

M

SECRET FILE COPY
ORIGINAL
FCC MAIL SECTION
Dec 3 9 50 AM '93
DISPATCHED BY

Before the
FEDERAL COMMUNICATIONS COMMISSION FCC 93-496
Washington, D.C. 20554

In the Matter of)
Policies and Rules) CC Docket No. 93-292 ✓
concerning Toll Fraud)

NOTICE OF PROPOSED RULEMAKING

Adopted: November 10, 1993 Released: December 2, 1993

Comment Date: January 14, 1994
Reply Date: February 10, 1994

By the Commission: Commissioner Barrett issuing a statement.

TABLE OF CONTENTS

	<u>Paragraph No.</u>
I. INTRODUCTION	1
II. BACKGROUND	2
III. DISCUSSION	11
A. The En Banc Hearing	11
B. PBX Fraud	14
C. Payphone Fraud	27
D. Cellular Fraud	32
E. Line Information Database Fraud (LIDB)	35
F. Other Proposals and Request for Comment.	40
IV. CONCLUSION	42
V. PROCEDURAL MATTERS	43
VI. ORDERING CLAUSES	44

- Appendix A List of Commenters - 93-TOLL FRAUD-01
- Appendix B En Banc Hearing
- Appendix C List of Commenters - Pacific Mutual Petition
- Appendix D List of Commenters - Florida Petition
- Appendix E Proposed Rules

I. INTRODUCTION

1. This Notice of Proposed Rulemaking (NPRM) seeks comment on proposals to: (1) achieve closer coordination between the industry, consumers, vendors, law enforcement agencies, Congress, and the Commission to aid in the detection and prevention of toll fraud; (2) improve consumer education initiatives by the Commission, consumer groups, and the telecommunications industry; (3) determine that tariff liability provisions that fail to recognize an obligation by the carrier to warn customers of toll fraud risks of using carrier services are unreasonable; (4) establish a federal policy assigning liability for payphone fraud; (5) codify a requirement for written warnings for all telecommunications equipment registered under Part 68; and (6) determine measures to prevent cellular and Line Information Database (LIDB) fraud.

II. BACKGROUND

2. Until the mid 1980s, carrier networks were the main targets of telecommunications fraud. Fraud perpetrators might use electronic devices or even a child's whistle to simulate carrier switching tones that would allow them to place calls and avoid paying for them. As carriers developed new methods to prevent these primitive forms of toll fraud, however, perpetrators began to use computers to access the carriers' networks.

3. Control over the use of telecommunications services has increasingly shifted from carriers to individual consumers. Technology is providing more flexible options for use of those services. With this shift in control, however, has come a shift in the toll fraud targets. Customers, as well as carriers, are now the victims. Fraud involving customer-owned private branch exchanges (PBXs) provides an example. Customers can now use a feature in their on-premises PBX equipment to route incoming remote access calls to an outgoing line. With this capability, a company's sales representative in the field can, for example, have the convenience of placing calls that would be billed to the employer's outgoing PBX line. Fraud perpetrators have discovered that they can call into a PBX and then use computers or "finger hacking" to identify the authorization code for the remote access feature connected to the outgoing line. Once the authorization code is found or "hacked," the perpetrator can obtain a dial tone and make outgoing calls that are billed to the PBX owner. In some cases, the PBX owner may also be billed for incoming 800 calls made by the perpetrator.

4. Both customers and carriers suffer the effects of fraud; industry and Secret Service estimates of annual losses range from one to five billion dollars, in an industry in which annual billings are approximately \$175 billion. Several different types

of fraud are creating these losses: the unauthorized remote access through PBXs already described; cellular "cloning," in which billing codes for legitimate cellular subscribers are installed in a perpetrator's cellular phones; the billing of operator-assisted calls to lines with billing restrictions, such as payphone lines; and "clip-on" fraud, in which the perpetrator physically attaches a calling device directly to a phone line. Fraud perpetrators may watch consumers using calling cards at payphones and sell the calling card numbers to others, or directly approach consumers and ask them to accept billing to their phones as part of a spurious "official" investigation. Industry and law enforcement sources expect that new types of fraud will develop even as these existing types of fraud are being combatted.

5. Experience has shown that those new telecommunications technologies offering the most convenience and flexibility for users, are often also most likely to present new toll fraud opportunities. The Commission's goal has been, and will continue to be, to work with consumers and the industry to find solutions to each fraud problem without hindering the development or use of these new technologies. In devising these solutions, we must ensure that telecommunications equipment and services remain accessible.

6. The Commission is not charged with enforcing criminal statutes or prosecuting toll fraud perpetrators.¹ The Department of Justice, local law enforcement agencies, and the U.S. Secret Service are among the agencies charged with the enforcement of criminal statutes. Nevertheless, the Commission has taken several steps toward developing solutions to toll fraud. First, the Commission issued a series of "Consumer Alerts" describing the dangers posed by telecommunications fraud and steps that can be taken to detect and prevent it.² Second, on October 9, 1992, we convened an en banc hearing on Toll Fraud.³ Panelists representing telecommunications consumers, carriers, equipment vendors,

¹ The Commission's jurisdiction relates to interstate and foreign communications by wire or radio. See 47 USC 152

² "Consumer Alert - Toll Fraud," Public Notice released April 19, 1991; "Consumer Alert, Telecommunications Toll Fraud, Second in A Series," Public Notice released June 9, 1992; "Consumer Alert, Toll Fraud Risks During the Year-End Holiday Season, Third in A Series," Public Notice No. 31003, released December 17, 1992; "Consumer Alert - Toll Fraud, Fourth in a Series," released June 15, 1993; "Consumer Alert - Toll Fraud - Impersonators of Investigative Officers, Fifth in A Series," Public Notice released August 3, 1993. Consumer Alerts have been distributed to the industry, trade associations, and the press.

³ See Public Notice No. 23921, July 9, 1992.

insurance providers, and law enforcement agencies presented diverse perspectives and detailed proposals for detection, prevention, and responsibility.⁴ Following the hearing, the Commission encouraged further comment by holding the record on toll fraud open until November 16, 1992.⁵ Third, the Commission has taken action in related proceedings to address toll fraud concerns. In July, 1992, in the operator service rulemaking proceedings, the Commission required local exchange carriers to offer services, to reduce payphone providers' and other aggregators' exposure to toll fraud.⁶ Earlier, in 1990, the Commission adopted standards for direct inward dial (DID) calls which require answer supervision on DID calls routed back to the public switched network by a PBX. This amendment of Part 68 of the Commission's rules was initiated because carriers were losing tens of millions of dollars of revenue in cases where PBXs failed to return an answer supervision signal to the central office, notifying it of a billable call. The Commission continues to resolve formal and informal complaints that raise toll fraud issues.

7. The Commission also coordinates with industry, consumers, vendors, and law enforcement agencies. Commission staff attends meetings with industry groups working to formulate prospective solutions to toll fraud problems.⁷ Some fraud issues appear to have been resolved by the industry, including, for example, dial tone reorigination, which permits the calling party to receive a second dial tone after the original call is terminated. The industry also has implemented intercompany cooperation on live call tracing. Many carriers have recently responded to the widespread concerns about toll fraud by offering services designed to provide early detection and prevention of the problems.

8. It does not appear, however, that private action can resolve all toll fraud problems or that incentives to control fraud

⁴ See Appendix B.

⁵ See Public Notice, DA 92-1464, released October 22, 1992; File No. 93-TOLL FRAUD-01; Appendix A.

⁶ See Order on Reconsideration, CC Docket No. 91-35, 7 FCC Rcd 4355 (1992).

⁷ E.g., the Toll Fraud Prevention Committee, a committee formed under the auspices of the Alliance for Telecommunications Industry Solutions (ATIS), formerly the Exchange Carriers Standards Association (ECSA), in order to identify issues involving toll fraud and develop resolutions for voluntary implementation by the industry; the Communications Fraud Control Association, a non-profit national clearinghouse for toll fraud information and prevention; the United States Secret Service, Electronic Crimes Branch of the Financial Crimes Division.

are structured in the best possible way. For example, the recent Chartways formal complaint proceeding⁸ presented the issue of liability for charges associated with unauthorized calls. Chartways, the complainant, was a private branch exchange (PBX) owner. It learned from AT&T that an unusual volume of calls to Pakistan was originating at its PBX. A subsequent investigation revealed that the calls were apparently being routed through the remote access feature of the PBX. Although Chartways informed AT&T that the calls were unauthorized, AT&T maintained that Chartways was liable for the related charges under the general payment obligation of AT&T's tariffs. Chartways responded by filing a formal complaint against AT&T with the Commission. The complaint alleged that AT&T's attempt to collect the charges was unreasonable and discriminatory, thus violating sections 201(b) and 202(a) of the Communications Act.⁹ The Common Carrier Bureau denied the complaint,¹⁰ based on a largely stipulated record, and following the same analysis, we denied Chartways' application for review of the Bureau decision.¹¹ First, we found that the Bureau was correct in determining that the tariff provisions at issue were clear and definite in requiring payment for the calls, in that the tariff provisions recognized no exception to the general payment obligation for unauthorized usage.¹² Next, we affirmed the finding that Chartways had control over the disputed calls.¹³ We noted that Chartways had stipulated that it had "the capability to restrict access to and egress from its PBX" at all times. Moreover, while the record contained no evidence that AT&T was negligent in any way with regard to the unauthorized calls, it also showed that Chartways had taken no steps available to it to detect or prevent unauthorized calling through its PBX. Finally, we

⁸ Chartways Technologies, Inc. v. AT&T Communications, Memorandum Opinion and Order, FCC 93-394 (released August 19, 1993). (Chartways).

⁹ See 47 U.S.C. §§ 201(b), 202(a).

¹⁰ Chartways Technologies, Inc. v. AT&T Communications, 6 FCC Rcd 2942 (Com.Car.Bur. 1991).

¹¹ We note that on November 5, 1992, Judge Irving Hill, United States District Court, Central District of California, granted summary judgment to the plaintiff, AT&T, in AT&T v. Pacific Mutual. Specifically, Judge Hill was persuaded by the logic of the Bureau's Chartways decision and found the tariff unambiguous. File No. CV 91-6793-IH (filed 11-5-92); see also AT&T v. Jiffy Lube, United States District Court, File No. K-9-2400 (concurring with Judge Hill and finding AT&T tariff unambiguous).

¹² Chartways, FCC 93-394, paras. 11-13.

¹³ Id. at para. 16.

agreed that AT&T's practices in this case were not discriminatory when compared to its liability limits on unauthorized calling card usage because calling card liability is controlled explicitly by a specific federal statute and related regulations.¹⁴

9. In United Artists, we examined the question of liability for charges associated with unauthorized calls that were either originated or accepted at the complainant's payphones.¹⁵ The threshold issue in the case was whether United Artists was AT&T's "customer," because only a "customer" who "orders" service could be held liable for charges under the terms of AT&T's tariff.¹⁶ We determined that the customer for the operator-assisted calls at issue was the caller or billed party, not United Artists, the owner of the payphones.¹⁷ We also found that United Artists did not presubscribe its payphone lines to AT&T for direct-dialed service.¹⁸ We then looked at whether United Artists had otherwise ordered service from AT&T, stating that if United Artists "had failed to take steps to control unauthorized operator-assisted and direct-dialed calling and had, instead, installed its phones in such a way as to allow callers to charge such calls to [its] payphone lines, [United Artists] could reasonably be held to have constructively 'ordered' service from AT&T, thus establishing an inadvertent carrier-customer relationship."¹⁹ The record showed that United Artists had adopted a number of measures designed to control potentially fraudulent calling.²⁰ For example, it told the local exchange carrier, New York Telephone (NYT), that its lines were to have no primary interexchange carrier at all. It also ordered originating line and billed number screening services from NYT, which were intended to inform operator service providers such as AT&T of any billing restrictions on those lines.²¹ In addition to such preventative steps, United Artists also monitored calling from its phones and regularly reported any apparently fraudulent calling to NYT and AT&T. Based on the record, we

¹⁴ Id. at paras. 19-20.

¹⁵ United Artists Payphone Corp. v. New York Telephone Co. and American Telephone and Telegraph Co., Memorandum Opinion and Order, FCC 93-387 (released August 18, 1993).

¹⁶ United Artists, FCC 93-387, at para. 5.

¹⁷ Id. at paras. 10-11.

¹⁸ Id. at para. 12.

¹⁹ Id. at para. 13.

²⁰ Id. at para. 14.

²¹ See paragraph 27, *infra*.

concluded that United Artists did not intentionally or constructively order service from AT&T and therefore could not be held liable as a customer for the disputed charges.²²

10. Our decision to begin this rulemaking is based upon our experience with complaints and the LIDB investigation;²³ the en banc hearing testimony; public comment solicited pursuant to a petition filed by the Pacific Mutual Life Insurance Company, which, among other things, asked the Commission to establish policies and rules to allocate the costs of unauthorized calls associated with PBX fraud among carriers, customers, and equipment suppliers;²⁴ and public comment solicited pursuant to a petition filed by the Florida Public Service Commission that asked the Commission to review tariffs relating to toll fraud.²⁵ The purpose of this rulemaking is to identify additional policies we should establish or steps we should take to avoid, or reduce the risks of, toll fraud.

III. DISCUSSION

A. The En Banc Hearing

11. Comments. During the En Banc Hearing on Toll Fraud, we heard testimony from eighteen panelists representing communications customers, common carriers, equipment manufacturers, law enforcement agencies, and others. A common theme emphasized by the panelists at the session was that effective approaches now exist to battle toll fraud if customers, carriers, equipment vendors, and law enforcement agencies cooperate to detect and prevent fraud. Included among these potential solutions are equipment-based measures that end-users may take themselves, carrier-based monitoring services, insurance products, law enforcement efforts, and proactive educational programs. The hearing was divided into three panels.²⁶ The first panel focused on PBX and other customer premises equipment (CPE)-based fraud. Participants included a PBX and CPE owner, a PBX trade association representative, a law enforcement expert, an equipment manufacturer, and a long distance company offering anti-fraud services. The second panel focused on network-based fraud and liability issues. Participants included a hacker expert, a representative of the Toll Fraud Prevention

²² Id. at para. 15.

²³ See paragraph 35, infra.

²⁴ See Public Notice released March 14, 1991.

²⁵ See Public Notice released April 5, 1993.

²⁶ See Appendix B.

Committee of the Exchange Carriers Standards Association,²⁷ a payphone equipment manufacturer, and a panelist discussing network-based validation services. The third panel focused on emerging technical, law enforcement, and business solutions to domestic and international toll fraud. Panelists included a manufacturer of new anti-fraud products, a law enforcement expert on detection and prevention of fraud, a toll fraud expert from a Canadian telecommunications corporation, a panelist discussing negotiation of international fraud disputes, and representatives of interexchange carriers, and an insurance company discussing contractual and insurance protection for toll fraud.

12. The record compiled as a result of the en banc hearing emphasized that toll fraud is a crime, that it is difficult to prosecute, that it migrates from one area of telecommunications to other areas as detection and prevention methods become effective, and that additional consumer education is necessary to detect and prevent toll fraud. Witnesses pointed out that because there is no specific federal legislation regarding toll fraud, prosecutors must deal with the limited effectiveness of the existing criminal statutes.²⁸ The record also indicates that the criminal prosecution of toll fraud perpetrators is infrequent. Law enforcement representatives on the panels asserted that this may be partially due to lack of training or familiarity with toll fraud cases on the part of law enforcement agents or U.S. Attorneys. It also may be due to the high dollar thresholds (victims must allege large monetary damages) set by the U.S. Attorneys because toll fraud cases generally are manpower intensive but often result in either suspended sentences or short incarcerations. Further, to establish access device fraud under 18 U.S.C. Section 1029 the prosecution must show that a person's account has been accessed. In many toll fraud cases, particularly cellular tumbling,²⁹ no account is accessed. Rather the fraud perpetrator changes both the identification number and the telephone number in order to confuse the cellular switch. Our day-long en banc hearing demonstrated that a plan to combat toll fraud must include an integrated program of detection, prevention and prosecution. The record in the toll fraud en banc hearing also brought out comments about PBX fraud,

²⁷ The Exchange Carrier Standards Association has recently been renamed the Alliance for Telecommunications Industry Solutions.

²⁸ According to the U.S. Secret Service most federal criminal investigations of toll fraud are undertaken pursuant to the Access Device Fraud statute, 18 U.S.C. Section 1029, which was enacted to stop credit card fraud. The Secret Service estimates that as few as thirteen states have enacted statutes specifically dealing with telephone fraud crimes.

²⁹ See infra paragraph 33.

payphone fraud, cellular fraud, and other types of fraud which we describe below at paragraphs 14 through 40, infra.

13. Comment Requested. In light of the persuasive testimony presented at the hearing, we request comment on specific ways to achieve closer and continuing coordination among the institutions fighting toll fraud. We seek comment on whether the Commission can add value to existing inter-institutional efforts, and, if so, how. We ask whether the Commission should establish a new Federal Advisory Committee representing all affected interests, to recommend specific solutions. Further, we request comment on whether to join with law enforcement authorities in encouraging Congress to enact legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute perpetrators of toll fraud. We invite proposals of specific statutory language that would achieve these objectives. Additionally, we request comment on ways to broaden established Commission and industry consumer education initiatives in order to better educate consumers about toll fraud risks and remedial steps that can be taken.

B. PBX Fraud

The Pacific Mutual Proceeding

14. Petition and Comments. Pacific Mutual Life Insurance Company (Pacific Mutual) filed a petition requesting the Commission to declare ambiguous and unlawful tariff provisions under which AT&T has held petitioner liable for payment of toll fraud charges incurred because of interstate, interexchange telephone calls made through remote access to petitioner's on-premises PBX. In addition, Pacific Mutual requests the Commission to establish policies and rules to allocate the costs of remote-access toll fraud among users, carriers, and suppliers, and to promote effective anti-fraud measures.³⁰ AT&T filed an opposition to the petition, 19 parties filed comments and 16 parties, including AT&T, filed reply comments.³¹

15. All commenters who support the petition state that they have been victims of toll fraud. Two commenters state that they relied on AT&T to supply the CPE and establish protocols for that equipment.³² Perkin-Elmer Corporation (PE) states that it relied on AT&T alleged misrepresentations or failure to warn of toll

³⁰ Public Notice, DA 91-284 (March 14, 1991).

³¹ See Appendix C for a list of commenters and abbreviations used throughout this NPRM to refer to these commenters.

³² See Comments of AVNET and Mitsubishi.

fraud risks associated with use of the equipment. Several commenters, including Chartways, state that fraudulent usage had originated from company-owned, on-premises CPE.³³ Credit Card Calling Systems, Inc. stipulated that the fraud of which it was a victim involved unique features of overseas resale of AT&T 800 services connected to a PBX, enabling customers to call inward to the U.S. from overseas. In contrast, AVNET stated that it was a victim of fraud involving the use of its software defined network (SDN).

16. Those commenters supporting the petition propose that the Commission prescribe guidelines that provide incentives for the development and proper use of safeguards to prevent non-card toll fraud. Most commenters who support the petition concur that the carriers are in the best position to monitor traffic patterns and call volume.³⁴ Many commenters concur with the comments of Securities Industries Association, et. al. (SIA), which proposes that the Commission require interexchange carriers (IXCs) to offer, at cost-based rates, services designed to help users prevent, and react quickly to fraud. Most commenters agree that new technologies will increase opportunities for fraud. Commenters also believe that new technologies such as multiple node virtual networks using many PBXs and other sophisticated network terminating equipment will make the impact of fraud more serious.

17. Specifically, in its comments supporting the petition, Aeronautical Radio, Inc., (ARINC), asserts that the airlines are substantial users of telephone carriers' switched voice services and many have been victimized by remote access-based toll fraud like the fraud described by the petitioner. ARINC requests that the Commission prescribe network-based preventive measures and require carriers to inform their customers about the potential for toll fraud. ARINC asserts that policies and guidelines should accomplish the following four objectives: 1) toll fraud prevention (carriers' detection and prevention plans); 2) prompt remedial action (detect and remedy in timely manner); 3) limited customer liability (forgive charges incurred in at least the first two billing cycles in which fraud is detected); and 4) notification and disclosure (carriers warn customers of vulnerabilities).³⁵ PE alleges that unauthorized calls totalling \$250,000 occurred despite the steps PE took to prevent fraud, including installation of additional access codes and reports of anomalous billings to AT&T. Although AT&T assured PE that PE would be credited as a billing error, AT&T took two years to complete the investigation. PE

³³ See e.g., Comments of Directel, Inc.

³⁴ See e.g., Comments of Broyhill, FMC, and Panel Concepts.

³⁵ See also Comments of CCCS, Inc.

contends that a carrier should not be permitted to limit liability unless the carrier has installed the best available techniques to detect and prevent remote access toll fraud; has advised customers, both in its tariffs and through marketing, of the vulnerability of its service offering; and has responded promptly to customer billing inquiries.

18. Similarly, SIA proposes that the Commission adopt specific guidelines in order to provide incentives for the development and proper use of safeguards by all affected parties to reduce toll fraud, and to spread losses equitably. SIA also proposes that the Commission require interexchange carriers (IXCs) to offer, at cost-based rates, services designed to help large users react quickly to toll fraud because the carriers are in the best position to monitor traffic patterns and call volume. SIA asserts that these services should include trunk-based monitoring against preset parameters and customized call blocking. Losses from fraud, SIA avers, could then be allocated between IXCs and customers based upon their respective responsibility. Carriers would be responsible if they fail to inform customers quickly of suspicious traffic (within 30 minutes if parameters are exceeded) or to restrict service when asked to do so. On the other hand, customers would be responsible if they fail to obtain monitoring services or obtain them and fail to act upon carrier warnings. SIA asserts that because carriers have cracked down aggressively on card fraud, hackers have turned to CPE and non-card based fraud, and, under the present rules, IXCs have no incentive to help prevent or curtail non-card fraud.

19. In its comments, Western contends that carriers and vendors should be required to issue warnings and precautions to users and revise their tariffs to reflect their responsibility for toll fraud when customers have no direct control of detection or prevention of fraud and act responsibly with regard to their equipment. Further, Western proposes that the Commission amend Part 68 to require equipment vendors (1) to implement specific hardware and software functions to help prevent toll fraud and (2) to provide specific warnings and instructions to PBX purchasers regarding the toll fraud hazards and vulnerabilities inherent in their products. NATA argues that Section 68.110(b) of the Commission's rules requires disclosure when carriers take actions that affect the network. NATA argues that customers are entitled to adequate notice of technological changes in carrier networks because carriers have made it more likely that customers would experience fraud through their facilities and equipment. NATA submits that the carriers failed to provide adequate notice and should not now be permitted to reap the benefits of the violation and hold customers liable.

20. Many commenters oppose the petition and contend that the responsibility for unauthorized use of a PBX should be placed on the PBX owner. These parties argue the PBX owner is in the best

position to prevent fraud by programming, configuring, disabling the remote access features, or installing adequate security or monitoring procedures.³⁶ Specifically, AT&T contends that the petition should be denied because the tariffs adequately establish customer responsibility and are enforced in a nondiscriminatory manner. AT&T contends that the rules petitioner proposes would eliminate the incentive for customers to secure their telephone systems and would encourage higher PBX fraud costs. AT&T asserts that the existing tariffs clearly require payment for Long Distance Service from all customers, whether usage was authorized or unauthorized, if the service originated from the customer's number. AT&T further asserts that it enforces its tariff in a uniform manner and only in cases where the fraud resulted because of AT&T's own fault as a carrier, or where a compromise would maximize AT&T's recovery does AT&T forgive any part of the disputed amount. AT&T argues that Pacific Mutual chose to use the remote access feature of its PBX, did not restrict the locations to which the PBX will permit remotely placed calls to be completed and therefore assumed the risk arising from interaction between its chosen systems and the network. In its reply comments, AT&T reiterates that it screens calling card calls because the individual database validation that is performed before each calling card call is completed enables AT&T to engage in screening and blocking functions which cannot readily be duplicated on non-card calls, where no such database validation occurs.

21. LiTel Communications, Inc. (LiTel) urges the Commission to deny petitioner's request regarding tariff issues because long-distance companies cannot distinguish legitimate PBX calls from fraudulent ones and would face enormous financial exposure if the tariff language is adjudged unlawful. MidAmerican concurs with AT&T in opposing the petition and contends that it is not in the public interest to make all consumers indirectly liable for PBX fraud. Southwestern Bell (SWB) contends that a cap on end user liability reduces the incentive for end users to prevent fraud. SWB submits that proposed restrictions on vendors through modification of Part 68 are vague. SWB also argues the proposed rules are unsupported because petitioner has not shown that end users lack either information or options necessary to guard against toll fraud.

22. Allnet submits that the comments in the proceeding have not adequately supported the granting of the petition because it is not the role of carriers to insure end users against theft of services. The theft of services, Allnet contends, was made possible by the end user's choice of equipment, its configuration, and its operation and only the PBX owner is able to know whether an outgoing call originated over an incoming line. Allnet asserts,

³⁶ See e.g., Comments of MCI, LiTel, MidAmerican, SWB, and Ameritech at Appendix C.

however, that if IXCs are required to insure end users against theft, then IXCs should be permitted to refuse to serve high risk end users. Allnet proposes that minimum conditions should be set out in Part 68, including anti-theft features on all PBXs, real time on-line printing and monitoring of CDRs (call detail records), limiting direct inward systems access (DISA) trunks to 7 digit outpulse, purchasing account codes from IXCs, purchasing 800 call detail from IXCs, and mandatory 24 hour in-house attendant at each PBX control console or an automatic alarm algorithm that would page a PBX attendant who could shut down the PBX from a remote location. Further, Allnet contends that if IXCs are required to waive toll charges, local exchange carriers (LECs) should be required to waive corresponding access charges because it is unfair for IXCs to carry the burden of toll fraud, while LECs collect the underlying access charges.

23. In its reply comments, Bell Atlantic urges the Commission to deny the petition because when the Commission deregulated CPE 13 years ago,³⁷ it severed responsibility for CPE. Under this policy, the customer selects the CPE and its features, and in concert with the vendor, bears the risk if the CPE selected fails to meet expectations. Bell Atlantic, however, proposes that the Commission should encourage CPE manufacturers and vendors to work with carriers to develop solutions to prevent toll fraud and would cooperate fully in any such Commission-inspired efforts.

24. Comment Requested. Although we reached different results in Chartways, a PBX fraud case, and United Artists, a payphone fraud case, the dispositive element in each of these cases was where responsibility for the detection and prevention of fraudulent calling lay. In Chartways, the complainant had taken no discernible action to detect or prevent the fraudulent calling and the carrier had not acted negligently with regard to the calls. We therefore determined that the carrier could hold Chartways liable for the disputed charges. In United Artists, by contrast, the victim of the toll fraud had taken several reasonable steps to detect and prevent unauthorized calling, which nonetheless occurred. There, we concluded that the carrier had acted unlawfully in attempting to hold United Artists liable. If customers are unaware of potential liability, they are unlikely to take steps to limit their exposure. And, if carriers have no economic incentive to help customers limit their exposure, they are unlikely to invest in developing proactive solutions to PBX, or other, kinds of fraud. In light of the liability findings that resulted from the records in proceedings such as Chartways and United Artists, we tentatively conclude that tariff liability provisions that fail to recognize an obligation by the carrier to warn customers of risks of using carrier services are unreasonable.

³⁷ In its comments, Bell Atlantic refers to Amendment of Section 64.702 of the Rules, 77 FCC 2d 384 (1980).

Moreover, we tentatively conclude that carriers have an affirmative duty to ensure that these warnings are communicated effectively to customers through for example, billing inserts, annual notices, or other information distribution methods.

25. We request comment on what other factors could or should be considered when liability determinations must be made.³⁸ Specifically, we seek comment on whether to apportion the cost of CPE-based fraud based on whether carriers, CPE owners, equipment manufacturers, or possibly others were in the best position to avoid, detect, warn of, or control the fraud. Further, we request comment on whether this apportionment should be based on a comparative negligence theory as proposed by Pacific Mutual and many commenters supporting its petition. We note that potential shared liability would require definition of the specific responsibilities of the CPE-owner to secure the equipment or communications system, of the manufacturer to warn of toll fraud risks associated with features of the CPE, and of the carrier to offer detection and prevention programs and educational services. We seek comment on what constitutes a failure to meet these responsibilities, on the nature of damages to be awarded to aggrieved parties, and on the appropriate forum to resolve these issues. For example, we request comment on whether arbitration or mediation should precede Commission involvement, and whether Commission involvement, if necessary, should begin with alternative dispute resolution or formal complaint proceedings. Further, we request comment on which party in a billing dispute involving allegations of toll fraud should bear the expense of arbitration. We also seek comment on whether residential ratepayers would bear the burden of business fraud by paying higher rates. Commenters should also discuss how carriers may recover charges for calling card fraud, where cardholder liability is limited to \$50.00. See para. 38, infra.

26. Commenters are asked to address fraud prevention measures various parties might take. The record shows that carriers have increased fraud detection service offerings during the last 18 months. In light of our tentative finding that tariff liability provisions that fail to recognize a duty by the carrier to warn customers of risks of using carrier service are unreasonable, we ask whether a failure to offer services to limit customers' exposure should be considered an unreasonable practice. Consequently, we seek comment on whether to require IXCs and LECs to offer customers protection through monitoring services, on what basis those services should be offered, and whether such services should be part of the basic interexchange service offering. We also seek comment on whether there is software or equipment that

³⁸ With regard to the reply comments of Bell Atlantic, we are not proposing to regulate carriers' provision of CPE, but rather carriers' imposition of charges for fraudulent interstate service.

customers should install in their CPE to prevent fraud. Further, we request comment on whether the programs offered by carriers such as MCI Detect, AT&T NetProtect and SprintGuard, designed to help businesses protect their CPE from toll fraud, include sufficient features as customer education, fraud detection equipment, traffic analysis, third party insurance, and real-time monitoring and detection. We seek comment on the availability of these programs to both large and small CPE owners, and their efficacy. In addition, we invite commenters to discuss in detail any other proposals or considerations relevant to liability determinations. We invite specific rule proposals for consideration.

C. Payphone Fraud

The Florida Petition

27. In its petition, the Florida Public Service Commission (Florida PSC) requests that the Commission review tariff provisions governing liability for toll charges resulting from fraudulent third party calls where payphone providers have purchased originating line screening (OLS) and billed number screening (BNS) services from carriers.³⁹ The Florida PSC proposes that the Commission adopt regulations mirroring recently adopted Florida regulations.⁴⁰ The Florida regulations, which became effective February 3, 1993, release a pay telephone provider from liability for charges resulting from certain types of fraudulent calls if the provider purchases call screening for the line (OLS and BNS).⁴¹ In addition to relieving payphone providers from liability, the Florida PSC rules require that the losses from fraud be allocated between the LECs and IXC's based on fault.⁴² Further, the Florida

³⁹ Originating line and billed number screening services inform operator service providers of any billing restrictions on its lines.

⁴⁰ Florida Administrative Code, rules 25-4.076, 25-24.475, and 25-24.515. Order No. PSC-93-0109-FOF-TP.

⁴¹ The Florida approach was raised by a commenter in the OSP rulemaking proceeding, but was not examined substantively by the Commission because it was beyond the scope of that proceeding. See Report and Order, CC Docket No. 91-35, 6 FCC Rcd 4736, 4744-45 (1991).

⁴² The Florida rule prohibits a company providing interexchange services or local exchange services from collecting from a pay telephone provider for charges billed to a line for calls that originated from that line through the use of 10XXX+0, 10XXX+01, 950-1/0XXX+0, or 1-800 access code, or when the call originating from that line otherwise reached an operator position,

PSC proposes that where a carrier does not accept or observe LEC OLS and BNS codes or fails to validate its calls via the appropriate LEC database, the carrier, not the payphone provider, should bear the costs of the resulting toll fraud under a uniform national policy. The Florida PSC argues that foreign carriers, through whom inbound international calls are initiated, have little or no incentive to validate calls because AT&T will bill the calls to payphone providers even though BNS could have been used to prevent the call from being completed.⁴³ The Florida PSC asserts that if AT&T were required to refuse payment to the foreign carrier for such calls, an incentive to validate will be created. The Florida PSC further contends that AT&T has insulated itself from this type of fraud at its own pay telephones.⁴⁴

28. Comments. Many commenters favor a multi-jurisdictional or national application of the recently adopted Florida PSC rule limiting liability and apportioning liability based on fault.⁴⁵

if the originating line is covered by outgoing call screening and the call was placed after the effective date of the outgoing call screening order. The rule also prohibits a company providing interexchange services or local exchange services from collecting from a pay telephone provider for charges for collect or third number billed calls, if the line to which the call was billed was covered by incoming call screening and the call was placed after the effective date of the incoming call screening order. The rule further provides that any calls billed through the LEC or directly by the IXC, or through a billing agent, that have been identified as not collectible must be removed from any pay telephone provider's bill after the pay telephone provider gives notice of the fraudulent charges to the billing party and such notice must be provided to the LEC and IXC in writing no later than the due date of the bill. The LEC is responsible for charges that are associated with the failure of the LEC's screening services, and the IXC is responsible for charges that are associated with its failure to properly validate calls via the appropriate LEC data base.

⁴³ Florida PSC petition at 3.

⁴⁴ See Attachment at 27, Question No. 5, Florida PSC petition. The Florida PSC asks what disposition would be made of toll fraud charges if they had originated or terminated at an AT&T payphone. AT&T responds that "because of the differing status of AT&T payphones which are part of AT&T's network, the calls could not have occurred under the same circumstances."

⁴⁵ See a.g., Comments of IMR Capital Corporation, Indiana Payphone Association, Intellical, Inc., Louisiana Payphone Association, Midwest Independent Coin Payphone Association, Mississippi Public Communication Association, Minnesota Independent

Several commenters also propose that a federal rule should provide that if a payphone provider subscribes to international call blocking, the payphone provider would not be liable for international direct dial calls. Most commenters who support the petition contend that because LECs and IXCs are able to ensure the integrity of OLS and BNS they should be liable for fraudulent calls completed despite the use of screening mechanisms. In its comments, Minnesota Independent Payphone Association asserts that requiring payphone providers to unblock phones to provide the public with their choice of carriers increases the risk of fraud.⁴⁶ Many of the commenters supporting the petition contend that it was implicit in the equal access decision that payphone providers could rely on screening devices.

29. NARUC and the California Payphone Association contend that liability should attach to the entities that control the blocking and screening services and receive revenue from those services. Many commenters concur that the LECs and IXCs are much better able to absorb the costs of fraud than payphone providers because their cost is marginal cost, whereas the cost to the payphone providers is marginal cost plus mark-up, plus the cost of the ineffective screening services, plus the cost to contest the charges. Commenters representing payphone providers contend that the charges are both unfair and discriminatory because LEC and IXC payphones are not charged for fraudulent calls. Further, these commenters contend that classifying payphone providers as "customers" is illogical because payphone providers do not want or order the service that the fraud occurs on, and they take affirmative steps to prevent its delivery.

30. In opposition to the petition, many commenters contend that the emphasis of any fraud proposal should be on fraud prevention, not on the apportionment or assignment of liability. These commenters assert that apportioning liability after the fraud will not prevent fraud from occurring.⁴⁷ They claim that adoption

Payphone Association, New Jersey Payphone Association, Inc., North Carolina Payphone Association, South Carolina Division of Information Resource Management, Utah Payphone Association, Arizona Payphone Association, California Payphone Association, Florida Payphone Association, Georgia Public Communications Association, GTE Service Corporation, and Independent Payphone Association of New York.

⁴⁶ Our operator service rules require only the unblocking of operator-assisted access, not direct-dialed (1+) access. See 47 CFR Section 64.704.

⁴⁷ See e.g., Comments of Sprint, Interexchange Carrier Industry Committee Toll Fraud Subcommittee, MCI, SWB, Ameritech, Bell Atlantic, BellSouth, and AT&T.

of the Florida PSC proposal would precipitate higher rates, and increased litigation before the Commission. Some argue that LECs do have incentives to fight fraud, as evidenced by their efforts to detect fraud and by increased competition in the local loop. Many commenters argue that equal access rules never were intended to make carriers insurers and guarantors because, if this were required, blocking and screening service fees would increase dramatically. These commenters further argue that increases in service fees would cause usage of the services to decline, with a net result that losses from fraud would increase. Moreover, these commenters argue, the payphone providers are not taking available fraud prevention precautions. They state that in some service areas, only a minority of payphone providers subscribe to blocking and screening services, and there is little demand from other aggregators.⁴⁸ These commenters further argue that Commission requirements for equal access did not project that screening services would be fool-proof protection against fraud and that before liability attaches, payphone providers should be required to do much more than merely subscribe to blocking and screening services. Many commenters propose that payphone providers should be required to purchase adjunct services, programmable phones, and special dial tones, and to locate their payphones where they can be observed. With regard to arguments by payphone providers that IXCs do not charge LEC or IXC phones for fraudulent calls, commenters argue that LECs and IXCs are not "customers."

31. Comment Requested. We agree with the Florida PSC that carriers should, as a general matter be held accountable for the services they provide. The Florida PSC rule which apportions liability based on fault accomplishes this general goal. We also find merit in the proposal by the Florida PSC that we review those portions of tariffs filed with the Commission that limit carrier liability associated with payphone fraud. Our decision in United Artists limited the payphone provider's liability where it took reasonable steps to limit its exposure to toll fraud because it was not a customer of the billing interexchange carrier. We tentatively conclude that payphone providers that take reasonable steps to limit their exposure to toll fraud and are not customers should not be required to pay bills generated as a result of toll fraud perpetrated through their equipment. We consider adopting the Florida approach but before adopting it as a national model, we are anxious to learn how it has worked in practice. We ask commenters to tell us whether the Florida approach has been an effective, efficient way of dealing with payphone fraud. We seek comment on whether carriers should be required to modify tariff language limiting carrier liability for payphone fraud and how this modification would affect carriers and payphone providers. We also seek comment on the general availability of blocking and screening services, whether they are priced reasonably, what percentage of

⁴⁸ See Comments of Bell Atlantic at 2.

payphone providers are using these services where they are available, and whether they are effective in reducing the risk of fraud.⁴⁹ Further, we seek comment on whether there are other services available to payphone providers that reduce the risk of fraud, or whether payphone providers can prevent the fraud. We request comment on whether a federal fraud policy based on the Florida model is necessary to apportion the costs of payphone fraud, or whether tariffs filed by carriers for blocking and screening services should be required to clearly articulate the responsibilities of the parties and apportion the costs of fraud incurred in the use of these services.

D. Cellular Fraud

32. The fraudulent use of cellular telephones has become a serious industry problem that results in financial losses to consumers, and increases the cost of doing business for the cellular industry. While there is no official reporting system, the industry estimates that cellular carriers lose between \$100 million and \$300 million per year because of cellular fraud.

33. The three major types of cellular fraud are: subscription fraud; stolen phone fraud; and access fraud. Subscription fraud occurs when someone subscribes to cellular service with fraudulent information or false identification and with no intention to pay for service. Stolen phone fraud involves the unauthorized use of a phone stolen from a legitimate customer before that customer can report the theft. Access fraud involves the unauthorized use of cellular service through the tampering, manipulation or programming of a cellular phone's Electronic Serial Number (ESN)⁵⁰ or Mobile

⁴⁹ In our Order on Further Reconsideration and Further Notice of Proposed Rulemaking, Policies and Rules Concerning Operator Service Access and Pay Telephone Compensation, 8 FCC Rcd 2863 (1993), we requested comment on whether to require BNS and OLS services to be tariffed at the federal level, whether these services should be available unbundled, to all customers, and at reasonable rates, and whether to require LECs to extend their international blocking services to non-aggregator business and residential subscribers. With regard to the issue of BNS and OLS, the record in this proceeding reflects that the LECs generally oppose federal tariffing of these services because these services are traditionally provided through state tariffs. The record in this proceeding also indicates, however, that existing state tariffed screening services are not uniform and are frequently not available to all classes of aggregators.

⁵⁰ The ESN is a 32 bit binary number that uniquely identifies a mobile station to any cellular system for billing and other purposes.

Identification Number.⁵¹ Access fraud represents the most sophisticated of the three types of fraud and the most serious in terms of dollars lost. There are two major types of access fraud: tumbling, and counterfeiting or cloning. In tumbling, an unauthorized user either randomly or sequentially changes the ESN or MIN after every call, thereby confusing a cellular system switch long enough to complete a call. Counterfeiting or cloning fraud occurs when an unauthorized user programs a valid subscriber MIN/ESN match into a phone. The unauthorized user then uses the cloned phone until detected. While recent developments involving pre-call validation⁵² greatly reduce the amount of fraud due to tumbling, cloning fraud continues to grow at a rapid pace. The Secret Service estimates that altered or cloned cellular phones are becoming as common as fake identification cards, and are the instruments of major crimes such as drug-trafficking.

34. Comment Requested. In Revision of Part 22 of the Commission's rules governing the Public Mobile Service (Notice of Proposed Rulemaking), 7 FCC Red 3658, 3741 (1992), we proposed a rule to help reduce cellular fraud caused by tampering with the ESN.⁵³ The proposed rule establishes additional technical specifications for mobile equipment to prevent tampering with the ESN. We now seek comment on what further efforts on the part of the cellular industry, manufacturers, vendors, law enforcement agencies, and the Commission would aid in combatting cellular fraud. We seek comment on whether the Commission should consider stricter measures where cellular fraud occurs, and if so, what measures the Commission should consider.⁵⁴ We recognize that certain types of cellular fraud could be included in the CPE-Based

⁵¹ The MIN is a 24 bit number that corresponds to the seven digit directory telephone number assigned to a mobile station.

⁵² Pre-call validation occurs when the cellular switch compares an incoming caller's ESN/MIN number against a subscriber database before the call is completed.

⁵³ See Proposed Section 22.929 which provides that each mobile transmitter must have a unique ESN that must be factory set, and must not be alterable, removable or otherwise able to be manipulated in the field. This proposed rule requires that the ESN host component must be permanently attached to a main circuit board of the mobile transmitter and the integrity of the unit's operating software must not be alterable. Finally, the cellular equipment must be designed so that any attempt to remove, tamper with, or change the ESN chip will render the mobile transmitter inoperative.

⁵⁴ See Section 503(b)(5) of the Commission's rules that provides for forfeiture proceedings against non-licensees or non-applicants who willfully or repeatedly violate the Commission's rules.

Fraud category. We, therefore, request comment on how the issues raised above in our discussion of CPE-based fraud should be resolved in the context of cellular fraud. Specifically, are adequate incentives in place for industry to develop anti-fraud solutions, or should new initiatives be chartered by the Commission? Is a shared liability theory for cellular fraud appropriate? Is unique criminal legislation necessary? Should labeling requirements be adopted? Comments should also present detailed proposals or alternatives to address cellular fraud.

E. Line Information Database (LIDB) Fraud

35. A LIDB is a line information database created by an individual local exchange carrier.⁵⁵ LIDB service enables customers such as interexchange carriers to query the database to determine whether a LEC joint use calling card⁵⁶ is valid for use, or whether a particular telephone number can accept collect or third-party billed calls, before transmitting any call using that card or line number. Each database can be accessed by other LECs, IXCs and other customers to obtain data on the account status of LEC joint use calling cards, as well as information on line numbers, such as third party billing or collect call restrictions. This information is stored in the LIDB and updated by the LEC on a regular basis.⁵⁷

36. Comment requested. As the owners of the database, it might be assumed that the LECs are able to detect fraudulent use, such as billing to restricted numbers or unauthorized credit card use. However, LIDB customers have an obligation as well; if a LEC card is offered for billing, the IXC or operator service provider (OSP) should query the LIDB to determine whether the card is valid for use. If the customer queries the LIDB each time the card is offered for payment, the LEC is able to detect high spikes of usage, i.e., multiple validation queries to the LIDB in a short

⁵⁵ See Local Exchange Carrier Line Information Database, CC Docket No. 92-24, FCC 93-400, 8 FCC Rcd [] (1993) (LIDB Investigation Order).

⁵⁶ LEC joint use calling cards bear account numbers supplied by a LEC, are used for the services of the LEC and an IXC, and are validated by access to data maintained by the LEC. See Second Report and Order, Policies and Rules concerning Local Exchange Carrier Validation and Billing Information for Joint Use Calling Cards, CC Docket No. 91-115, 8 FCC Rcd 4478, 4478 fn.5 (1993).

⁵⁷ In the recent LIDB Investigation Order, the Commission investigated 10 LIDB databases offering validation services. The record indicates that these databases are updated 24 hours a day, seven days a week, and that each LEC offering LIDB validation services also has a fraud control program.

time period, prompting the LEC to investigate and then to determine whether it should deactivate the card. However, the fraud does not always consist of multiple calls within a short period of time and, therefore, may not be detectable by the LEC. For example, the fraud might consist of one call of long duration. In addition, the fraud perpetrator might discover the usage spike set by the LEC and place calls in such a manner that the LEC would not immediately detect the fraud. The LECs assert that detection of usage spikes is the only mechanism available for detecting fraud associated with the LIDB.

37. It has been alleged that losses from calling card fraud would be substantially reduced if the LEC had access to the calling number and the called number from the IXCs, as those numbers provide information on the origination and termination points of the call. This would allow the LEC to identify a call originating from or going to an area associated with fraud problems. This information would assist the LECs in developing a customer calling pattern profile that could be accessed in a case of suspected fraud. We seek comment on whether the carriers querying LIDB should provide the LECs with the originating calling party number and the called numbers. Commenters are also requested to explain how the presence or absence of this information should affect any decision concerning the allocation of liability for toll losses, and whether carriers should be permitted to charge for the provision of this information.

38. Under the Truth in Lending Act and Federal Reserve Board regulations, cardholder liability for unauthorized use of calling credit cards is limited to \$50.00.⁵⁸ Therefore, when a card number is stolen or used without the cardholder's knowledge or permission, the LECs and their LIDB customers (IXCs, OSPs) must decide between themselves who will bear the cost of the uncollectible toll revenues. Of course, cardholders are under an affirmative obligation to report lost or stolen credit cards immediately, and to protect against theft of their card numbers. In the LIDB Investigation Order, the Commission required the LIDB providers subject to that investigation to include in their tariffs certain minimum procedures to help reduce the number of fraudulent calls.⁵⁹ However, the Commission left open the issue of liability for toll fraud losses that results from LEC provision of erroneous LIDB information.⁶⁰

39. Assignment of liability for toll losses among LIDB providers and LIDB customers raises two concerns that should be

⁵⁸ 15 U.S.C. § 1643; 12 C.F.R. § 226.12(b)(1).

⁵⁹ LIDB Investigation Order, 8 FCC Rcd at ¶ 19, 27-34.

⁶⁰ Id. at ¶ 29-30.

addressed. First, there may be many different fact patterns each time a loss is generated, making the development of a general rule difficult. In addition, limitation of liability provisions have long been accepted by the courts in the absence of willful misconduct or gross negligence.⁶¹ Consequently, clauses limiting a carrier's financial liability to the cost of the service are found in virtually all common carrier tariffs. While the carrier's customers in this case are likely to have a sophisticated understanding of the risks of credit card fraud, LIDB providers should have incentives to make LIDB as effective as it can be. We seek comment on whether these limitations of liability should be permitted to shield the LECs from responsibility for toll losses incurred when a joint use calling card is used to bill fraudulent calls or whether the Commission should establish a rule for allocating liability for toll losses. Commenters are also requested to comment on whether such liability should be described in the LECs' tariffs.

F. Other Proposals and Request for Comment

40. In addition to proposals already made herein, we propose to amend Part 68 of the Commission's rules to require equipment manufacturers to provide warnings regarding the potential risk of toll fraud associated with use of equipment.⁶² We further propose that the warnings be prominent and conspicuous and included in any instruction manual or other literature accompanying the equipment, and on the exterior packaging of the equipment. Further, we propose that the warning in the instructional manual or literature discuss the customer's financial exposure and measures available to limit that exposure. We also propose in the case of PBX and similar equipment, if default codes are set by the manufacturer, vendor, or carrier, those codes must be fully explained in the instructional manual or literature and must explain the risks of using the equipment without modifying these default codes. We seek comment on specific language of warnings, whether warnings should be required for only newly registered equipment or whether they should be required for all telephone equipment already registered pursuant to Part 68. We also seek comment on whether the Commission should adopt standards for determining whether FCC registrations for any classes of particularly risk-prone equipment should be revoked, or whether warnings should be required as updates to manuals currently in use. Further, we seek comment on how others in the manufacturing and distribution chain of telephone equipment could warn consumers of the risks of fraud.

⁶¹ See, e.g., Western Union Telegraph Company v. Esteve Brothers & Co., 256 U.S. 566, 571 (1921); Primrose v. Western Union Telegraph Co., 154 U.S. 1 (1894); Robert Gibb & Sons, Inc. v. Western Union Telegraph Co., 428 F.Supp. 140 (D.N.D. 1977).

⁶² See Proposed Rule at Appendix E.

41. Many comments filed in response to the en banc hearing, the Pacific Mutual proceeding, and the petition of the Florida PSC conclude that carriers need to incorporate more safeguards into their network operations to protect against and detect instances of toll fraud and abuse. For example, in its comments, Science Dynamics Corporation (SDC)⁶³ explains that it develops products for carriers that can curb or eliminate some sources of toll fraud. SDC manufactures a device that controls inmate access to the telecommunications network, and a system that monitors toll usage by predetermined customers and places a cap on long distance usage over a monthly billing cycle. Many commenters contend that such solutions that would minimize the fraud problem are available; however, they argue that as long as the regulated carriers do not have to absorb directly the losses attributable to fraud, carriers have little incentive to invest in preventive systems. The issue has been raised regarding LEC and IXC incentives to prevent fraud in light of their billing and collection arrangements. We request comment on whether incentives that the telecommunications industry has to initiate anti-fraud solutions can be strengthened, and what other actions the Commission should take to further fraud prevention. We also seek comment regarding network changes which could influence toll fraud detection or prevention. Specifically, we request comment on how, when, and where a carrier should release such information when it makes a network change.

IV. CONCLUSION

42. The Commission's obligation to regulate interstate telecommunications services so that the public has rapid and efficient service at reasonable rates requires that our policies keep pace with rapidly changing technology and industry structure. In this Notice of Proposed Rulemaking, we request comment on the questions and proposals set forth above, the proposed rule set forth in Appendix E, and encourage participation by interested parties. The purpose of this rulemaking is to develop effective and efficient measures to address both existing and developing toll fraud problems, without hindering the development of new technologies that provide benefits to the public.

IV. PROCEDURAL MATTERS

43. Initial Regulatory Flexibility Act Analysis on the Notice of Proposed Rulemaking and Ex Parte Rules

Ex Parte Rules - Nonrestricted Proceeding

⁶³ See Comments of Science Dynamics Corporation (SDC). Pacific Mutual proceeding.

This is a nonrestricted notice and comment rulemaking proceeding. Ex Parte presentations are permitted, except during the Sunshine Agenda period, provided they are disclosed as provided in Commission rules. See generally 47 C.F.R. Sections 1.1202, 1.1203 and 1.1206(a).

Objectives.

This rulemaking proceeding is initiated to develop effective and efficient measures to address toll fraud problems. The Commission requests comment on proposals to achieve closer coordination between the industry, consumers, vendors, law enforcement agencies, Congress, and the Commission to aid in the detection and prevention of toll fraud; improve consumer education initiatives by the Commission, consumer groups, and the telecommunications industry; determine that tariff liability provisions that fail to recognize an obligation by the carrier to warn customers of risks of using carrier services are unreasonable; establish a federal policy assigning liability for payphone fraud; and codify a requirement for written warnings for all telecommunications equipment registered under Part 68.

Reporting, Recordkeeping and Other Compliance Requirements

The actions proposed in this Notice of Proposed Rulemaking may affect large and small common carriers, manufacturers of equipment registered under Part 68, and CPE owners. It is not estimated that the burden of including warnings with the filing of Part 68 registration applications will be a significant economic burden on manufacturers. It is not estimated that the burden of including warnings in tariff filings or in billing inserts will be a significant economic burden on subject common carriers.

Description, Potential Impact, and Number of Small Entities Involved

The proposals discussed in this Notice of Proposed Rulemaking primarily could affect the degree to which small businesses are responsible for charges associated with fraudulent calls made over their equipment. The Secretary shall send a copy of this Notice of Proposed Rulemaking including the certification to the Chief Counsel for Advocacy of the Small Business Administration in accordance with paragraph 603(A) of the Regulatory Flexibility Act. Pub. L. No. 96-354, 94 Stat. 1164, 5 U.S.C. Section 601 et seq. (1981).

Any Significant Alternatives Minimizing the Impact of Small Entities Consistent with the Stated Objectives

The Notice of Proposed Rulemaking solicits comments on a