

ORIGINAL

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 14 1994

Stephen Satchell  
PO Box 6900  
Incline Village, NV 89450

FCC MAIL ROOM

January 12, 1993

Office of the Secretary  
Federal Communications Commission  
1919 M Street, NW  
Washington, DC 20554

Reference: CC Docket 93-292

Sirs,

This letter constitutes my comments on your Notice of Proposed Rulemaking (NPRM) CC 93-292, FCC 93-496 entitled "In the Matter of Policies and Rules concerning Toll Fraud." I am commenting as an individual, a customer of plain ol' telephone service (POTS) and a victim of toll fraud on my residential lines.

No. of Copies rec'd  
List A B C D E

0 1 9

TABLE OF CONTENTS

SUMMARY ..... 1

COMMENTS ..... 2

1—Agreement to proposed Part 68 amendment ..... 2

2—Identification of victims of toll fraud ..... 2

3—Types of fraud identified ..... 3

4—The en banc Proceeding, Participants of ..... 3

5—Conflicting Statements Summarizing the en banc Hearing ..... 3

6—Answer to Paragraph 13 Comment Request ..... 4

    a—Press Releases ..... 4

    b—Notification of Radio and Television Licensees ..... 5

    c—User of Internet, Commercial On-Line Services, BBS ..... 5

    d—LECs, Cellular Carriers Include Notices on Bills ..... 5

7—Answer to Paragraph 24 Comment Request ..... 6

    Carrier has obligation to warn customers of risk ..... 6

8—Answer to Paragraph 25 Comment Request ..... 6

    a—Fraud-Detection Tools a Factor When Determining Liability ..... 6

    b—Carrier/LEC Traffic Monitoring Not a Factor ..... 7

    c—Ultimate Responsibility Lies With Customer ..... 7

9—Answer to Paragraph 26 Comment Request ..... 7

    a—PBX Access Control ..... 7

    b—Improved CPE Administration Tools ..... 8

    c—Improved CENTREX™ et al. Access Control and Administration Tools ..... 9

    d—User/Employee Liability ..... 9

    e—Intrusion alerts printed on the bill ..... 10

10—Answer to Paragraph 34 Comment Request ..... 10

    a—Extend cellular tariffs to enable “extensions” ..... 10

    b—Improved Access Controls ..... 11

    c—Intrusion alerts printed on the bill ..... 12

11—Answers to Paragraph 36 Comment Request ..... 12

    a—typographical error in the NPRM ..... 12

    b—Intrusion alerts printed on the bill ..... 12

12—Access by LEC to Source/Destination Telephone Numbers ..... 13

13—Liability for LIDB Reporting Errors ..... 14

14—Description of Proposed Rule Overly Broad ..... 14

15—Answer to Paragraph 40 Comment Request ..... 15

    a—Language of warning shall be in non-technical, non-legal English ..... 15

    b—Warnings required for existing equipment ..... 15

    c—Minimal effect on existing registrations ..... 16

    d—LECs, cellular carriers to provide warning literature ..... 16

    e—The Internet, Commercial On-Line Services, BBSes ..... 16

    f—Encryption Between the Customer and Carrier ..... 17

    g—Role-Playing Game as Fraud-Fighting Training Tools ..... 18

16—Commenter’s Conclusion ..... 20

[End of comments] ..... 20

SUMMARY

This letter is organized as a series of points pertaining to portions of and questions asked by the NPRM. Each point is numbered, and the paragraph(s) or other entity(ies) in the NPRM to which the point is directed is indicated.

The major point I wish to make as a commenter is that the key to toll fraud is the telephone service customer, not the service providers and carriers. More important, "customers" include those people who subscribe to "plain ol' telephone service"—a rather large group of customers who seem to be virtually ignored in the NPRM.

I am commenting as an individual, one of those POTS customers—and one who has been affected by toll fraud of two flavors: "clip-on" fraud (fixed with a padlock on my network interface box) and calling-card fraud. While my total loss was less than \$300 I consider any loss important.

By profession, I am a computer technologist specializing in telecommunications and security issues. I am not commenting in my professional capacity, however.

Throughout this comment, you will continue to see the phrase "vendors can provide the lock; customers have to turn the key." As the Commission itself mentioned, many of the tools required to detect and avert fraud are there. People have to learn how to use them, and the tools themselves have to be made easier to use.

COMMENTS

1—Agreement to proposed Part 68 amendment

[Appendix E] I agree with the text as proposed in Appendix E of the NPRM, but see my point (14) below.

2—Identification of victims of toll fraud

[Paragraph 3] While the Commission uses the term "customers" in the third sentence of this paragraph in its most general sense, much of the discussion throughout the NPRM focuses on large users of telecommunications, providers of telecommunications service, and issues involving the resolution of disputes among providers.

The lists of commenters (Appendixes A, C, and D) includes no readily-identifiable individuals, advocate organizations devoted to presenting the views of individuals, or news media. In Appendix B, there were no panel members who were identified as speaking in any way with respect to small telephone customers.

Fraud against residential, "life-line," and small-business users (those without PBX or similar equipment) is perpetrated across state lines and Local Access and Transport Area borders. This means that the scope of actions which can be taken against fraud which victimizes the small user is beyond the charter of individual local exchange carriers and State telephone authorities. The only organizations with jurisdiction to make rules to help prevent the occurrence of and assist in investigating instances of fraud against "the little guy" is the Federal Communications Commission and the Congress.

### 3—Types of fraud identified

[Paragraph 4] Calling card fraud using what cryptographers call “practical cryptography” as described in the NPRM is one way in which LEC-supplied calling cards are abused. Another method which is not under the control of the customer is the calculation of the most probable PINs using information obtained (usually illegally) from the LEC issuing the card.

Another source of fraud not identified in the NPRM which affects small users as well as large is the abuse of third-party-billed calling, when the operator services provider does not verify that the party being charged is willing to accept the charge. This—coupled with the agreements between LECs and operator service providers and the rules and regulations of the telephone authority of the several States—shifts the burden of the fraud onto the small consumer, said consumer not having the resources to fight the action either in Court or in front of the telephone authority for the State.

### 4—The en banc Proceeding, Participants of

[Paragraph 6] Please see point (2) above. I feel that the absence of any representation by small telephone consumers at the *en banc* proceeding represents a significant defect in the proceeding, particularly with regards to Panel 2, *Network-Based Toll Fraud, Responsibility, and Liability Questions*.

[Appendix B]

### 5—Conflicting Statements Summarizing the en banc Hearing

[Paragraph 11 and 12] In paragraph 11 the second sentence reads

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. [emphasis mine]

Yet the first sentence of paragraph 12 refutes this by saying

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 ... and that additional consumer education is necessary to detect and prevent toll fraud.  
[emphasis mine]

The remainder of paragraph 12 shows just how weak the statements are in paragraph 11, as these excerpts from the NPRM show:

...criminal prosecution of toll fraud perpetrators is infrequent. ... [Lack of prosecution] may be due to the high dollar thresholds set by the U. S. Attorneys because toll fraud cases generally are manpower intensive but often result in either suspended sentences or short incarcerations.

...

In short, the law is no help to the small, individual telephone consumer. That consumer is further hamstrung by the monopoly position of the LEC, such that collection actions on amounts owing due to disputed items may well result in loss of telephone service by the customer as the LEC disconnects service for non-payment. (One IXC refers to this as "the leverage of dial-tone.")

#### 6—Answer to Paragraph 13 Comment Request

##### a—Press Releases

Toll fraud affects everyone, yet I personally have seen few articles in the mass media (magazines, books, electronic media) about toll fraud and how to combat it at the individual customer level. Education efforts should include press releases and white papers from the Commission's engineering departments and other interested parties to major news outlets, including but not limited to television stations, radio stations, television networks, major computer magazines, consumer-advocate organizations, and the major newspaper chains.

b—Notification of Radio and Television Licensees

In the case of radio and television stations, the Commission is in a unique position since it knows from its own records the mailing address of every single licensed station in the United States.

c—User of Internet, Commercial On-Line Services, BBS

One inexpensive and effective way to gain access to a number of news outlets is to sponsor an Internet host site. Such a host site should sponsor one or more newsgroups, and have available via the various means (anonymous FTP, gopher) information on toll fraud and other topics.

To reach people outside of the industry, the Commission should participate on a number of on-line services. As a member of the press, I get many ideas from stories from discussions taking place on the CompuServe Information Service and from BIX. Such participation can be on an informal basis, with one or two Commission employees working on each service.

For example, I found out about this NPRM when a participant on the TELECOMMUNICATIONS Forum on CompuServe mentioned it in a message posted on January 7, 1994. I ended up getting a copy of the NPRM from my local telephone company office in Reno, NV — and they told me that mine was the first such request for any material relating to any Notice of Proposed Rule-Making in the memory of the people there.

d—LECs, Cellular Carriers Include Notices on Bills

Finally, I feel that the LECs and cellular carriers need to make their customers aware of actions by the FCC that will affect them. I ask the Commission to consider a Rule which would require LECs and cellular carriers (indeed, any provider of dial tone) to include brief notices, as part of the monthly bill, of Notices of Proposed Rulemaking which would affect the customer. Without such notice, small customers without the resources of a full-time telecommunications expert (or FCC-watcher) will not be able to participate in these proceedings. Look at me: I'm able to comment only because of a fluke!

7—Answer to Paragraph 24 Comment Request

Carrier has obligation to warn customers of risk

I agree with the Commission in ruling the way it did in the case of *Chartways*, *United Artists*, and *Pacific Mutual*. Fraud control starts with the telephone service customer, always. While “ignorance of the law” is no defense in court, I feel that the Commission is correct in saying that service providers have an obligation to inform customers of the fraud possibilities in using certain features.

I also feel that the Proposed Rule is a good start in giving telephone customers a fighting chance to prevent or limit the effect of fraud.

8—Answer to Paragraph 25 Comment Request

a—Fraud-Detection Tools a Factor When Determining Liability

I believe that fraud control starts, stops, and resides in the customer’s control; only the customer can know when a shift in calling pattern is expected or an indication of fraud.

N.B.: In the case of a telephone number not assigned to a customer, the LEC becomes the customer for the purposes of this discussion.

That said, the customer has to be provided the opportunity to obtain the tools needed to protect against fraud, detect fraud, or both. I would give weight in making such a determination of shared liability to the availability of fraud-detection tools and education in the use of them from the CPE vendor, from the local exchange carrier, and in the case of CPE equipment connected directly to the interexchange carrier’s switch the IXC.

b—Carrier/LEC Traffic Monitoring Not a Factor

I oppose Pacific Mutual's position that LECs and IXC's should be required to perform traffic monitoring or other actions to detect fraud, and to be liable for any breakdown in such monitoring or other actions, as a part of standard service. The LEC or IXC or both can offer fraud-detection or fraud-blocking services at additional cost (subject to tariff restrictions) with the measure of performance specified in the contract or tariff.

c—Ultimate Responsibility Lies With Customer

But the ultimate responsibility for fraud detection lies with the customer.

9—Answer to Paragraph 26 Comment Requesta—PBX Access Control

One of the defects in the case of *Pacific Mutual* is that there is no mention of access controls of any kind mentioned in the summary provided in paragraphs 14-23. Access controls would permit the customer to substantially prevent fraud, and when fraud is detected to put a stop to the activity without materially affecting non-fraudulent use of the facility.

In the case of outpulsing, I would require that the user be positively identified. After being identified, I would then determine if that user has been authorized to use outpulsing. Finally, I would include access control to the capability itself: to outpulse, you have to know both the access code and a password associated with the access code.

Standards for access control have been studied in the computing community, and studies showing the cost/benefit trade-off for access control are available. I suggest that the Commission ask the Telecommunications Industry Association (TIA) to create a standard for PBX access control, if such a standard does not already exist within the ANSI framework, and that the Commission then determine if Rules referencing such a standard should be added to Part 68 for PBX devices.

Such a standard should include specifications and recommendation for: password management; password audits; access "rings"; capabilities-based access control; intrusion-alert criteria, with particular emphasis on minimizing false alarms; and call tracking within a private network.

b—Improved CPE Administration Tools

Most PBX systems have some method available to record calls originating from or answered by the PBX, and to make those transaction records available to the customer. What I see lacking is inexpensive software to properly analyze those records to detect and alert the customer to potentially fraudulent activity.

While I have little direct experience with maintaining CPE (other than the headaches I have administrating an Extrom 6x16 system which doesn't even have an RS-232 port!) I keep hearing about how bewildering the admin tools and documentation for those tools are that CPE vendors provide to their customers. This is particularly true for smaller, lower-priced PBX systems. I would be interested in receiving comments, and perhaps being involved in a formal review of CPE management tools. (My ten years as a product reviewer for the major computer magazines and consultant to magazine testing labs can be of use here.)

Tools that are easy to use and easy for a non-technical administrator to use would remove one of the barriers to effective CPE fraud control: "Don't rock the boat, it still works." More important, it means that a company doesn't need to have a consultant on call to perform basic security tasks such as taking a capability away from an ex-employee's station, so the lockout happens faster and potential fraud is avoided—particularly when an employee is fired on the spot for cause.

Vendors who refuse to develop the necessary adjunct software and tools and to provide them to customers as part of the equipment, or at worst as an attractively priced option, should be required to shoulder some of the fraud liability in the event that the lack of the software and tools contributed to the occurrence of fraud.

In particular, it is not enough for the CPE vendor to offer to perform administration functions on behalf of the customer as a substitute for on-premises direct control by the customer in order to avoid liability. Such a service opens the CPE vendor to liability in the event that the vendor is instructed to take a particular measure in order to prevent fraud and fails to do so; even worse is when the CPE vendor is instructed to take a particular measure and applies the measure *to the wrong station*, or takes a measure (either in error or by malicious intent) which the customer did not request.

In fraud detection and abatement, time is of the essence. Minutes can mean the difference between a threat removed and a penetration.

c—Improved CENTREX™ et al. Access Control and Administration Tools

The comments in proposal (a) and (b) above also apply to the access controls and administration tools provided to customers of central-office-located enhanced business services provided by the LEC. The LEC, either as part of the offering or as an attractively-priced service, can work with the customer in developing procedures for detecting and controlling fraud; yet, again, it is the customer who ultimately *knows* whether a change in call pattern is due to changes in business or because of potential or actual fraud.

d—User/Employee Liability

Ultimately, the security of any system is only as good as the people who use it. The Commission should take a hard look at the responsibilities of authorized users, the procedures and policies written by PBX customers which apply to those users, and the administration tools offered or provided to the PBX customers to monitor compliance with the policy.

In my career as an employee and as a consultant, I have seen many instances of authorized users of PBX systems disabling security for their station, leaving the door wide open for fraud through the access capabilities of that station. I have seen PBX administrators provide "initial access passwords" which are easily guessed—and authorized users not changing them.

Without the help of the user, everything that the PBX customer, PBX administrator, LECs, IXC, OSPs, and cellular carriers can do to help prevent fraud is a waste of time.

All anyone can provide the authorized user is the lock; the user has to turn the key.

e—Intrusion alerts printed on the bill

In the event that an attempt is made to make a collect call, or to charge a third-party call or a calling-card call to a PBX trunk number or to a DID number and that attempt fails for any reason, the operator services provider shall be required to provide a billing record of such an attempt. The OSP (or IXC) shall not charge for this billing record. The billing record shall include the originating telephone number and the destination telephone number. This specifically includes calls which are blocked because of LEC billing restrictions placed on the line or PBX billing rejection of the call.

10—Answer to Paragraph 34 Comment Request

a—Extend cellular tariffs to enable “extensions”

Part of the problem with cellular fraud as it is currently defined is that the cellular carriers have not defined a way to add “extension” phones to a current account. Most people consider that opening a completely separate account so that they can have a three-watt phone in the car and a 600-milliwatt phone in their pocket is excessive. Moreover, there is no provision for making both cellular telephones ring when a call comes in. The “quick fix” for the cellular customer is to have one of the telephones modified so that it has the same ESN and MIN—a situation which can cause the cellular carriers trouble, and is considered fraud.

I propose that the Commission consider reviewing the tariffs on file to see if an accommodation can be made in the tariff for the equivalent of an extension. Rates could be structured such that if both phones are in use at the same time that a surcharge could be added for those calls.

Suggested as a starting point for such an extension telephone: a charge for each additional telephone registration equal to at most one-quarter of the monthly rate for the first telephone. In the event that two or more phones are in use at the same time, a surcharge equal to the air time charges for both calls would be added to the bill. In other words, when you use multiple phones at the same time, the air time charges double for each call.

This proposal would remove the one "supportable" reason for changing ESNs in a cellular telephone.

#### b—Improved Access Controls

The lockout features currently available for cellular telephones are not very effective in controlling fraud from stolen telephones. In the case of a car-jacking involving an automobile with a cellular telephone, very few if any cellular-telephone users would lock their telephone between calls. In the case of a portable telephone in use at a trade show, the same situation applies in that the telephone could be "boosted" while unlocked between calls.

By providing the cellular phone customer with the ability to control access to local, intra-state, interstate, and international calls using carrier services rather than depending on in-phone security measures, liability for stolen-phone fraud can then rest with the user or the customer of the phone as required. This is true in particular when dealing with rented cellular telephones, cellular telephones in rental cars, taxis, and limos, and with loaned phones.

This customer-set access control would provide a measure of security against cellular phones which have been cloned or with phones that are being tumbled.

I recommend that the Telecommunications Industry Association (TIA) be asked to prepare a standard for carrier-equipment-based access control, if such a standard does not already exist in the ANSI framework. Once such a standard has been created, then the Commission can determine if it is appropriate to reference such a standard in the Rules.

Such a standard should define how access control is handled and on what conditions access control shall be implemented. As a starting point, I suggest the following list: an "unlock code" at phone power-on; an access password for each outgoing call which meets certain protection criteria (local, intraLATA, interLATA, interstate, foreign), potentially with different access codes for each class of protected access; an access password requested randomly by the cellular carrier's switch on any call; an access password to answer calls; and an access password to use special features such as voicemail.

c—Intrusion alerts printed on the bill

In the event that an attempt is made to make a collect call, or to charge a third-party call or a calling-card call to a cellular number and that attempt fails for any reason, the operator services provider shall be required to provide a billing record of such an attempt. The OSP (or IXC) shall not charge for this billing record. The billing record shall include the originating telephone number and the destination telephone number. This specifically includes calls which are blocked because of LEC or cellular-carrier billing restrictions placed on the line.

11—Answers to Paragraph 36 Comment Request

I believe that the LECs, as owners of the LIDBs, are able to detect *potentially* fraudulent use and billing attempts; it's the customer, though, who must make the final determination.

a—typographical error in the NPRM

Picky detail: you use the word "customer" in the third sentence. The reference should be corrected to "IXC or OSP." To my knowledge, I as a customer have no direct access to the LIDB.

b—Intrusion alerts printed on the bill

It's a question of telling the telephone-service customer what is going on. In one respect, I as a customer know when a check with the LIDB returns a successful result: I get a line item on my telephone bill for the charge.

What if the LIDB check says to block the call? The customer is the only one who knows when a particular call attempt is a successfully block fraudulent call or a blocked call caused by human error. To facilitate early fraud detection, I propose the following:

In the event that an attempt is made to charge a collect call, a third-party-billed call, or a calling-card call to a telephone number and that attempt fails for any reason, the operator services provider shall be required to provide a billing record of such an attempt. The OSP (or IXC) shall not charge for this billing record. The billing record shall include the originating telephone number and the destination telephone number. This specifically includes calls which are blocked because of LEC billing restrictions placed on the line.

If the number of alerts for a single number grows significantly, the LEC can send an advisory letter to the customer at the time that the number of alerts exceeds a certain threshold. In addition, the LEC can use the information provided in the advisory to take action to curb the fraud and to assist law enforcement.

#### 12—Access by LEC to Source/Destination Telephone Numbers

[Paragraph 37] My proposal above says that the LEC would have access, and that no charge would be imposed for that information. The question as posed by the Commission, though, asks if queries to the LIDB should include source and destination telephone number information. I have no particular feeling one way or the other on this particular question, as long as the information about an intrusion attempt alert is transmitted as part of the standard billing system.

The advantage of having this information provided at the time of query is to ensure that a record of a failed attempt is made even if there is a billing problem or the OSP is not for some reason providing the intrusion attempt alert information.

13—Liability for LIDB Reporting Errors

[Paragraph 39] If the LIDB query return OK's a call when it shouldn't be, then the LEC should be held responsible for the error, and therefore liability should lie with the LEC. If the LIDB query return says "no" and the IXC or OSP lets the call go through anyway, then the IXC or OSP should be held responsible for the error, and therefore liability should lie with the IXC or OSP.

Part of the problem is that it may be hard to tell the difference. I suggest that the LEC, as part of the LIDB query reply, include an authorization number which then must be returned by the IXC or OSP as part of the billing data. This practice is common in commercial credit card operations to control billing errors and billing fraud on the part of the retailer.

Such a requirement will also point up quickly when an IXC or OSP does not take advantage of the LIDB database for fraud prevention. In the case of an IXC or OSP that does not subscriber to the LIDB service, any fraud liability should be borne by the IXC or OSP and not the LEC or the customer.

Again, the LEC can provide the lock, but the IXC/OSP has to turn the key.

14—Description of Proposed Rule Overly Broad

[Paragraph 40] I think the Commission should be applauded for its efforts in controlling toll fraud, but putting the requirement on every single Part 68 applicant to "provide warnings regarding the potential risk of toll fraud associated with the use of equipment" is excessive.

How can use of a modem expose a customer to toll fraud? A standard telephone set? An external ringer? An RJ-11 extension cord? An answering machine?

With this NPRM as background material in any litigation or pleading, I feel that the proposed Rule needs to be modified so as to say that no warnings are required by the Rule if use of the equipment does not increase the risk of toll fraud to the customer. I recommend that the Commission develop classes of Part 68 equipment, and for each class of equipment determine the toll fraud warning requirements. I also recommend that the Commission add language which states that for equipment which does not clearly fall into one of the classes specified in the Rule, that the vendor must either provide the warnings as required by the Rule or justify how the equipment does not contribute to toll fraud.

A starting point for the class list: interconnection equipment (no warning required), single-line set (no warning required), multi-line equipment with no cross-connect capabilities (no warning required), multi-line equipment with cross-connect capabilities (warning required), PBX equipment (warning required), central office equipment (warning required), and cellular equipment (warning required).

15—Answer to Paragraph 40 Comment Request

a—Language of warning shall be in non-technical, non-legal English

Nothing galls me more than to have to read a warning multiple times in order to understand it. If the only people who understand it are engineers and lawyers, then the warning is not serving its purpose and will be ignored by the customers. The Commission may not be able to mandate writing as clear as that found in the *Economist* magazine, but it can require that the warnings and supporting material be written such that a high school graduate can easily read and understand the material.

b—Warnings required for existing equipment

Subject to the modification I describe in point (14) above, I feel that existing equipment (1) subject to the requirements of providing warnings, (2) registered under Part 68, (3) which is still being sold by the original manufacturer shall be required to develop the necessary warning material and supplementary information within a "reasonable" time period. I proposed a time period of 120 days from the date notice is provided of the new Rule.

c—Minimal effect on existing registrations

Revoking registrations of any equipment should be considered a last resort, to be used only in the case of equipment providers who refuse to provide software and manual updates to existing customers at a reasonable price.

If the equipment providers were to share in the liability for toll fraud caused by defects in their equipment design or implementation, they would have an incentive to correct the problems in a timely manner.

d—LECs, cellular carriers to provide warning literature

If there is one focal point for knowing who might or might not be a potential victim of toll fraud, it's the entity supplying dial tone. Using the LECs and cellular carriers as distributors of information means that the customer, from the largest corporation to the retiree with "life-line" service, has a single place to go for more information.

Free information pertaining to residential and non-CPE business fraud could be provided at minimum cost by the LECs and cellular carriers, perhaps by publishing that information in the telephone books already provided each and every customer in the case of the LECs, or in the service book provided to cellular customers.

For larger business customers and customers of special services, and in particular PBX customers, fraud information could be provided at a nominal cost by the LECs.

Initial marketing of such information can be done using the monthly telephone bill, for all customers.

e—The Internet, Commercial On-Line Services, BBSes

If the LECs feel that the burden is too much for them to carry the message, there is always the computer community. The success of the FCC PAL (Public Access Link) for Part 15 registration information shows just how valuable a computer-based solution can be.

More and more businesses are "getting connected" into the Internet. Universities and other organizations providing Internet host services would be happy to add information on toll fraud to their collections, information which can be made available by "anonymous FTP" or by using a "gopher".

Commercial on-line services — CompuServe, GENie, America OnLine, BIX, Delphi, among others — would be happy to accept toll-fraud information and make it available without charge (other than standard connection charges). The CompuServe Information Service and BIX have strong special-interest sections on telephone equipment, and both would welcome and advertise the availability of toll fraud information. Other on-line service may have similar special-interest groups and places to store information for download.

The network of Bulletin Board Systems would also welcome information on toll fraud and make that information available for download. The growth of the FIDO and other interconnection networks for BBSes mean that information on toll fraud will spread rapidly.

I recommend that the Commission approach the Telecommunications Industry Association and ask them to write white papers, free from copyright royalty, on toll fraud. I would be happy to coordinate the posting of those white papers on both the Internet and commercial services, as well as seed the paper into the BBS community.

#### f—Encryption Between the Customer and Carrier

"Clip-on" fraud is possible because once a perpetrator gains access to the two (or four) wires of the circuit, there is no bar to his gaining access to the services available to the subscriber. Passive monitoring gains all the access codes and other protocols required because all that information is sent in the clear.

Encrypting the subscriber-to-central-office link robs the perpetrator of this valuable information, and makes the task of said perpetrator that much harder. Wiretaps ordered by a Court can still access information in the clear on the central-office side of such an encryption device.

This would be an added service over and above the service currently offered by the LEC to the subscriber. I would suggest that businesses, particularly business which deal in sensitive information (doctors, lawyers, banks, securities brokers, and law enforcement to name a few) and businesses which need to transfer trade secrets over telephone circuits would welcome such a service. By attractively pricing such a service, the cost increase to the LEC can be spread over a large number of users, further encouraging its use.

Payphone providers would welcome low-cost encryption so as to minimize payphone fraud using equipment external to the telephone.

The Commission has its choice of technologies to use. The Clipper system (using the SkipJack algorithm with law-enforcement tap capabilities) is starting to come on-line, and products are coming on the market. TIA TSSC TR-45 (cellular phones) has already incorporated into a standard the use of the RSA public-key encryption system with Diffie-Hellman key exchange and RC4 streaming cipher, and I'm in the process of creating a proposal to TIA TSSC TR-30 (data modems) to use the same technology for an in-modem encryption standard.

I recommend that the Commission ask the Telecommunications Industry Association (TIA) to develop a standard for subscriber-loop and PBX-trunk encryption, unless such a standard already exists in the ANSI framework. Once such a standard is in place, then the Commission can investigate whether to reference such a standard in its Rules and Regulations.

#### g—Role-Playing Game as Fraud-Fighting Training Tools

Russell Brand, a security consultant to the computer industry, developed a role-playing game for system administrators of Unix and other multi-user dial-in computer systems. In this game, Russell sets up an environment where computers set up to perform specific functions become targets for "crackers" and cyber-vandals, and the job of each player-administrator is to do what they can to: protect their system; detect the cracking activity; close the barn doors; deal with the howls of the users as certain handy functions are shut down due to their risk for cracking; and always, always, always deal with the mess the cyber-vandals leave behind.

Each game is run as a seminar, with a security expert setting up the situation and a collection of "bad guys" with varying skill levels and experience in cracking computer systems. Player-administrators are allowed to discuss things with each other—it happens in real life, so it should happen in the game.

Throws of dice (or other random-number source) dictate the actions of the phantom players, the results of actions taken by the administrators, and any "collateral damage" which may occur because of a break-in or because of administrator action. During each "turn" the player-administrators are told of certain events, such as system alarms from software they've installed, specific items from reports they have generated, telephone calls, and visits from the boss. The player-administrator then specifies certain actions to be taken. Some results happen instantly, while others (because they take a while to implement) don't show any effect until the next turn. In the games I've played, each turn represents a half-day of computer system operation.

I've "played" this game several times at several conferences where Russell has set up sessions. I can say that one hour sitting at a desk sweating taught me more about Unix system security than sixteen hours of book reading. The first time I played the game (I was responsible for a VAX connected to medical equipment) a patient died. The second time I was able to keep the cracker out, but at the expense of not getting *anything* done for my mythical employer.

The role-playing game teaches many things: basic security techniques for specific operating systems; what reports to get, how to get them, and how often to get them; how to spot suspicious action; how to audit the system to catch an otherwise undetected break-in; and most important, how to balance security actions with user needs.

Russell's technique of having the administrators in a role-playing game has an interesting side effect: the administrators need not be exposed to exactly *how* the perpetrators are breaking in. Hence, Russell's game cannot be used as a "finishing school for crackers" because no cracking techniques are revealed. The fixes are couched in the form "you need to replace the finger(1) program with one that doesn't allow access" without specifying exactly how the finger(1) program is broken or how to take advantage of the flaw.

PROPOSAL: I feel that similar role-playing games can be developed for toll fraud and related issues. Preparing such a game would require an expert who is well-versed in current fraud techniques to set up situations and then "hand control" over to the players. Such a role-playing game can be extended to become a simulator for equipment and software vendors to examine just how easy and effective such products are at stopping fraud.

I would particularly encourage PBX vendors to consider setting up such a game on computers as part of a seminar on operating and administering the equipment. This sort of a game, which interacts with the user with the same administration tools the customer would use every day with the product, would provide valuable hands-on experience, as well as familiarizing the administrator with the fraud detection tools in the equipment.

In closing, the role-playing games would get across three messages: fraud happens; fraud can be detected; fraud can be beaten. The participant learns *how* to detect fraud, and *how* to beat it and protect against it; it's the school of hard knocks, but the wounds are imaginary—the lessons are real.

#### 16—Commenter's Conclusion

I believe that the actions already taken by the Commission represent a good start toward identifying the disease known as "toll fraud" and have started to find measures to treat the symptoms. Like cancer, I suspect that a magic cure is not going to be found in the short term, and perhaps not in the long term, either.

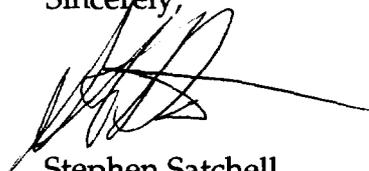
I feel that any emphasis on toll fraud must concentrate on getting as much useful information, and information in a useful form, to the *customer*. Technical advances in the network itself has reduced in all cases, except cellular, fraud against the carriers themselves. . . and the Commission has already taken steps to reduce cellular-carrier fraud.

[End of comments]

If anyone wishes to reply directly (and informally) to this comment, please send U.S. Mail to the address shown on the first page, or send email to any of the following Internet addresses:

70007.3351@compuserve.com  
ssatchell@bix.com  
sts@well.sf.ca.us

Sincerely,

A handwritten signature in black ink, appearing to read 'Stephen Satchell', with a long horizontal line extending to the right.

Stephen Satchell  
Incline Village, NV