurate or misleading caller identification information on behalf of someone violating the Act, as discussed below, we choose to follow Congress' lead in not imposing additional obligations on spoofing providers.[47] We find that the proposed rules and the rules we adopt today are consistent with Congressional intent to focus on whether a person or entity has knowingly manipulated the caller identification information in order to defraud, cause harm, or wrongfully obtain anything of value, and

(...continued from previous page)
manipulate caller ID information with the intent to cause harm"); NCTA Reply at 2 (agreeing that liability should fall on those entities possessing both intent and knowledge of the harmful or fraudulent activity).

[43] PRC Reply at 3–4. Under PRC's proposal the rule would provide that "No person or entity in the United States shall, acting with intent to defraud, cause harm, or wrongfully obtain anything of value, cause, directly or indirectly, any caller identification service to **knowingly** transmit or display misleading or inaccurate caller identification information." (emphasis added). Whereas the proposed rule, and the rule we adopt today provides that "No person or entity in the United States, shall, acting 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." (emphasis added).

[44] *Id.*

[45] *Caller ID Act NPRM*, 26 FCC Rcd at 4134, para. 13; *see also* AT&T Comments at 7; ATIS Comments at 5; USTelecom Comments at 4; VON Comments at 4–5.

[46] To the extent PRC's concern is that the rules may not cover bad actors that engage a third party to cause the transmission or display of inaccurate or misleading caller identification information, we address such concern in our rules. As explained below, the rules adopted herein cover situations in which a person or entity "directly or indirectly" causes a caller identification service to transmit or display misleading or inaccurate caller ID. *See infra* para. 20.

[47] *See infra* paras. 38–39.

therefore we adopt the prohibition on caller ID spoofing as proposed in the *Caller ID Act NPRM*.[48] The person or entity that knowingly causes caller ID services to transmit or display misleading or inaccurate information may, in some cases, be a carrier, spoofing provider or other service provider, and we do not exempt such conduct from the purview of our rules.[49]

21. Like the proposed rules, the rules we adopt today address both transmission and display of misleading or inaccurate caller identification 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 anything of value. We also note that the rules we adopt today cover situations in which a person or entity is "directly or indirectly" causing a caller identification service to transmit or display misleading or inaccurate caller ID. We include the concept of "indirect" action in our rules to foreclose those acting with the requisite harmful intent from arguing that they are not liable merely because they have engaged a third party to cause the transmission or display of inaccurate or misleading caller identification information.

22. In the *Caller ID Act NPRM*, the Commission sought comment on whether the proposed prohibition on causing any caller identification service to transmit or display "misleading or inaccurate" caller identification information with the "intent to defraud, cause harm, or wrongfully obtain anything of value" provides clear guidance about what actions are prohibited.[50] Commenters generally agreed that the terms in the proposed rule were sufficiently clear.[51] We agree. Although we do not believe it is necessary to offer additional definitions to clarify the meaning of the prohibited actions, we do agree with the National Network to End Domestic Violence (NNEDV) that the term "harm" is a broad concept that encompasses financial, physical, and emotional harm, include stalking, harassment, and the violation of protection and restraining orders.[52] Moreover, NNEDV offers substantial evidence that abusive spouses

[48] One commenter asks that we clarify that the word "knowingly" applies to the words "misleading or inaccurate." Copilevitz Comments at 2. We intend for the word knowingly to modify the balance of the sentence that follows the word "knowingly."

[49] *See* NECA *et al.* Comments at 7; USTelecom Comments at 3 (asserting that to the extent a carrier or provider manipulates caller ID to defraud, cause harm, or wrongfully obtain anything of value, the Commission's rules should apply); Copilevitz Comments at 3 (asserting that "knowingly" would not apply to the caller ID service itself, absent intent to defraud); inContact Comments at 3–4 (stating that the FCC should only penalize providers who are themselves acting with intent to defraud or deceive consumers). By contrast, in its reply comments, Verizon suggested that we amend the proposed rule to specify the prohibition is directed at the entity that initiates the call. *See* Verizon Reply at 6–7. We decline to adopt Verizon's suggestion, as it is not supported by the language of the Act and could lead to an unnecessarily cramped reading of our rule. Indeed, we believe that caller ID spoofing done to wrongfully avoid payment of intercarrier compensation charges—whether by the originating provider, an intermediate carrier, or other intermediate entity—would be a violation of our rules.

[50] *Caller ID Act NPRM*, 26 FCC Rcd at 4134, para. 14.

[51] *See, e.g.*, DOJ Comments at 14–15 (arguing that there is no need to clarify the meaning of the term "defraud."); PRC Reply at 4–5 (advising the Commission to refrain from further defining these terms to avoid the danger of creating loopholes); Google Reply at 3 (asserting that the statutory language in the proposed rules provides sufficient guidance to enable parties to determine the actions prohibited). *But cf.* inTouch Comments at 4 (asserting that the Commission should narrowly define "defraud, cause harm or wrongfully obtain anything of value" to protect legitimate uses of caller ID blocking technology); SLSA Comments at 2 (asserting that the proposed regulations do not provide definitions for the key terms such as defraud, cause harm or wrongfully obtain anything of value).

[52] *See* NNEDV Comments at i, 4–8.

use third-party caller ID services to harass and stalk their victims.[53] We consider knowing manipulation or alteration of caller identification information for the purpose of harassing or stalking someone to be an egregious violation of the Act and of our rules implementing the Act. We intend to enforce our rules vigorously, including against those who engage in such malicious practices, and we encourage spoofing providers to notify their customers in no uncertain terms that such actions are illegal.[54]

B. Exemptions

23. The Act directs the Commission to exempt from its regulations (i) any authorized activity of a law enforcement agency; and (ii) court orders that specifically authorize the use of caller identification manipulation.[55] Separately, the Act also makes clear that it "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State or a political subdivision of a State, or of an intelligence agency of the United States."[56] DOJ requested that the Commission explicitly incorporate lawfully authorized investigative, protective, or intelligence activities into the exemptions to the Commission's implementing rule.[57] In light of the statutory language specifying that such activities are not prohibited by the Act and DOJ's request that such activities be included in the exemptions to the Commission's implementing rule, the proposed rule incorporated the two exemptions specified in the Act, and expanded the exemption for law enforcement activities to cover protective and intelligence activities. No commenters objected to the proposed rule, and AT&T, the only commenter other than DOJ that addressed the exemptions in the proposed rule, supported their adoption.[58] Thus, the record supports our decision to include those exemptions in the rule we adopt today.[59]

24. We decline to adopt any other exemptions from the Act. Commenters have proposed a number of additional exemptions, all of which cover practices that, as described by the commenters themselves, would not violate the plain language of the Act. Some commenters assert that absent additional exemptions, the rules might be misinterpreted to prohibit normal and helpful business practices, such as those designed to facilitate communications with customers.[60] As a result some commenters ask for broad exemptions to the Act. AT&T, for example, asks the Commission to make clear that caller ID manipulation "for legitimate business reasons" is exempt; inContact asks the Commission to "exempt all uses not specifically intended to defraud or deceive consumers"; and USTelecom and Verizon ask the

[53] *See* NNEDV Comments at 4; *see also* DOJ Comments at 3 (warning that caller ID spoofing services are often used in connection with stalking and harassment).

[54] As explained *infra* at para. 39, while we decline to require third-party spoofing providers to notify their users of the legal ramifications of impermissible caller ID spoofing, we think the public interest would be well served should they choose to do so. *See* NNEDV Comments at 5–13 (describing postings on spoofing providers' websites that talk about using the services to scare or otherwise harass others).

[55] *See* Truth in Caller ID Act, 47 U.S.C. § 227(e)(3)(ii).

[56] *Id.* § 227(e)(7).

[57] Letter from Lanny A. Breuer, Assistant Attorney General, U.S. Department of Justice, to Marlene H. Dortch, Secretary, FCC, at 4 (Jan. 26, 2011) (DOJ Jan. 26, 2011 Letter); DOJ Comments at 15 (supporting the language in the proposed rule exempting law enforcement activity).

[58] *See* AT&T Comments at 7 (supporting the two exemptions proposed by the Commission); *see also* DOJ Comments at 15 (supporting the exemptions in the proposed rule).

[59] *See, e.g.*, AT&T Comments at 7 (supporting the two exemptions proposed by the Commission); DOJ Comments at 15 (supporting the language in the proposed rule exempting law enforcement activity).

[60] SLSA Comments at 1; AT&T Comments at 9.

Commission to exempt "any action required by law or permitted under 64.1601(d)."[61] Still other commenters propose exemptions for caller identification manipulation involving specific types of practices or actors. For example, a number of commenters representing telecommunications and VoIP providers express support for an exemption for carriers and providers that transmit caller ID information they receive from their customers or other providers, even if it turns out to be inaccurate.[62] Commmenters that provide call management services for telemarketers and debt collectors, and those that provide caller ID spoofing services to the public, suggest that they should be exempt from responsibility for bad actors, unless the service provider has the necessary intent to defraud, cause harm, or wrongfully obtain anything of value.[63] Companies that provide call management services to telemarketers and debt collectors have also asked the Commission for an exemption allowing manipulation of caller ID information so that a call recipient's caller ID displays a local number, regardless of where the calling party is located.[64] NNEDV suggests that the Commission exempt victim service providers, and a private investigator requests that the Commission include an exemption for lawful use by licensed private investigators.[65] We do not find any of these exemptions to be necessary or appropriate.

25. The legislative history of the Act makes clear that manipulation or alteration of caller ID information done without the requisite harmful intent does not violate the Act.[66] Nothing in our implementing rules changes that fact.[67] Likewise, the transmission of incorrect caller ID information by carriers and providers acting without the requisite intent to defraud, cause harm or wrongfully obtain anything of value does not violate the Truth in Caller ID Act or our rules implementing the Truth in Caller ID Act. Moreover, we agree with DOJ that "none of the commenters who advocated for a status-based exemption to the Truth in Caller ID Act were able to articulate any scenario whereby legitimate

[61] AT&T Comments at 9; inContact Comments at 6; USTelecom Comments at 4; Verizon Reply at 4–5; *see also* SLSA Comments at 1 (seeking an exemption for "valid commercial operations not involving intent to defraud, cause harm or wrongfully obtain anything of value"); SoundBite Reply at 3; NCTA Reply 1–3.

[62] ATIS Comments at 5; AT&T Comments at 7–8; NECA *et al*. Comments at 11; USTelecom Comments at 3; NCTA Reply at 1–3; Verizon Reply at 3–4.

[63] *See* inContact Comments at 6 (asserting that while the statute arguably immunizes third-party providers that do not "knowingly" attempt to mislead or defraud consumers, entities that neither provide a spoofed ID nor mask calls with intent to defraud should be fully protected); Itellas Comments at 9–10 (arguing that the Commission should make clear that any provider of spoofing services is exempt from liability unless the service provider has the necessary intent to defraud, cause harm, or wrongfully obtain anything of value); TelTech Comments at 15.

[64] *See* NobelBiz Comments at 4–6; NobelBiz Reply at 3; SoundBite Reply at 3.

[65] NNEDV Comments at 2–4; Inter-Agency Comments at 1.

[66] *See* Senate Commerce Committee Report at 2 (recognizing that there are legitimate uses of caller ID manipulation and stating that "efforts to curtail Caller ID spoofing should focus on actions by persons with intent to deceive or cause harm"). *See also* Google Reply at 2 (recognizing that "the proposed rules have been carefully tailored to fulfill Congress' intent to stop harmful practices while ensuring that legitimate conduct is not stifled by unnecessary regulation"). Indeed, some of the commenters seeking exemptions for caller identification manipulation done without intent to defraud, cause harm, or wrongfully obtain anything of value, acknowledge that the activities in question do not violate the Act. *See, e.g.*, Verizon Reply at 2 (acknowledging that "[b]y its very terms, the Act would not cover existing practices relating to Caller ID by carriers and interconnected VoIP providers because the providers would lack the necessary knowledge and intent").

[67] We note that those commenters that requested that the Commission exempt manipulation of caller ID information in order to display a local phone number, asked in the alternative that the Commission clarify that manipulating caller ID to display a local number is not a violation of the Act. NobelBiz Comments at 4–8; NobelBiz Reply at 3–4. We agree that such a practice is not in and of itself a violation of the Act. We note, however, that if the display of a "spoofed" local number is done as part of a scheme to defraud, cause harm, or wrongfully obtain anything of value, then the person or entity perpetrating the scheme would be in violation of the Act.

conduct would fall within the prohibitions of the Act."[68] Like DOJ, we fear that allowing any such exemptions could "create dangerous loopholes under the Act that could be exploited by criminals."[69] Therefore, we decline to adopt any further exemptions from the Act at this time, primarily because the ones that have been presented to us are unnecessary.

C. Definitions

26. The *Caller ID Act NPRM* proposed adding definitions to the Commission's CPN rules for "Interconnected VoIP service"; "Caller identification information"; "Caller identification service"; and "information regarding the origination" of a call. We adopt the proposed definitions for all four of those terms, with slight modifications to the definitions of "Caller identification service" and "information regarding the origination."

27. *Interconnected VoIP service*. The Truth in Caller ID Act covers caller ID spoofing done "in connection with any telecommunications service or IP-enabled voice service."[70] As mentioned above, the rules we adopt today use the term "interconnected VoIP service" instead of "IP-enabled voice service."[71] We define "interconnected VoIP service" to have the same meaning given that term in section 9.3 of the Commission's rules. We do this because the Act specifies that the term IP-enabled voice service has the "meaning given that term by section 9.3 of the Commission's regulations (47 C.F.R. 9.3) as those regulations may be amended by the Commission from time to time."[72] Section 9.3 of the Commission's rules defines "interconnected VoIP service," not "IP-enabled voice service."[73] Therefore, to be consistent with the apparent intent of Congress in enacting the Truth in Caller ID act, we limit the scope of the rule's coverage to telecommunications services and interconnected VoIP services.[74]

28. DOJ and some other commenters recommend that we adopt rules that cover VoIP services more expansively than the Commission's definition of "interconnected VoIP" service in section 9.3 of its rules does.[75] We find that the Act's incorporation of the Commission's rule defining interconnected VoIP

---

[68] DOJ Reply at 7.

[69] *Id.*

[70] 47 U.S.C. § 227(e)(1).

[71] *See supra* note 37.

[72] 47 C.F.R. § 222(e)(8)(c).

[73] *See* 47 C.F.R. § 9.3 which defines "interconnected VoIP service" and states:

An interconnected Voice over Internet Protocol (VoIP) Service is a service that:
(1) Enables real-time, two-way voice communications;
(2) Requires a broadband connection from the user's location;
(3) Requires Internet protocol-compatible customer premises equipment (CPE); and
(4) Permits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network.

[74] We note that while "telecommunications service" is defined in the Communications Act to mean the offering of telecommunications to the public for a fee, 47 U.S.C. § 153(46), there is no such commercial requirement for interconnected VoIP service. Therefore, an entity that self-provisions a VoIP service that interconnects with the PSTN in a manner that meets the criteria of section 9.3 is covered by the Truth in Caller ID Act.

[75] *See* DOJ Jan. 26, 2011 Letter at 4–5; DOJ Reply at 7-8; *see also* ATIS Comments at 4 (supporting DOJ's proposal to use the definition of IP-enabled voice service in 18 U.S.C. § 1309(h)(4) because it would allow the Commission to apply the prohibitions in the Act more broadly); AT&T Comments at 4–5 (arguing that the Commission should use the term IP-enabled voice service, rather than interconnected VoIP, because spoofing is technology neutral); NENA Comments at 2 (commending the DOJ proposal as a workable definition of IP-Enabled services); NECA *et al*. Comments at 4–5 (agreeing with DOJ that the Commission should use a broader definition of IP-enabled voice

(continued....)

service calls for applying the current definition found in section 9.3 (as it may be amended over time).[76] Consequently, the rules we adopt today use the term "interconnected VoIP service" and specify that it has the same meaning given the term "interconnected VoIP service" in 47 C.F.R. § 9.3 as it currently exists or may hereafter be amended. However, we are cognizant of the importance of protecting consumers from malicious caller ID spoofing as broadly as possible. To that end, we raise this issue in the Report to Congress for further consideration.

29. *Caller identification information.* We define "caller identification information" to mean "information provided by a caller identification service regarding the telephone number of, or other information regarding the origination of, a call made using a telecommunications service or interconnected VoIP service." This is the definition the Commission proposed in the *Caller ID Act NPRM* and no commenters offered any reason not to use this definition.[77]

30. *Caller identification service.* We define "caller identification service" to mean "any service or device designed to provide the user of the service or device with the telephone number of, or other information regarding the origination of, a call made using a telecommunications service or interconnected VoIP service." Unlike the proposed rule, the definition of "caller identification service" that we adopt today does not explicitly reference automatic number identification (ANI) because, as discussed below, we have defined "information regarding the origination" to include "billing number information, including charge number, ANI, or pseudo-ANI."[78] By including such billing number information in the definition of "information regarding the origination" we effectively include within the definition of "caller identification service" any service or device designed to provide the user with any form of the calling party's billing number, including charge number, ANI, or pseudo-ANI.

31. *Information regarding the origination (of a call).* The definitions of "caller identification information" and "caller identification service" in the Act and in the rules we adopt today both use the phrase "the telephone number of, or other information regarding the origination of, a call." We define "information regarding the origination" to mean any: (1) telephone number; (2) portion of a telephone number, such as an area code; (3) name; (4) location information; (5) billing number information, including charge number, ANI, or pseudo-ANI; or (6) other information regarding the source or apparent source of a telephone call. The definition we adopt today mirrors the proposed definition, but adds "billing number information including charge number, ANI, or pseudo-ANI" to the types of information that constitute "information regarding the origination." We add these types of information to the definition of "information regarding the origination" in response to commenters' concerns about the

---

(...continued from previous page)
services to ensure that caller ID requirements will apply to voice services regardless of the network configuration used to connect customers and transport calls); Texas 911 Agencies Comments at 2–3 (agreeing with DOJ's suggestion for a broader definition of IP-enabled services to make clear that it covers VoIP services that arguably are not covered by the current definition of interconnected VoIP services).

[76] Our conclusion is in line with past Congressional actions. For example, in 2008, Congress amended section 222 of the Communications Act, which addresses privacy of customer information, to include a reference to "the user of an IP-enabled voice service (as such term in defined in section 615(b) of this title)." *See* 47 U.S.C. §§ 222(d)(4), (f)(1); Pub.L. 110-283, § 301(1). Section 615(b), in turn, defines IP-enabled voice service as "the meaning given the term interconnected VoIP service by section 9.3 of the Federal Communications Commission's regulations (47 CFR 9.3)." *See* 47 U.S.C. § 615(b). The purpose of the amendment to section 222 was to add "VoIP 911 service to the established 911 exceptions." New and Emerging Technologies 911 Improvement Act of 2008 (NET 911 Improvement Act of 2008), H.R. REP. No. 110-442 (Nov. 13, 2007).

[77] We note that we do expand the definition of "information regarding the origination" to include "the calling party's billing number information, including ANI information and pseudo-ANI information," which effectively expands the definitions of both "caller identification information" and "caller identification service."

[78] *See infra* paras. 31–33.

importance of transmission of accurate billing information, including charge number, ANI and pseudo-ANI, to caller identification services used by emergency services providers.

32. Our current rules relating to the delivery of CPN services define ANI as referring to the "delivery of the calling party's billing number by a local exchange carrier to any interconnecting carrier for billing or routing purposes, and to the subsequent delivery of such number to end users."[79] The *Caller ID Act NPRM* sought comment on whether the Commission should use a different definition of ANI for purposes of the Truth in Caller ID Act, and in particular, whether the Commission should include a definition of ANI that encompasses charge party numbers delivered by interconnected VoIP providers.[80] Some commenters requested that the Commission revise the current definition of ANI to encompass billing numbers delivered by interconnected VoIP providers.[81] The terms ANI, calling party number, and charge number in section 64.1600 of our rules are used in sections of the rule that we have not addressed in this rulemaking; therefore we decline to amend those definitions at this time.[82] Other commenters more generally suggested that the Commission make sure to include billing numbers, charge number, ANI and pseudo-ANI information within the ambit of the rule.[83]

33. Spoofing caller identification information transmitted to emergency services providers is a particularly dangerous practice, and one that Congress was particularly concerned about when adopting the Truth in Caller ID Act.[84] ANI and pseudo-ANI are the foundations of the emergency services routing infrastructure in the United States and derive their data exclusively from information maintained in the records of the originating carrier.[85] The delivery of accurate information for any person who dials 911 or seeks assistance via 10-digit emergency and non-emergency numbers is fundamental to ensuring that the correct identifying information is transmitted with those calls.[86] While this information may not be subject to manipulation by callers in the ordinary course, if an individual or entity did spoof ANI, the individual could conceal his or her identity and location, and could tie up public response capacity by initiating spoofed calls designed to cause the dispatch of responders to locations where no emergency is at hand.[87] Given the rapid evolution of technology, and the consequences of spoofing ANI and pseudo-ANI, we find that the delivery of caller identification information to E911 public safety answering points (PSAPs), which use ANI or pseudo-ANI to look up the caller's name and location information on emergency calls, should be considered a type of "information regarding the origination" of a call.

34. The *Caller ID Act NPRM* sought comment on whether there are other things that should be included in the definition, specifically, information transmitted in the SS7 Jurisdiction Information

[79] 47 C.F.R. § 64.1600(b).

[80] *See Caller ID Act NPRM*, 26 FCC Rcd at 4136, para. 18. Although ANI's original purpose was to enable carriers to bill customers for calls, carriers now offer ANI services to their business customers who use ANI services for a wide range of purposes including improving customer service provided on inbound calls by pulling up customer-specific information based on identification of the billing number.

[81] *See, e.g.*, AT&T Comments at 5–6 (suggesting that we amend our definitions of CPN, ANI, and charge number to include telephone number and billing information transmitted by IP-enabled voice service providers via any signaling technology because the proposed definitions could limit the Caller ID subject to anti-spoofing regulations).

[82] In considering whether a person or entity has altered or manipulated pseudo-ANI we will look to the definition of pseudo-ANI in section 20.3 of our rules. *See* 47 C.F.R. § 20.3.

[83] *See, e.g.*, NENA Comments at 2.

[84] *See* Senate Commerce Committee Report at 2.

[85] *See* NENA Comments at 2–3.

[86] *See* Texas 911 Agencies Comments at 1–2.

[87] *See* NENA Comments at 3.

Parameter (JIP) code that provides information about the location of a caller who has ported his number or is calling over a mobile service. As the record demonstrates, use of the JIP code can benefit law enforcement and public safety, and can be used for improved routing for emergencies.[88] Therefore, we clarify that "location information" includes information transmitted in the SS7 JIP code. However, in encompassing information transmitted in the JIP code within our definition, we do not require that any providers, including CMRS and VoIP providers, populate the JIP in signaling data.[89]

D. Caller ID Blocking

35. The Truth in Caller ID Act specifies that it is not intended to be construed to prevent or restrict any person from blocking the transmission of caller identification information.[90] The legislative history shows that Congress intended to protect and preserve subscribers' ability to block the transmission of their own caller identification information to called parties.[91] Consequently, like the proposed rules, the rules we adopt today provide that a person or entity that blocks or seeks to block a caller identification service from transmitting or displaying that person or entity's own caller identification information shall not be liable for violating our rules implementing the Truth in Caller ID Act.

36. Although our rules generally allow callers to block caller ID, as discussed in the *Caller ID Act NPRM*, telemarketers are required to transmit caller identification information, and the phone number they transmit must be one that a person can call to request placement on a company-specific do-not-call list.[92] This requirement allows consumers to more easily identify incoming telemarketing calls and to make informed decisions about whether to answer particular calls. It also facilitates consumers' ability to request placement on company-specific do-not-call lists. Additionally, the requirement assists law enforcement investigations into telemarketing complaints.[93] Therefore, our rules specify that they "do not relieve any person or entity that engages in telemarketing, as defined in section 64.1200(f)(10), of the obligation to transmit caller identification information under section 64.1601(e)."

E. Third-Party Spoofing Services

37. As discussed above, one of the reasons that it is easy for anyone to spoof their caller ID is that third-party caller ID spoofing services are widely available and inexpensive.[94] There are typically four steps to the process of using a third-party caller ID spoofing service to spoof a call, as illustrated in Figure 1. First, the customer places a call to a company-controlled toll free or POTS line number. Second, after the first call is connected, the customer enters a personal identification number and then enters the number he or she wants to substitute as the caller ID that is transmitted to the called party. Third, the customer enters the phone number he or she wants to call; and fourth, the spoofing provider—or the

[88] *See* NECA *et al.* Comments at 9 n.25; *see also* NENA Comments at 2 (urging the Commission to include JIP within the definition of Caller Identification Information).

[89] *See* ATIS Comments at 5 (urging the Commission not to explicitly reference JIP in its rules because it is not populated by all carriers, nor is it technically feasible for it to be populated in all situations).

[90] *See* 47 U.S.C. § 227(e)(2).

[91] *See* Senate Commerce Committee Report at 3 ("FCC regulations currently provide callers with the right to block the capability of any caller identification service to transmit caller identification information. This bill makes clear that it would not prevent or restrict persons from blocking services this way.").

[92] *Caller ID Act NPRM*, 26 FCC Rcd at 4138, para. 26; *see also* 47 C.F.R. § 1601(e).

[93] *See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 18 FCC Rcd 14014, para. 179 (2003).

[94] *See supra* para. 8.

carrier it uses—delivers the call to the terminating carrier serving the called number with the requested substitute number transmitted as the caller's CPN.[95]

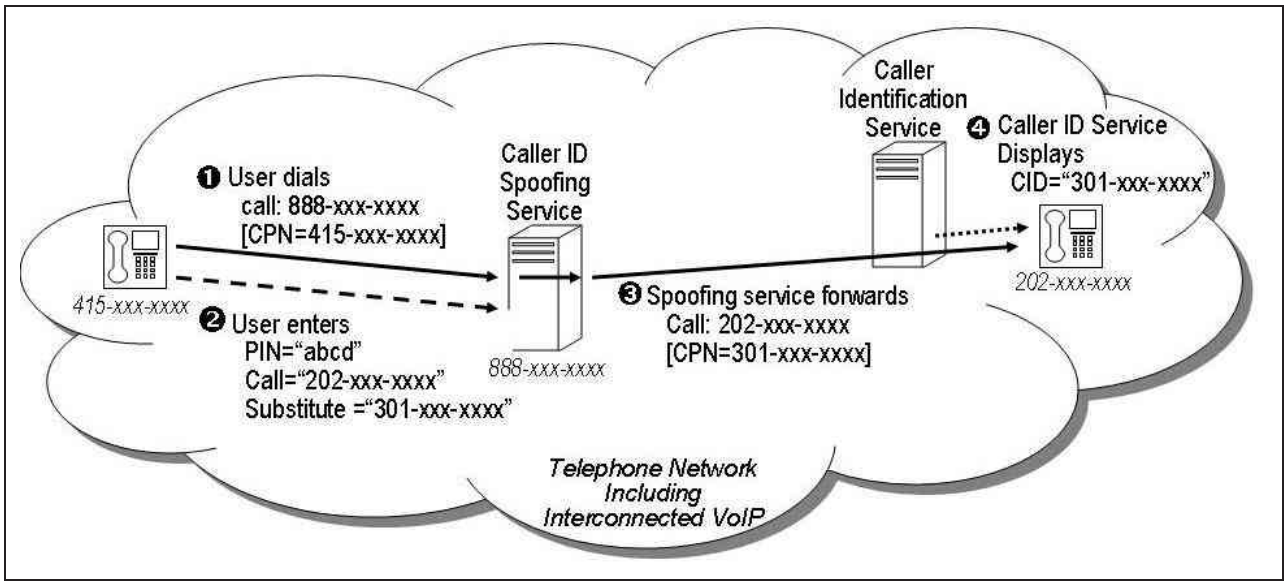

Figure 1. Operation of Third-Party Spoofing Service

38. Recognizing the role spoofing providers play in facilitating caller ID spoofing, the Commission sought comment on whether the Commission may, and should, adopt rules imposing obligations on providers of caller ID spoofing services when they are not themselves acting with intent to defraud, cause harm, or wrongfully obtain anything of value. More specifically, the Commission also sought comment on whether it should impose record-keeping requirements on caller ID spoofing providers. In addition, the Commission sought comment on a proposal made by DOJ, and supported by the Minnesota Attorney General, to adopt rules requiring "public providers of caller ID spoofing services to make a good-faith effort to verify that a user has the authority to use the substituted number, such as by placing a one-time verification call to that number."[96]

39. Although Itellas and Teltech, the two third-party caller ID spoofing services that commented on the *Caller ID Act NPRM*, indicate that they do maintain records of the calls they facilitate and that they cooperate with law enforcement investigations, there is little support among the commenters for the adoption of rules requiring third-party spoofing providers to maintain records.[97] The third-party spoofing providers strongly object to any rule requiring them to verify that their customers have a right to use the phone number they choose to spoof.[98] Itellas and TelTech both argue that requiring users of caller ID services to verify that they have authority to use the spoofed number would be pointless and ineffective, because people or entities using caller ID spoofing to carry out a criminal enterprise can purchase the software to spoof caller ID rather than use a third-party provider.[99] They also argue that verification

[95] *See* Itellas Comments at 2; TelTech Comments at 5–6.

[96] DOJ Jan. 26, 2011 Letter at 4; Minnesota AG Comments at 3.

[97] *See* Itellas Comments at 4–5; TelTech Comments at 8–9. However, TelTech points out that it does not have any customer information about the people who buy prepaid cards to use its services. TelTech Comments at 9.

[98] *See* Itellas Comments at 5–6; TelTech Comments at 9–10.

[99] *See* TelTech Comments at 10 (also arguing that verification would be expensive); Itellas Comments at 6.

cannot establish a caller's intent, and absent malintent there can be no violation of the Truth in Caller ID Act.[100] As TelTech explains, "[u]sing a number you do not have permission to spoof is not illegal under the Act."[101] In its reply comments, NNEDV agrees that verification requirements would be inconsistent with the intent expressed in the legislative history of the Act, which recognized the importance of caller ID spoofing to protect victims of domestic violence.[102] According to NNEDV, a verification requirement "would endanger victims and 'domestic violence shelters that provide false caller ID number (sic) to prevent call recipients from discovering the location of victims.'"[103] Although NNEDV objects to DOJ's proposal that the Commission impose verification requirements on caller ID spoofing services, it does propose that the Commission require spoofing services to give prominent notice that use of their services in violation of the Truth in Caller ID Act is unlawful.[104]

40. We are very concerned about the harmful effects of caller ID spoofing done with malicious intent. We also recognize that requiring caller ID spoofing services to verify that users have the authority to use the substitute number would likely reduce the use of caller ID spoofing to further criminal schemes, and could simplify law enforcement efforts to determine who is behind a caller ID spoofing scheme.[105] Likewise, the public would benefit from having third-party caller ID spoofing providers clearly and conspicuously notify their users about the practices prohibited by the Truth in Caller ID Act. However, we are not convinced that it is appropriate for the Commission to impose such obligations on third-party caller ID spoofing service providers at this time. In crafting the Truth in Caller ID Act, we believe that Congress intended to balance carefully the drawbacks of malicious caller ID spoofing against the benefits provided by legitimate caller ID spoofing.[106] The Act prohibits spoofing providers, like all other persons and entities in the United States, from knowingly spoofing caller ID with malicious intent. However, the Act does not expressly impose additional obligations on providers of caller ID spoofing services. Following Congress' lead, we decline to impose additional obligations on third-party spoofing providers at this time.

41. We are cognizant of the fact that spoofing providers can, and sometimes do, detect and prevent some types of illegitimate manipulation of caller ID spoofing. Itellas, for example, noted in its comments that its system does not allow customers to call or display 911, in order to prevent use of its service for swatting.[107] Itellas' system also prevents its customers from using a specific spoofed number when placing calls to toll free numbers in order to prevent users from using the phone number associated with a stolen credit card or with a specific bank account to activate the credit card, or to transfer money from the compromised bank account.[108] In its comments, TelTech represents that it has closed accounts that it has

[100] *See* TelTech Comments at 10.

[101] *Id*.

[102] NNEDV Reply at 3.

[103] *Id.* To make it possible for legitimate caller ID spoofing even where a verification requirement is in place, DOJ suggested that spoofing providers could maintain a pool of alternate numbers controlled by the spoofing provider. *See* DOJ Reply at 5–6. NNEDV argued that such an arrangement would allow call recipients to identify and reject such calls as spoofed. According to NNEDV, that would be a particular problem for domestic violence victims living in shelters who are required by a court order to call an abuser to discuss child custody issues. NNEDV Reply at 4.

[104] NNEDV Comments at i, 14–15; *see also* PRC Reply at 6.

[105] As noted, it is possible to spoof caller identification information without using a third-party provider, so requiring third-party providers to make a good faith attempt to verify that their customers have authority to use the substitute number they are seeking to use will not stop sophisticated criminals from using caller ID spoofing.

[106] Google Reply at 2.

[107] *See* Itellas Comments at 7.

[108] *See id.*

identified as appearing to be used to commit crimes, including money transfer fraud, activation of stolen credit cards, or identity theft.[109] However, spoofing services do not necessarily know the intent with which their customers place spoofed calls.[110] Once the Commission's rules are in force, we will have the opportunity to determine whether the current rules are sufficient to deter malicious caller ID spoofing. If they are not, we can revisit the issue. In the meantime, we raise the issue of liability for third-party providers in the report the Act requires the Commission to submit to Congress.

42. We want to make clear that our decision not to impose additional obligations on third-party caller ID spoofers in no way immunizes them from the obligation to comply with the Act. Where a caller ID spoofing service causes, directly or indirectly, the transmission or display of false or misleading caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value, such service will be in violation of the Truth in Caller ID Act and our rules. Our conclusion follows from a natural reading of the statute, which applies to any "person" who causes caller ID services to transmit misleading or inaccurate caller ID information. Likewise, although we do not decide the matter here, liability questions would arise if the totality of the circumstances demonstrated that a third-party spoofing provider had promoted its services to others as a means to defraud, cause harm, or wrongfully obtain anything of value.

43. *Caller ID Unmasking.* As mentioned in the *Caller ID Act NPRM*, some entities—often the same ones that offer spoofing services—also offer the ability to unmask a blocked number, effectively stripping out the privacy indicator chosen by the calling party.[111] We remain deeply concerned about these unmasking services, which circumvent the privacy protections afforded by the Commission's CPN rules. The record reflects concern regarding these services as well.[112] However, the record is not sufficiently robust to support amendments to our rules at this time. The Commission will consider whether to take further rulemaking action to address these services in the future. In the meantime, we take this opportunity to remind carriers of their obligations to honor callers' privacy requests.

F. Amendments to the Commission's Enforcement Rules

44. The Act provides for additional forfeiture penalties for violations of subsection 227(e) of the Communications Act, and new procedures for imposing and recovering such penalties.[113] In order to fully implement the Truth in Caller ID Act, the Commission proposed amendments to its forfeiture rule, 47 C.F.R. § 1.80. The proposed amendments specified the forfeiture penalties the Commission proposed to assess for violations of the Truth in Caller ID Act, and proposed procedures for imposing penalties and recovering such penalties. The Commission also proposed some minor revisions to our forfeiture rules to address issues not directly related to the Truth in Caller ID Act. For the reasons discussed below, we now adopt the proposed amendments to our forfeiture rules, with some minor modifications.

45. *Amount of Penalties*. The Act specifies that the penalty for a violation of the Act "shall not exceed $10,000 for each violation, or 3 times that amount for each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $1,000,000 for any single act or failure to act."[114] These forfeitures are in addition to penalties provided for elsewhere in the

[109] TelTech Comments at 13.

[110] *See* TelTech Reply at 3–4.

[111] *See, e.g.*, www.trapcall.com.

[112] *See, e.g.*, NNEDV Comments at 17–23; PRC Reply at 7; *but cf.* TelTech Comments at 19–20 (arguing that "[t]he proposed rules should not address consumer-focused caller ID unmasking services").

[113] 47 U.S.C. § 227(e)(5).

[114] 47 U.S.C. § 227(e)(5)(i).

Communications Act.[115] Therefore, to implement these provisions of the Truth in Caller ID Act, we adopt the Commission's proposal to amend section 1.80(b) of our rules to include a provision specifying the maximum amount of additional fines that can be assessed for violations of the Truth in Caller ID Act. In the interest of consistency and clarity, we also amend the text and chart in Section III of what is now the "Note to Paragraph (b)(5)" to include information about the maximum additional forfeitures provided for by the Truth in Caller ID Act.

46. The Truth in Caller ID Act establishes the maximum amount of additional forfeiture penalties the Commission can assess for a violation of the Act, but it does not specify how the Commission should determine the forfeiture amount in any particular situation. In order to provide guidance about the factors the Commission will use in determining the amount of penalty it will assess for violations of the Truth in Caller ID Act, we adopt the Commission's proposal to employ the balancing factors the Commission typically considers when determining the amount of a forfeiture penalty. Those factors are set out in section 503(b)(2)(E) of the Communications Act and section 1.80(b)(4) of the Commission's rules. The balancing factors include "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."[116] These factors allow the Commission to properly consider the specific facts of each case when determining an appropriate forfeiture penalty.

47. *Procedure for Determining Penalties.* With respect to the procedure for determining or imposing a penalty, the Act provides that "[a]ny person that is determined by the Commission, in accordance with paragraphs (3) and (4) of section 503(b) [of the Communications Act], to have violated this subsection shall be liable to the United States for a forfeiture penalty."[117] It also states that "[n]o forfeiture penalty shall be determined under clause (i) against any person unless such person receives the notice required by section 503(b)(3) or section 503(b)(4) [of the Communications Act]."[118] As the Commission indicated in the *Caller ID Act NPRM*, taken together, sections 503(b)(3) and 503(b)(4) allow the Commission to impose a forfeiture penalty against a person through either a hearing or a written notice of apparent liability (NAL), subject to certain procedures. The Truth in Caller ID Act makes no reference to section 503(b)(5) of the Communications Act, which states that the Commission may not assess a forfeiture under any provision of section 503(b) against any person, who: (i) "does not hold a license, permit, certificate, or other authorization issued by the Commission"; (ii) "is not an applicant for a license, permit, certificate, or other authorization issued by the Commission"; or (iii) is not "engaging in activities for which a license, permit, certificate, or other authorization is required," unless the Commission first issues a citation to such person in accordance with certain procedures.[119] As the Commission explained in the *Caller ID Act NPRM*, that omission suggests that Congress intended to give the Commission the authority to proceed expeditiously to stop and, where appropriate, assess a forfeiture penalty against, any person or entity engaged in prohibited caller ID spoofing without first issuing a citation.[120] Having received no comments disagreeing with the Commission's proposed approach, we find that it is appropriate and consistent with Congressional intent to adopt rules that allow the Commission to determine or impose a forfeiture penalty for a violation of section 227(e) against "any

[115] *Id.*

[116] *See* 47 U.S.C. § 503(b)(2)(E).

[117] *See* 47 U.S.C. § 227(e)(5)(i). By "subsection," the Act is referring to subsection (e) of 47 U.S.C. § 227.

[118] *Id.* § 227(e)(5)(iii).

[119] *See* 47 U.S.C. § 503(b)(5).

[120] *See generally* Senate Commerce Committee Report at 1–3. The Senate Commerce Committee Report discusses the harm caused by caller ID spoofing engaged in by individuals and specifies that, if passed, the Act would authorize civil penalties of up to $10,000 for each violation or up to three times that amount for each day of a continuing violation, up to a total of $1 million.

person," regardless of whether that person holds a license, permit, certificate, or other authorization issued by the Commission; is an applicant for any of the identified instrumentalities; or is engaged in activities for which one of the instrumentalities is required.

48. We also adopt rules that amend section 1.80(a) of our rules to add a new subsection (4) providing that forfeiture penalties may be assessed against any person found to have "violated any provision of section 227(e) of the Communications Act or of the rules issued by the Commission under section 227(e) of that Act."[121] In contrast to section 503(b)(1)(B) of the Communications Act, which provides for a forfeiture penalty against anyone who has "willfully or repeatedly" failed to comply with any provisions of the Communications Act, or any regulations issued by the Commission under the Act, the Truth in Caller ID Act does not require "willful" or "repeated" violations to justify imposition of a penalty. Therefore, we adopt new section 1.80(a)(4), in accordance with Congressional direction that the Commission have authority to assess a forfeiture penalty for all violations of section 227(e) or of the rules issued by the Commission under that section of the Act.

49. *Statute of Limitations*. The Truth in Caller ID Act specifies that "[n]o forfeiture penalty shall be determined or imposed against any person under [section 227(e)(5)(i)] if the violation charged occurred more than 2 years prior to the date of issuance of the required notice or notice of apparent liability."[122] We note that this differs from the more general limitations provision of section 503(b)(6) of the Communications Act, which provides for a one-year statute of limitations in most cases. Given the explicit language of the Truth in Caller ID Act, however, we find that the longer two-year statute of limitations applies to enforcement of the Truth in Caller ID Act.

50. *Miscellaneous*. We also take this opportunity to revise the undesignated paragraph in section 1.80(a) to address issues not directly related to implementation of the Truth in Caller ID Act and to redesignate that undesignated text as "Note to paragraph 1.80(a)." First, with respect to the proposed revisions, in order to ensure that the language in the rule encompasses the language used in all of the statutory provisions, we amend the rule to specify that the forfeiture amounts set forth in section 1.80(b) are inapplicable "to conduct which is subject to a forfeiture penalty *or fine*" under the various statutory provisions listed. (Emphasis added). Second, we amend the rule to change the references to sections 362(a) and 362(b) to sections 364(a) and 364(b) respectively, in order that the statutory provision references match those used in the Communications Act, rather than the sections of the U.S. Code.[123] Third, we delete section 503(b) from the list of statutory provisions to which the forfeiture amounts in section 1.80(b) do not apply, because the inclusion was in error; section 1.80(b) implements the forfeiture amounts of section 503(b), and so the penalties set forth in section 1.80(b) apply to forfeiture under section 503(b).

IV. PROCEDURAL ISSUES

A. Paperwork Reduction Act

51. This document does not contain new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. In addition, therefore, it does not contain any new or modified information collection burdens for small business concerns with fewer than 25 employees, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44

[121] In order to find someone in violation of section 227(e) of the Communications Act, the Commission will need to find that the person engaged in caller ID spoofing with intent to "defraud, cause harm, or wrongfully obtain anything of value."

[122] 47 U.S.C. § 227(e)(5)(iv).

[123] Section 364 of the Communications Act is codified as 47 U.S.C. § 362.

U.S.C. 3506(c)(4).

B. Congressional Review Act

52. The Commission will send a copy of this Report and Order in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. § 801(a)(1)(A).

C. Final Regulatory Flexibility Certification

53. The Regulatory Flexibility Act of 1980, as amended (RFA)[124] requires that a regulatory flexibility analysis be prepared for rulemaking proceedings, unless the agency certifies that "the rule will not have a significant economic impact on a substantial number of small entities."[125] The RFA generally defines "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[126] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[127] A small business concern is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration (SBA).[128]

54. In this Report and Order, the Commission adopts rules implementing the Truth in Caller ID Act. The Truth in Caller ID Act and the implementing rules we adopt today prohibit any person or entity in the United States from knowingly altering or manipulating caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value. The *Caller ID Act NPRM* sought comment on benefits and burdens that would be imposed on small entities by the proposed rules and sought comment on an initial regulatory flexibility analysis (IRFA).[129] No commenters sought to argue that the proposed rules would have a significant impact on a substantial number of small entities. Indeed, no commenters raised any concerns about the impact of the proposed rules on small entities, as such.

55. The NPRM also sought comment on whether the Commission may, and should, adopt rules imposing obligations on providers of caller ID spoofing services when they are not themselves acting with intent to defraud, cause harm, or wrongfully obtain anything of value.[130] It also sought comment more specifically on whether the Commission should impose record-keeping requirements on caller ID spoofing providers, as well as on a proposal made by DOJ and supported by the Minnesota Attorney General to adopt rules requiring "public providers of caller ID spoofing services to make a good-faith effort to verify that a user has the authority to use the substituted number, such as by placing a one-time verification call to that number. In this Order, we decline to impose any additional obligations on

[124] The RFA, see 5 U.S.C. § 601 *et seq*., has been amended by the Contract With America Advancement Act of 1996, Pub. L. No. 104-121, 110 Stat. 847 (1996) (CWAAA). Title II of the CWAAA is the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA).

[125] 5 U.S.C. § 605(b).

[126] 5 U.S.C. § 601(6).

[127] 5 U.S.C. § 601(3) (incorporating by reference the definition of "small business concern" in Small Business Act, 5 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[128] Small Business Act, 5 U.S.C. § 632.

[129] *Caller ID Act NPRM*, 26 FCC Rcd at 4139, para. 28; *id.* at 4148, Appendix B.

[130] *Id.* at 4137, para. 21.

providers of caller ID spoofing services at this time.[131] Therefore, to the extent that such requirements would have had an economic impact on some small entities, that impact will not occur. Indeed, the record contains nothing showing that the cost of compliance obligations would be economically significant or would affect a substantial number of small entities. Indeed, based on the record before us, we are persuaded that a substantial number of small businesses do not engage in caller ID spoofing with the intent to defraud, cause harm, or wrongfully obtain anything of value, and those that do are already prohibited from doing so by the Truth in Caller ID Act. Therefore, we certify that the requirements of this Report and Order will not have a significant economic impact on a substantial number of small entities. The Commission will send a copy of the Report and Order including a copy of this final certification, in a report to Congress pursuant to the Small Business Regulatory Enforcement Fairness Act of 1996, *see* 5 U.S.C. § 801(a)(1)(A). In addition, the Report and Order and this certification will be sent to the Chief Counsel for Advocacy of the Small Business Administration, and will be published in the Federal Register. *See* 5 U.S.C. § 605(b).

D. Accessible Formats

56. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer and Governmental Affairs Bureau at (202) 418-0531 (voice), (202) 418-7365 (TTY).

V. ORDERING CLAUSES

57. Accordingly, IT IS ORDERED that, pursuant to section 2 of the Truth in Caller ID Act of 2009, Pub. L. No. 11-331, and Sections 1, 4(i), 4(j), 227, and 303(r) of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154(i), 154(j), 227 and 303 (r), this Report and Order, with all attachments, IS ADOPTED.

58. IT IS FURTHER ORDERED that Parts 1 and 64 of the Commission's rules are amended as set forth in Appendix A.

59. IT IS FURTHER ORDERED that pursuant to sections 1.4(b)(1) and 1.103(a) of the Commission's rules, 47 C.F.R. §§ 1.4(b)(1), 1.103(a), this Report and Order SHALL BE EFFECTIVE 30 days after publication of a summary in the Federal Register.

60. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Report and Order, including the Final Regulatory Flexibility Certification, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[131] *See supra* paras. 38–42.

Appendix A

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR parts 1 and 64 as follows:

PART I – PRACTICE AND PROCEDURE

1. The authority citation for part 1, of Title 47 of the Code of Federal Regulation is revised to read as follows:

Authority: 15 U.S.C. 79 *et seq.*; 47 U.S.C. 151, 154(i), 154(j), 155, 157, 225, 227, 303(r), and 309.

2. Amend section 1.80 as follows:

a. Designate the undesignated paragraph following (a)(4) as "Note to Paragraph (a)" and revise it;

b. Redesignate paragraphs (a)(4), (b)(3), (b)(4), (b)(5), and (c)(3), as paragraphs (a)(5), (b)(4), (b)(5), (b)(6), and (c)(4), respectively;

c. Redesignate "Note to Paragraph (b)(4)" as "Note to paragraph (b)(5)" and revise it;

d. Add new paragraphs (a)(4), (b)(3), and (c)(3);

e Revise redesignated paragraph (b)(4); and

f. Revise paragraph (d).

§ 1.80 Forfeiture proceedings.

(a) * * *

(3) Violated any provision of section 317(c) or 508(a) of the Communications Act;

(4) Violated any provision of section 227(e) of the Communications Act or of the rules issued by the Commission under section 227(e) of that Act; or

(5) * * *

Note to paragraph (a):

A forfeiture penalty assessed under this section is in addition to any other penalty provided for by the Communications Act, except that the penalties provided for in paragraphs (b)(1), (b)(2), (b)(3), and (b)(4) of this section shall not apply to conduct which is subject to a forfeiture penalty or fine under sections 202(c), 203(e), 205(b), 214(d), 219(b), 220(d), 223(b), 364(a), 364(b), 386(a), 386(b), 506, and 634 of the Communications Act. The remaining provisions of this section are applicable to such conduct.

(b) * * *

(3) Any person determined to have violated section 227(e) of the Communications Act or the rules issued by the Commission under section 227(e) of the Communications Act shall be liable to the United States for a forfeiture penalty of not more than $10,000 for each violation or three times that amount for each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $1,000,000 for any single act or failure to act. Such penalty shall be in addition to any other forfeiture penalty provided for by the Communications Act.

(4) In any case not covered by paragraphs (b)(1), (b)(2) or (b)(3) of this section, the amount of any forfeiture penalty determined under this section shall not exceed $16,000 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $112,500 for any single act or failure to act described in paragraph (a) of this section.

(5) * * *

Note to paragraph (b)(5):

Guidelines for Assessing Forfeitures

The Commission and its staff may use these guidelines in particular cases. The Commission and its staff retain the discretion to issue a higher or lower forfeiture than provided in the guidelines, to issue no forfeiture at all, or to apply alternative or additional sanctions as permitted by the statute. The forfeiture ceiling per violation or per day for a continuing violation stated in section 503 of the Communications Act and the Commission's rules are described in §1.80(b)(5)(iii). These statutory maxima became effective September 2, 2008. Forfeitures issued under other sections of the Act are dealt with separately in section III of this note.

Section I. Base Amounts for Section 503 Forfeitures

Forfeitures	Violation Amount
Misrepresentation/lack of candor	([1])
Construction and/or operation without an instrument of authorization for the service	$10,000
Failure to comply with prescribed lighting and/or marking	10,000
Violation of public file rules	10,000
Violation of political rules: reasonable access, lowest unit charge, equal opportunity, and discrimination	9,000
Unauthorized substantial transfer of control	8,000
Violation of children's television commercialization or programming requirements	8,000
Violations of rules relating to distress and safety frequencies	8,000
False distress communications	8,000
EAS equipment not installed or operational	8,000
Alien ownership violation	8,000
Failure to permit inspection	7,000

Transmission of indecent/obscene materials	7,000
Interference	7,000
Importation or marketing of unauthorized equipment	7,000
Exceeding of authorized antenna height	5,000
Fraud by wire, radio or television	5,000
Unauthorized discontinuance of service	5,000
Use of unauthorized equipment	5,000
Exceeding power limits	4,000
Failure to respond to Commission communications	4,000
Violation of sponsorship ID requirements	4,000
Unauthorized emissions	4,000
Using unauthorized frequency	4,000
Failure to engage in required frequency coordination	4,000
Construction or operation at unauthorized location	4,000
Violation of requirements pertaining to broadcasting of lotteries or contests	4,000
Violation of transmitter control and metering requirements	3,000
Failure to file required forms or information	3,000
Failure to make required measurements or conduct required monitoring	2,000
Failure to provide station ID	1,000
Unauthorized pro forma transfer of control	1,000
Failure to maintain required records	1,000

[1]Statutory Maximum for each Service.

Violations Unique to the Service

Violation	Services affected	Amount
Unauthorized conversion of long distance telephone service	Common Carrier	$40,000
Violation of operator services requirements	Common Carrier	7,000
Violation of pay-per-call requirements	Common Carrier	7,000
Failure to implement rate reduction or refund order	Cable	7,500
Violation of cable program access rules	Cable	7,500
Violation of cable leased access rules	Cable	7,500
Violation of cable cross-ownership rules	Cable	7,500
Violation of cable broadcast carriage rules	Cable	7,500

Violation of pole attachment rules	Cable	7,500
Failure to maintain directional pattern within prescribed parameters	Broadcast	7,000
Violation of main studio rule	Broadcast	7,000
Violation of broadcast hoax rule	Broadcast	7,000
AM tower fencing	Broadcast	7,000
Broadcasting telephone conversations without authorization	Broadcast	4,000
Violation of enhanced underwriting requirements	Broadcast	2,000

Section II. Adjustment Criteria for Section 503 Forfeitures

Upward Adjustment Criteria

(1) Egregious misconduct.

(2) Ability to pay/relative disincentive.

(3) Intentional violation.

(4) Substantial harm.

(5) Prior violations of any FCC requirements.

(6) Substantial economic gain.

(7) Repeated or continuous violation.

Downward Adjustment Criteria

(1) Minor violation.

(2) Good faith or voluntary disclosure.

(3) History of overall compliance.

(4) Inability to pay.

Section III. Non-Section 503 Forfeitures That Are Affected by the Downward Adjustment Factors

Unlike section 503 of the Act, which establishes maximum forfeiture amounts, other sections of the Act, with two exceptions, state prescribed amounts of forfeitures for violations of the relevant section. These amounts are then subject to mitigation or remission under section 504 of the Act. One exception is section 223 of the Act, which provides a maximum forfeiture per day. For convenience, the Commission will treat this amount as if it were a prescribed base amount, subject to downward adjustments. The other exception is section 227(e) of the Act, which provides maximum forfeitures per violation, and for continuing violations. The Commission will apply the factors set forth in section 503(b)(2)(E) of the Act and section III of this note to determine the amount of the penalty to assess in any particular situation. The following amounts are adjusted for inflation pursuant to the Debt Collection Improvement Act of 1996 (DCIA), 28 U.S.C. 2461. These non-section 503 forfeitures may be adjusted downward using the "Downward Adjustment Criteria" shown for section 503 forfeitures in section II of this note.

Violation	Statutory amount ($)

Sec. 202(c) Common Carrier Discrimination	9,600, 530/day.
Sec. 203(e) Common Carrier Tariffs	9,600, 530/day.
Sec. 205(b) Common Carrier Prescriptions	18,200.
Sec. 214(d) Common Carrier Line Extensions	1,320/day.
Sec. 219(b) Common Carrier Reports	1,320.
Sec. 220(d) Common Carrier Records & Accounts	9,600/day.
Sec. 223(b) Dial-a-Porn	75,000/day.
Sec. 227(e)	$10,000/violation $30,000/day for each day of continuing violation, up to $1 million for any single act or failure to act
Sec. 364(a) Forfeitures (Ships)	7,500 (owner).
Sec. 364(b) Forfeitures (Ships)	1,100 (vessel master).
Sec. 386(a) Forfeitures (Ships)	7,500/day (owner).
Sec. 386(b) Forfeitures (Ships)	1,100 (vessel master).
Sec. 634 Cable EEO	650/day.

* * * * *

(c) * * *

(3) In the case of a forfeiture imposed under section 227(e), no forfeiture will be imposed if the violation occurred more than 2 years prior to the date on which the appropriate notice is issued.

(4) * * *

(d) *Preliminary procedure in some cases; citations*. Except for a forfeiture imposed under subsection 227(e)(5) of the Act, no forfeiture penalty shall be imposed upon any person under this section of the Act if such person does not hold a license, permit, certificate, or other authorization issued by the Commission, and if such person is not an applicant for a license, permit, certificate, or other authorization issued by the Commission, unless, prior to the issuance of the appropriate notice, such person:

(1) Is sent a citation reciting the violation charged;

(2) Is given a reasonable opportunity (usually 30 days) to request a personal interview with a Commission official, at the field office which is nearest to such person's place of residence; and

(3) Subsequently engages in conduct of the type described in the citation.

However, a forfeiture penalty may be imposed, if such person is engaged in (and the violation relates to) activities for which a license, permit, certificate, or other authorization is required or if such person is a cable television operator, or in the case of violations of section 303(q), if the person involved is a nonlicensee tower owner who has previously received notice of the obligations imposed by section 303(q) from the Commission or the permittee or licensee who uses that tower. Paragraph (c) of this section does not limit the issuance of citations. When the requirements of this paragraph have been satisfied with respect to a particular violation by a particular person, a forfeiture penalty may be imposed upon such person for conduct of the type described in the citation without issuance of an additional citation.

* * * * *

PART 64 – MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

3. The authority citation for Part 64 is revised to read as follows:

Authority: 47 U.S.C. 154, 254(k), 227; secs. 403(b)(2)(B), (c), Pub. L. 104-104, 100 Stat. 56. Interpret or apply 47 U.S.C. 201, 218, 222, 225, 226, 207, 228, and 254(k) unless otherwise noted.

4. Section 64.1600 is amended by redesignating paragraphs (c), (d), (e) and (f) as paragraphs (e), (f), (i) and (j) respectively and by adding new paragraphs (c), (d), (g), and (h) to read as follows:

§ 64.1600 Definitions

* * * * *

(c) *Caller identification information.* The term "caller identification information" means information provided by a caller identification service regarding the telephone number of, or other information regarding the origination of, a call made using a telecommunications service or interconnected VoIP service.

(d) *Caller identification service.* The term "caller identification service" means any service or device designed to provide the user of the service or device with the telephone number of, or other information regarding the origination of, a call made using a telecommunications service or interconnected VoIP service.

* * * * *

(g) *Information regarding the origination.* The term "information regarding the origination" means any:

(1) Telephone number;
(2) Portion of a telephone number, such as an area code;
(3) Name;
(4) Location information;
(5) Billing number information, including charge number, ANI, or pseudo-ANI; or
(6) Other information regarding the source or apparent source of a telephone call.

(h) *Interconnected VoIP service*. The term "interconnected VoIP service" has the same meaning given the term "interconnected VoIP service" in 47 CFR § 9.3 as it currently exists or may hereafter be amended.

* * * * *

5. Section 64.1604 is redesignated as section 64.1605, and a new section 64.1604 is added to read as follows:

§ 64.1604 Prohibition on transmission of inaccurate or misleading caller identification information.

(a) No person or entity in the United States shall, with the 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.

(b) *Exemptions*. Paragraph (a) of this section shall not apply to:

(1) Lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States; or

(2) Activity engaged in pursuant to a court order that specifically authorizes the use of caller identification manipulation.

(c) A person or entity that blocks or seeks to block a caller identification service from transmitting or displaying that person or entity's own caller identification information pursuant to § 64.1601(b) of this section shall not be liable for violating the prohibition in paragraph (a) of this section. This subsection does not relieve any person or entity that engages in telemarketing, as defined in § 64.1200(f)(10), of the obligation to transmit caller identification information under § 64.1601(e).

APPENDIX B

List of Comments

Commenter	Abbreviation
Alliance for Telecommunications Industry Solutions	ATIS
American Teleservices Association	ATA
AT&T, Inc.	AT&T
Copilevitz and Canter, LLC	Copilevitz
Horowitz, Nicholas A.	Horowitz
InCharge Systems, Inc.	InCharge
inContact, Inc.	inContact
Inter-Agency Investigations	Inter-Agency
Itellas, LLC	Itellas
John Q. Public	John Q. Public
JSM Tele-Page, Inc.	JSM
Lee, Mark R.	Lee
Minnesota Attorney General	Minnesota AG
National Emergency Number Association	NENA
National Exchange Carriers Association, National Telecommunications Cooperative Association, Organization for the Promotion and Advancement of Small Telecommunications Companies, Western Telecommunications Alliance, and Eastern Rural Telecom Association	NECA et al.
National Emergency Number Association	NENA
National Network to End Domestic Violence	NNEDV
NobelBiz, Inc.	NobelBiz
Open Identity Exchange	OIX
Silverblatt, Alan N.	Silverblatt
Student Loan Servicing Alliance and Student Loan Servicing Alliance Private Loan Committee	SLSA
Telineage	Telineage
TelTech Systems, Inc.	TelTech
Texas Commission on State Emergency Communications and the Texas 9-1-1 Alliance	Texas 911 Agencies
Transaction Network Services, Inc.	TNS
United States Telecom Association	USTelecom
United States Department of Justice	DOJ
Voice on the Net Coalition	VON

List of Reply Comments

Commenter	Abbreviations
Stewart Abramson	Abramson
Google Inc.	Google
National Cable & Telecommunications Association	NCTA
National Exchange Carriers Association, National Telecommunications Cooperative Association,	NECA et al.

Organization for the Promotion and Advancement of Small Telecommunications Companies, Western Telecommunications Alliance, and Eastern Rural Telecom Association	
National Network to End Domestic Violence	NNEDV
National Telecommunications Cooperative Association	NTCA
NobelBiz, Inc.	NobelBiz
Privacy Rights Clearinghouse	PRC
SoundBite Communications, Inc.	SoundBite
TelTech Systems, Inc.	TelTech
United States Department of Justice	DOJ
Verizon and Verizon Wireless	Verizon