



Exploding The Phone

db570

www.explodingthephone.com

Bibliographic Cover Sheet

- Title** **AT&T memo/backgrounder on toll fraud**
- Date** 1977-05-18
- Abstract** Backgrounder paper (possibly press handout, or briefing for Bell System media relations people) on toll fraud. Discusses electronic toll fraud, credit card fraud, and third number fraud. Provides statistics on number of arrests, convictions and recoveries for electronic toll fraud from 1972-1976.
- Keywords** toll fraud; blue box; red box; black box; credit card fraud; toll fraud

The following pages may contain copyrighted material. We believe that our use of this material for non-commercial educational and research purposes constitutes "fair use" under Section 107 of U.S. Copyright Law. If you wish to use this material for purposes that go beyond "fair use," you must obtain permission from the copyright owner, if any. While it will make us slightly sad to do so, we will nonetheless comply with requests from copyright owners who want their material removed from our web site.

5-18-77

file

TOLL FRAUD

Background

Toll fraud imposes a big financial burden on the telephone industry and its honest customers. The three principal types of toll fraud are credit card, third number, and electronic.

The chief tool of electronic fraud is the so-called blue box (it's called that because in 1961 the first one found was blue). This electronic toll fraud device looks like a simple metal box with 13 pushbuttons. Each button produces a distinct tone. Besides the 10 pushbuttons that represent the 10 numbers on any dial or Touch-Tone® phone, there are three others that control network signalling. Because the tones that activate most telephone equipment are carried over the same circuits people speak on, a blue box user can do just about anything a long distance operator can.

Blue boxes are used by the calling party. Blue box users avoid being billed for their calls by getting into the long distance network on a legitimate toll-free number (or by making a short haul toll call). Once into the network they use their blue boxes to disconnect themselves from the number they've dialed, seize the circuit, and then connect themselves with any other number they wish, virtually worldwide.

Today, there is an arsenal of weapons being introduced to give preliminary indications of blue box usage, running from the time-consuming check of computer printouts of Accounting Office AMA tapes to more sophisticated and swifter methods, up to immediate detection of the calling and called lines by using advanced computer systems.

Other electronic devices include the red box and the black box. The red box generates sounds akin to those associated with the insertion of coins by the long distance caller into a coin telephone. The possibilities here of fraud are obvious. The black box is an electronic device that, when connected to a telephone receiving a long distance call, prevents charge information being registered against the calling telephone.

We estimate blue boxes can be mass-produced at a cost of \$25 to \$50 per unit, and black boxes at a cost of a dollar or less. Experience has shown that these devices most often appeal to the criminal element, whether it be a member of organized crime or an unprincipled businessman. This is so because not only is payment of telephone charges evaded, but also any record of the communication concealed, permitting users to conduct their unlawful activities anonymously.

Credit card fraud is much simpler to commit. Since no device is required it is practiced by a broader segment of the general public. Hints and outright advice on how to escape credit card charges appear, not only in the underground press, but also in national and regional magazines and newspapers.

In 1971 the credit card numbering system was revised to provide the operator with a validity check within the number. TSPS has been arranged to automatically make credit card validity checks.

The federal laws relating to "fraud by wire" are tough and explicit. The cover electronic, third number, and credit card fraud. Conviction under the federal law carries a penalty of up to five years in prison and a fine not to exceed \$1,000 or both. Virtually all states have similar criminal statutes, with varying penalties.

Sixteen states have passed laws making it illegal to publish a credit card number or the codes for forming a credit card number with the intent that it be used, or with reason to believe that it will be used, to avoid payment of lawful charges. "Publish" as defined by the laws includes

oral communication, in person or by telephone, radio or television, or in writing of any kind.

Due to the nationwide character of such fraud, the Bell System is vigorously supporting an amendment to the Federal Omnibus Crime Control Act which would prohibit the manufacture, assembling, possession, sale or other distribution, of electronic toll fraud devices. Such a statute would also prohibit the publication of any advertisement of devices for the theft of service. Some 35 states have already passed laws of a similar nature.

Status

Currently, all forms of known toll fraud losses mount up to about \$15 million a year (credit card \$8.3 million, third number \$6.7 million, electronic \$1 million).

However, this amount of electronic toll fraud may represent only the tip of the iceberg since we cannot be fully certain how much undetected fraud takes place. It has been estimated that the actual amount of electronic toll fraud may be ten to twenty times greater than that detected.

Most media interest is in electronic toll fraud, most probably because of its novelty and previous notoriety. One of the most often asked questions, aside from the dollar loss, is the number of people we have caught and the number of boxes recovered.

For example, Bell System electronic toll fraud experience over the past five years is as follows:

	Arrests	Convictions	Blue Box	Recovery Black Box
1972	57	26	59	8
1973	119	66	217	29
1974	158	54	174	19
1975	176	121	205	12
1976	160	144	168	21

Credit Card, Third Number, and Other Fraud

	Arrests	Convictions
1972	1023	848
1973	978	857
1974	733	657
1975	834	728
1976	931	828

To counteract widespread credit card fraud the 1971 credit card number format was revised to provide the operator with a validity check within the number. Further changes were made in the 1972 number format. The introduction of TSPS has also inhibited this kind of fraud.

As more stringent preventive procedures have gone into effect, and as the System continues to prosecute offenders with the attendant publicity, credit card fraud has been reduced.

Policy

Bell System companies vigorously prosecute fraud offenders and publicize these cases. In addition, major steps have been taken and are continuing to be taken to protect the integrity of the credit card numbering plan and combat electronic toll fraud.

As a last recourse, to obtain sufficient evidence to prosecute cases of electronic toll fraud, limited recording of the connection and start of some calls have to be made for presentation to the courts. Recordings are only made of calls known to have been illegally placed, and solely to identify the thief and establish that the fraudulent call was completed. Further, they are not made until the possibility of plant trouble has been ruled out and all other investigative measures exhausted.

Further, each recording must have the prior approval, under Bell System practices, of the Vice President/Operations and the Vice President/General Counsel.

The recording begins only when the caller's "blue box" emits a special tone to illegally seize the line. The recording is brief -- the fraudulent dialing, the ensuing ringing, and the opening salutations of the parties -- usually only 60 seconds or less of conversation.

Virtually all cases are prosecuted in which evidence of electronic toll fraud is gathered. In these criminal cases, our entire process of gathering evidence (including the limited recording done) has been subjected to close judicial scrutiny. With virtual unanimity, the courts have held that the methods used have been lawful.

With reductions in credit cards fraud losses in recent years, third number billing losses are increasing. Constant scrutiny of these losses is maintained. Preventive measures to deter this type of fraud are costly and must be measured against the potential dollar losses.