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

**PUBLIC NOTICE**

**Released: June 9, 1992**

## CONSUMER ALERT
## TELECOMMUNICATIONS TOLL FRAUD

**Second in a Series**

Unfortunately, telecommunications fraud is not a new problem. It existed in the past, exists today, and continues to move to new technologies. Any person or business -- large or small -- can fall victim to toll fraud. Every day calling card numbers are being stolen, private branch exchange (PBX) systems are being used fraudulently to make calls across state lines or to foreign countries, and people claiming to be law enforcement officials or telephone company representatives trick unsuspecting consumers into accepting the charges for calls or divulging their calling card numbers. These fraudulent calls may mean large telephone bills for unsuspecting consumers.

While the Commission and the telecommunications industry are working together to develop solutions to this problem, consumers also need to be involved. We urge consumers to take preventative steps *now* to avoid possible financial losses from fraud associated with telephone services and equipment.

This Consumer Alert outlines different types of toll fraud, identifies steps consumers can take to detect it and lessen their chances of becoming victims, and informs consumers what they can do if they become victims of toll fraud.

### WHAT ARE SOME EXAMPLES OF TOLL FRAUD?

**Private Branch Exchange (PBX) Fraud - Remote Access**

Businesses that use private branch exchange (PBX) equipment may be vulnerable to toll fraud through remote access features in their equipment. Remote access features allow business employees who are away from the office, such as sales agents in the field, to call the PBX and then, after entering an authorization code, receive a new dial tone for an outgoing call that will be billed to the outgoing telephone line connected to the PBX. In some cases, an 800 service call may be used for the incoming call to the PBX. Unauthorized people may use computers to call a PBX and to test random authorization codes until the correct one is found. Once the correct authorization code is found, calls can be made that will be billed to the PBX owner. If an incoming 800 line has been used, the PBX owner may be billed for the 800 calls as well.

**Voice Mail Fraud**

Voice mail users can be victims of toll fraud. Some voice mail systems may have features that provide a link to a PBX remote access feature or that give a caller a dial tone after the main voice mail function has finished. These features can be used to make outgoing calls that will be billed to the voice mail user or PBX owner. Unauthorized people may attempt to use a voice mail system to arrange third number billing to the telephone number served by the system.

**Calling Card Fraud**

Many consumers use local or long distance telephone company-issued calling cards. Unauthorized people may try to obtain calling card and personal identification (PIN) numbers by watching callers dial their numbers or by overhearing them read to an operator at a public pay telephone. They also may call people at their home or business requesting number verification. Cards also may be lost through theft or loss of a wallet or purse.

**Third Number Billing Or Collect Call Fraud**

Sometimes unauthorized people pose as FCC, telephone company, or law enforcement officials and ask the subscriber to accept billing for calls as part of a "sham" investigation. Telephone company operators unwittingly can be used by unauthorized people to place fraudulent calls. The unauthorized person may tell an operator to bill a call to a third telephone line, such as a line serving a pay telephone or a line serving a PBX, or may use a pay telephone to accept collect calls. Unauthorized people also may attach calling devices directly to a telephone line and then place outgoing calls or accept collect calls that, in both cases, would be billed to the subscriber of the line.

### WHAT CAN BUSINESSES DO TO PROTECT THEIR SYSTEMS FROM TOLL FRAUD?

1) Contact your equipment vendor, your local telephone company, and your long distance telephone company to determine what security systems are available to protect your equipment and telephone service from toll fraud, and what monitoring services are available to help you quickly detect unusual usage.

2) Determine if your authorization codes are susceptible to fraudulent usage. Many long distance carriers recommend that you use as many digits in these codes as possible. Changing access codes frequently also is recommended.

3) Take steps to safeguard the security of your authorization codes. Regularly remind employees of the need to keep codes secure. Remove codes from voice mail bulletin boards; do not write codes on credit card receipts; do not provide codes to unknown callers; and delete all unneeded codes, including default codes installed by the equipment manufacturer.

4) Disable any part of your system that is not in regular use.

5) Consider disabling your system during non-business hours.

6) Ask your equipment vendor and local or long distance telephone company about limiting international calls or blocking calls to countries that you do not normally call.

7) Consider using a voice recording, rather than a steady tone, to signal when to enter an authorization code.

**HOW CAN CONSUMERS PREVENT UNAUTHORIZED PEOPLE FROM OBTAINING THEIR CALLING CARD NUMBERS?**

1) Whenever possible, use a telephone that reads your calling card number from the magnetic strip on the back of the card. If this type of telephone is unavailable, take steps to prevent others from watching you dial your number or overhearing you give your number to an operator.

2) Immediately report a lost or stolen calling card to the local or long distance telephone company that issued it. The company will cancel your card and issue you a new one.

3) Avoid using your telephone calling card as identification for consumer purchases or cashing checks.

4) Do not provide your card number to unknown persons. Telephone companies already have this information for their calling card customers and therefore would not ask you for your number.

5) Educate cardholders with whom you share cards on how to protect their card numbers. Emphasize the need not to disclose the numbers to other people.

**ARE CONSUMERS RESPONSIBLE FOR PAYING UNAUTHORIZED CALLING CARD CHARGES?**

Your liability for unauthorized use of a calling card can be as much as $50 under the Truth in Lending Act and Federal Reserve Board regulations. You should *immediately* contact your local or long distance company to discuss the charges *and* to cancel your calling card if an unauthorized person has obtained your calling card or calling card number.

**WHAT ACTION SHOULD CONSUMERS TAKE IF THEY SUSPECT THAT A CALL IS A TOLL FRAUD ATTEMPT?**

1) Advise the caller that you are going to call the telephone company yourself to make sure that a problem exists.

2) Immediately hang up and call your local telephone company or the long distance telephone company identified by the caller to determine if a problem exists with your telephone line or telephone bill. You also may wish to contact the company's security office.

3) Never accept third number billing or collect calls unless you are absolutely certain of the caller's identity and the purpose of the call.

4) If you do not normally accept third number billing or collect calls, you may wish to discuss with your local telephone company a blocking service for your line to prevent such calls from being billed to your number.

5) Contact local or federal law enforcement officials.

**WHAT IF CONSUMERS HAVE ACCEPTED THE CHARGES FOR SOME FRAUDULENT CALLS?**

You should contact your local telephone company and the long distance company identified on your bill as the carrier of the fraudulent calls. You may also contact local or federal law enforcement officials. You should make these contacts as soon as you realize that something suspicious has happened.

**WHAT FEDERAL LAW ENFORCEMENT AGENCIES CAN CONSUMERS CONTACT IF THEY BECOME VICTIMS OF TOLL FRAUD?**

Consumers can contact the Federal Bureau of Investigation (FBI) by writing to the FBI, 7799 Leesburg Pike, South Tower, Suite 200, Falls Church, VA 22043. The FBI and the Electronic Crimes Division of the United States Secret Service jointly investigate telecommunications fraud.

**HOW CAN CONSUMERS KEEP UP-TO-DATE ON TOLL FRAUD ISSUES?**

The FCC seeks to keep consumers advised of developments in the telecommunications industry by issuing public notices or fact sheets. The first *Public Notice* addressing toll fraud was released by the FCC on April 19, 1991. Copies of the *Public Notice* can be obtained by writing to the FCC, Informal Complaints Branch, 2025 M Street, N.W., Suite 6202, Washington, D.C. 20554.

**WHAT IS THE TELECOMMUNICATIONS INDUSTRY DOING TO PREVENT FRAUD?**

The major long distance telephone companies have established fraud prevention programs and are actively working with their customers to assist them in protecting their telecommunications systems and services from fraud. You should contact your long distance telephone company for specific program offerings.

**WHERE CAN CONSUMERS GET FURTHER INFORMATION ON TOLL FRAUD?**

The Communications Fraud Control Association, a nonprofit organization, serves as a clearinghouse for consumer information and complaints regarding toll fraud. This association is located at 2033 M Street, N.W., Suite 402, Washington, D.C. 20036 (telephone: (202) 298-8900).

**DOES THE FCC HANDLE COMPLAINTS INVOLVING TELEPHONE BILLINGS FOR FRAUDULENT CALLS?**

Yes, the FCC does have authority to handle complaints that involve billing disputes that arise from acts of interstate or international toll fraud. You should *first* call your local telephone company if the billing page was included with your local telephone bill or if the long distance company was identified on the billing page. If you are unsuccessful in your attempts to resolve the complaint yourself, you can file a complaint with the FCC. A copy of the telephone bill or bills listing the disputed charges should be included with the complaint. There is no special form to fill out. You can simply write a letter in your own words to:

Informal Complaints and Public Inquiries Branch
Enforcement Division, Common Carrier Bureau
Federal Communications Commission
2025 M Street, N.W. - Suite 6202
Washington, D.C. 20554

FEDERAL COMMUNICATIONS COMMISSION