



# ***Exploding The Phone***

db514

www.explodingthephone.com

Bibliographic Cover Sheet

Title	<b>Training Key 193: Fraudulent Telephone Calls</b>
Date	1973-00-00
Author(s)	International Association Chiefs of Police
Abstract	Training guide regarding fraudulent telephone calls published by the international Association of Chiefs of police. Describes black boxes, blue boxes, cheese boxes, red boxes, and credit card fraud.
Keywords	Black box; blue box; cheesebox; cheese box; red box
Source	Anonymous

*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.*

# Fraudulent Telephone Calls



Through trickery, fraud and misuse of electronic devices, thousands of unrecorded and unpaid telephone calls are made each year. Police officers should realize that fraudulent telephone calls are often linked to other crimes. Gamblers, organized crime figures, and other criminals make fraudulent calls in order to avoid a traceable record of their communications. In addition, many other unscrupulous individuals foreseeing a ready market have embarked upon the manufacture and sale of electronic toll fraud devices in the last few years.

## Training Key®

#193

The practice of making fraudulent telephone calls usually has implications that go beyond merely "ripping off Ma Bell." People who go to the trouble of concealing telephone calls often have more compelling reasons for doing so than just saving the cost of the call. Generally, they are more interested in avoiding any traceable record of the call.

Fraudulent telephone calls are made by gamblers, organized crime figures, members of revolutionary groups, and so-called "phone freaks." This last category includes a small number of skilled individuals who enjoy defrauding the telephone company in technologically complex ways. Phone freaks rarely derive any monetary gain from their fraudulent calls. Instead, they use electronic devices to place expensive calls merely for the "sport" or entertainment of accomplishing the feat without being charged. These same electronic devices can be used by criminals to make unrecorded long distance calls or to conceal locations where calls are being received.

All fraudulent calls are not made with electronic devices. Credit card numbers are often falsified to obtain free telephone service. Several "anti-establishment" publications have provided readers with the basic information needed to make fraudulent credit card calls. Some underground newspapers, available in most large cities, routinely inform readers of the latest scheme devised to obtain free telephone service. Some of these underground publications have printed detailed instructions for building illegal electronic devices. The "black box", the "blue box", and the "cheese box" are three devices used to make fraudulent telephone calls.

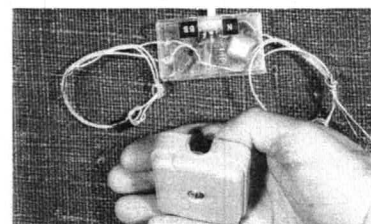
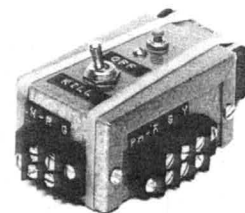
### Black Box

The so-called black box is an electronic device that permits the owner to receive calls without the caller having to pay for the service. Essentially, the black box consists of resistors connected in series to create a condition on the line that misinforms the telephone

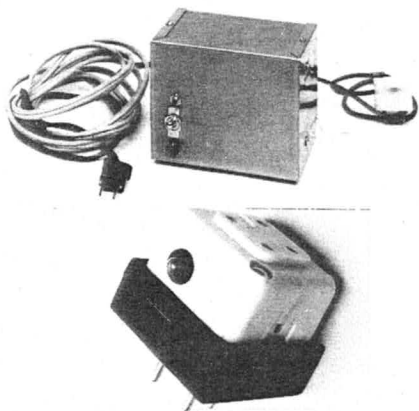
company's automatic equipment that the call has gone unanswered when, in fact, the connection is complete.

Of all illegal electronic devices used to defraud the telephone company, the black box is probably the simplest to construct. Plans for black box construction have been published in several underground newspapers, and the devices are popular among anti-establishment groups. Gamblers also use the black box to prevent any record being made of long distance calls to their location.

In operation, the black box has certain limitations. It is functional only on the receiving end of a call. It cannot be used to make illegal calls, only to conceal incoming calls. When a black box is connected to a receiving set, the telephone ringing device does not function. Therefore, the receiver of the call cannot be summoned to the phone by a caller. He must expect a call at a given time, or he must watch the black box for a visual indicator from the resistors when the incoming call is received. Of course, the caller can remain on the line indefinitely after the call has been received by the black box, so the timing needn't be exact. For instance, if the owner of a black box is a few minutes late for an expected long distance



Black Box



*Black Box*

call at 8 P.M., the black box can hold the line open. A few minutes later, when the owner of the black box lifts the receiver, he is immediately in contact with the caller who has been holding the line.

The black box is not necessarily black. (Color designations for electronic devices have historical reference to the color of the original illegal devices discovered.) A black box can vary in size from a shoe box to a pencil. It can be made to fit within a standard junction cap identical to those used by legitimate telephone installers. It can be installed within the handle of the telephone receiver itself. At times the black box is housed in a transparent case or beneath a removeable cover so that visual signals of incoming calls can be observed. This is accomplished by using a neon tube which will light up when someone rings the telephone line.

In most cases the black box will contain an on/off switch which permits normal ringing. Operating the switch to ON prior to lifting the telephone handle will stop the ring and give the caller a free unrecorded call. Black boxes without a switch may also have a jack plug for easy removal from the telephone line to restore normal incoming service. The off/on switch is the most prominent identifying characteristic of the black box that can be observed by police officers.

## *Blue Box*

The blue box is a sophisticated electronic instrument which permits the user to make telephone calls free of charge without creating any true record of the communication. The blue box is the most difficult illegal electronic device to build. Essentially, the blue box reproduces the precise electronic signals that are used by the telephone company to guide and control its own automatic equipment.

Once the blue box becomes operative, the illegal caller directs these signals to automatic sensing devices within the telephone company system. By transmitting key sounds from the blue box into the telephone system, the caller gains control of the company's automatic equipment and is able to place his calls wherever he wishes.

Blue boxes are often used by "phone freaks" who delight in making complicated long distance calls to demonstrate their control over the equipment. Expert phone freaks can easily dial a public phone booth in London for idle conversation with whomever answers.

Organized crime figures purchase blue boxes and use them to place calls to various parts of the nation. Interstate gambling operations make use of blue boxes to hold long distance lines open for hours without paying



*Blue Box*

for the service or creating any traceable record of communications. Virtually anyone who has a need for frequent use of telephone service for illegal purposes can benefit from possession of a blue box.

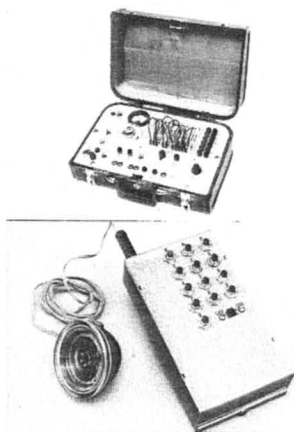
Because it is a complicated piece of equipment, the blue box is also expensive. Presently, the typical selling price for a blue box is \$1,500. Technological improvements (such as miniaturization) keep the price high for the latest models while increasing availability of "old" technical information makes cruder products more available.

The blue box is not always blue. It may range in size from something that fits inside a suitcase to something that fits inside a jacket pocket. The only common identifying characteristic is the presence of at least 13 keys on the box, which are depressed to produce certain sounds. Each key develops a different electronic emission. For instance, an important key is one that produces a tone frequency that is used to initially seize control of long distance lines by misinforming automatic equipment that a legitimate call is forthcoming. Other keys produce tones at various frequencies that correspond to codes used for specific numbers.

A call made with a blue box does not go entirely unrecorded. The initial call made to gain access to the system (usually to a toll-free 800 number) is recorded, although subsequent calls made with the blue box remain off the record. Because repeated lengthy calls made from the same number to toll free numbers could call attention to the user of the blue box, the illegal caller usually prefers to use a public telephone booth. Calling from a public booth removes the possibility of any permanent record involving an individual's personal phone, but it also places him in a position where he is vulnerable to alert police patrol.

For instance, one arrest was made when the manager of a hotel called police and said, "Every night this nut comes into my lobby, goes into the phone booth, and plays a musical instrument." When officers investigated, they apprehended a man using a blue box.

To operate the blue box, the device must be placed over the mouthpiece of the telephone. While held in this position, the tone producing keys are depressed. Officers should become familiar with the appearance of a typical blue box and be alert to persons who are seen repeatedly using public phones for long periods of time. Officers should know which local laws are violated by the use of this kind of equipment and be prepared to make a proper charge. If the officer discovers a blue box, he should attempt to determine the purpose of the call. When known criminals who are associated with organized crime groups are found in possession of a blue box, the discovery could have far reaching implications.



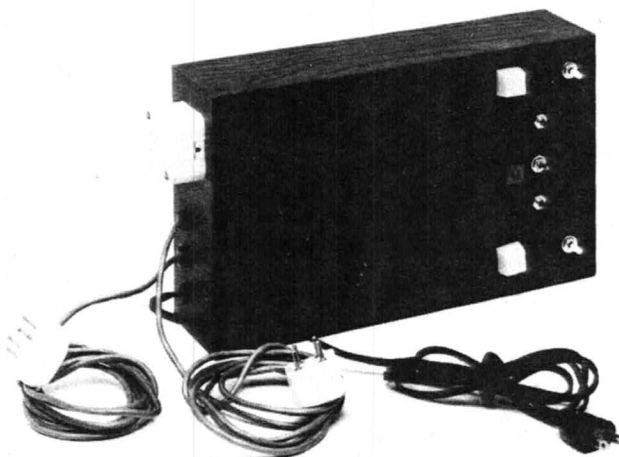
Blue Box

## Cheese Box

The cheese box is basically an automatic transferring device. It is often used by bookmakers to disguise the location where gambling calls are being received. The cheese box automatically switches a call received by one phone onto the line of another phone, thereby permitting a listener at a remote location to receive the message.

The name "cheese box" is derived from the size of the first such devices that were discovered (roughly 4" x 4" x 12", a size commonly used to package cheese). At present, a cheese box can be as large as two shoeboxes or as small as three or four flashlight batteries wrapped in tape. Usually, the cheese box is not visible at all from the location where the "dummy" phone is located. The presence of the cheesebox must be deduced from other situational factors at the scene.

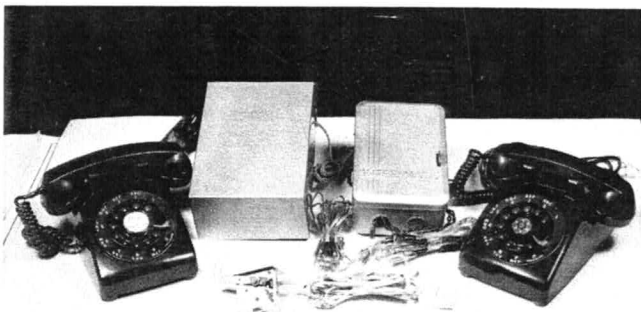
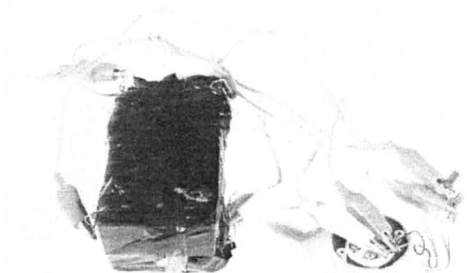
For instance, it is necessary to have two telephones with different numbers installed at the same location in order to have an operational cheese box. When officers note the presence of two or more telephones at locations that do not appear to warrant the service (such as an empty office or a small, dingy apartment) reasonable suspicions would be aroused.



Cheese Box

The cheese box can be located at the central terminal box in the building or at some other location remote from the phones themselves. It may be in an adjoining room. Cheese boxes even have been installed inside walls to avoid discovery. Wherever the device is located, it must be connected by wire to the telephone. Any secondary wiring connected to a telephone should be tracked by investigating officers. If the officer lacks the technical expertise to recognize a cheese box and disconnect it, he should obtain assistance from the local telephone company. The telephone company will cooperate with the officer by performing whatever technical services are required to conduct a thorough search.

The use of a cheese box in a gambling operation is a complicated process. For instance, bettors in a gambling operation are instructed to call a particular telephone number during certain hours to place bets. A few minutes before incoming calls are expected, the writer or bookie places a call from an unknown location to the *second* telephone installed at the cheesebox location. The number of this second phone is unknown to callers. The gambler holds this line open for the entire period of time that he



Cheese Box





expects to receive calls. Incoming calls received on the *first* telephone are automatically relayed onto the *second* line which he is holding open. The gambler's phone does not ring to signal incoming calls. New callers simply come onto the line and place their bets as they are automatically transferred by the cheese box at the dummy location.

When police officers discover the number being used to contact the bookmaker, an investigation of the premises where that telephone is located will reveal only the dummy office or apartment. An effort to trace calls from the dummy location to the gambler himself cannot progress until the number of the second phone is known.

Technically, there is no reason for the gambler to be anywhere in the vicinity. He can be miles away. In practice however, the gambler is often located not far from the dummy phone. He may be elsewhere in the same building or in an adjoining building. This is done because the cost of a good cheese box is quite high, and the equipment is worth saving. If a raid is made on the dummy premises, the gambler usually will attempt to salvage his expensive equipment before it is discovered by police. If the police are raiding the office or apartment and the cheese box has been installed in the basement, the gambler may attempt to remove it.

## Other Devices

Other electronic devices are also used to defraud the telephone company. Good quality tape recorders have been used to record the electronic tones produced by the telephone apparatus to designate specific long distance numbers. When these same tones are played back into the telephone, the call can be made without paying the normal service charge. This technique is common among students who record numbers that are called repeatedly (for example, calls to girl friends or to their own families.)

Another device that is now being used on college campuses is the so-called "red box". This device duplicates the sounds produced by coins as they fall into a coin operated telephone. An individual who places a long distance call can use the "red box" to falsely indicate that he has deposited the proper amount of coins into the telephone to receive service.

## Credit Cards

The introduction of the telephone credit card has made possible numerous schemes to obtain service without paying for it. Alert police patrol officers can collect evidence of credit card misuse and even apprehend suspects in the act of making fraudulent calls when notified promptly by telephone company officials.

Seventy percent of estimated losses suffered by the telephone company from fraudulent calls are attributed to improper use of credit card numbers.<sup>1</sup> Some of these illegal calls are made with numbers that have been overheard or copied from legitimate credit cards. A much larger percentage of calls are made with composed false numbers.

In order to use a credit card to obtain telephone service, the caller merely gives his credit card number to

<sup>1</sup>"Crime by the Numbers", National District Attorney's Association, 1972, p.1.

<sup>2</sup>Training Key # 188, "Credit Card Investigation," contains detailed information about other types of credit card crimes.

034-Va 703  
024-N.Y. 212  
042-Md. 301  
Do not use  
117-4195-034-W  
453-9286-042-S  
O.K.  
356-1234-034-W  
192-7689-042-T  
O-A  
3-S  
4-T  
5-W

119-4532-042-S  
973-1248-042-S  
356-1234-034-W

Typical Lists of Fraudulent  
Credit Card Numbers

the operator and requests that charges for service be applied to that account. There is no face-to-face confrontation at the point of sale as there is with other credit cards. Nor is there any opportunity for the telephone operator to check a signature or other means of identification.<sup>2</sup> It is a simple matter for anyone who knows the basic style of numbering used on telephone credit cards to manufacture a number and try it out on a coin operated telephone.

Telephone companies have taken some steps to protect themselves against this type of fraud. The credit card number usually includes a code that can be verified by the operator. For instance, a letter that appears somewhere in the credit card identification may have to match up with a number appearing elsewhere; the letter "B" in the suffix may have to match the number "2" at some other position. This code is changed periodically.

This kind of security code probably limits the number of fraudulent calls that are made, but it is insufficient to prevent the problem. Information about security codes and methods to circumvent them quickly becomes known. Information of this kind is often published in "anti-establishment" newspapers and magazines accompanied by sample numbers that can be used to obtain free service.

Another preventive measure used by the telephone company is distribution of a "hot list" of fraudulent numbers used frequently. Telephone operators are instructed to check this list while placing the call. Recently, the telephone companies also initiated a computer verification check in some areas that can be used to detect records of fraudulent calls much earlier so that they can be quickly investigated.

## Arresting the Caller

The following advice concerning fraudulent telephone calls has been published in underground newspapers:





- (1) Use a coin operated public telephone. (2) Do not use the same credit card number too often. (3) Keep the calls short.

These techniques, which fraudulent users employ, help determine the appropriate police response to the problem. (1) The call will be initiated from a public place, which makes it possible for officers to apprehend the caller when they are promptly notified by the telephone company that a fraudulent call is in progress. (2) Because the caller does not want to use the same number too often, he will probably have a list of alternate credit card numbers in his possession which can be collected as evidence. (3) Because the calls are brief, police must be ready to act promptly when a request for assistance is received.

At times when telephone company security officers are making special efforts to locate fraudulent callers within a jurisdiction, police officers will probably be alerted to expect requests for assistance at telephone booths where fraudulent calls are in progress. Such requests should be answered promptly.

As police officers approach a telephone booth where a fraudulent call is in progress, the caller will probably hang up the receiver. Since the operator is aware of the fraudulent call and has requested police assistance, she will probably hold the line open for a short time. The officer should immediately pick up the receiver of the phone to re-establish contact with the telephone operator. The officer should identify the telephone number where he is speaking. When the operator verifies that the fraudulent call was made at this location, the suspect can be arrested. The officer should obtain the name and number of the telephone operator and carefully note the telephone number and the time of the arrest. This information will later be compared to telephone company records of the fraudulent call.

When the suspect has been taken into custody, an authorized representative of the telephone company should be instructed to meet the arresting officer at the police station to sign a formal complaint. The effort to deter fraudulent calls depends on vigorous prosecution of offenders. Although the amount of money lost because of a fraudulent call may appear small to the arresting officer, telephone companies are concerned about total annual losses from this practice. Vigorous prosecution is the most effective means to deter fraudulent callers.

## Continue the Investigation

The investigation of fraudulent use of the telephone does not end with the arrest of the suspect. The investigation should always be broadened to include the means by which the electronic device or the credit card number was obtained. Continuation of an investigation of fraudulent telephone calls can develop leads for solving other crimes. The credit card may have been stolen during a burglary or robbery. The electronic device may have been obtained from persons involved in the illegal manufacture of such devices. The fraudulent call investigation may contribute to an organized crime investigation, or it may develop into an investigation of a major gambling operation.

During the course of the investigation, police officers should not hesitate to contact telephone company security officers for information about telephone frauds. These security officers will assist in the apprehension and prosecution of persons fraudulently using telephones. They are experts in their field, and their records and abilities can provide valuable assistance for establishing links to other crimes.

## Discussion Guide

1. The subject of wiretapping is charged with emotion and prejudice. The term "wiretap" is often equated with flagrant invasion of privacy, thought control, and repression. This has been so since the first public uproar on the subject, which occurred in 1916 when a committee of the New York State Legislature investigated wiretapping by the New York City Police. Briefly review wiretapping.

A. Wiretap provisions are contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

(1) Prohibited:

... wiretapping and electronic surveillance by persons other than duly authorized law enforcement officials engaged in the investigation of specified types of major crimes after obtaining a court order.

... manufacture, distribution, possession and advertising of wiretap devices by private parties where the mails or interstate commerce are involved.

(2) Permitted:

... controlled use of wiretapping by law enforcement authorities in certain heinous crimes often associated with organized syndicates, such as murder, kidnapping, extortion, and certain bribery and narcotic offenses.

... a specified due process of law to control the use of wiretaps.

... during emergencies a wiretap can be established without court approval for up to 48 hours.

... monitoring or taping conversations on one's own phone, or tapping a telephone of another who has consented is lawful.

B. Wiretap control as outlined in the Omnibus Crime Bill

... Secure a court order from a judge.

... Show probable cause.

... Particularize the offenses under investigation and the type of conversations expected to be overheard.

... Limit the time period of the surveillance.

... Terminate the wiretap when the stated object is achieved.

... Renew the wiretap by showing continued probable cause to renew authorization.

... Show that normal investigative procedures have been tried and have failed, or that they are too dangerous to be used.

... Show why the objective would be thwarted if the person to be overheard were notified of the wiretap.

... Report the results of each wiretap.

C. Private Investigators

... Private detectives who engage in illegal electronic or wiretap surveillance are subject to prosecution and may jeopardize a client's case.

D. Party Consent

... One important exception is provided to the federal statute governing wiretaps.

... "It shall not be unlawful for a party to any wire or oral communication or a person given prior authority to the communication to intercept such communication, as long as it is not done for the purpose of committing an unlawful or injurious act."

... A permissible technique while investigating annoying phone calls is to record the call, and then play it back to the suspect during an interrogation.

E. Local Application

... The above discussion is based on federal law.

... Parallel legislation needs to be considered in state governments.

... Federal requirements for official wiretapping make no exception for police action that is not authorized by a state law conforming to Title III.

... Patrol officers should be alert for individuals who may be improperly working on telephone lines.

... Identify individuals observed climbing telephone poles or working at terminal boxes.

The usually off Ma telephor doing so they are of the c

Fraud organize and so-c small n the tele Phone f fraudule place ex These s make u tions wl

All devices. free telc cations needed ground tinely i obtain t publicat illegal "box", e make fr

Blac

The permits having consists conditio

# questions

The following questions are based upon material in the Training Key. Select the best answers.

1. To the police officer, the most important reason for investigating fraudulent telephone calls is:

- (a) *because of the potential threat to communications posed by revolutionary groups.*
- (b) *because people who go to the trouble of concealing their telephone calls often are involved in other illegal operations.*
- (c) *because fraudulent use of the telephone is a direct attack against the establishment.*
- (d) *because fraudulent calls amount to enormous annual losses for the telephone company.*

2. Which of the following electronic instruments does not permit the user to make telephone calls free of charge?

- (a) *Red Box*
- (b) *Black Box*
- (c) *Cheese Box*
- (d) *Blue Box*

3. Which of the following means of fraudulently using the telephone will patrol officers most likely encounter?

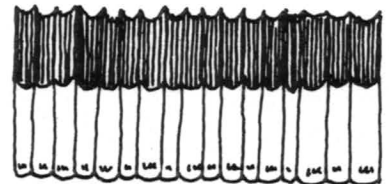
- (a) *Black Boxes*
- (b) *Cheese Boxes*
- (c) *False credit card numbers*
- (d) *Tape recorded numbers.*

# answers

1. (b) Police officers should realize that fraudulent telephone calls are often linked to other crimes. Gamblers, organized crime figures, and other criminals make fraudulent calls in order to avoid a traceable record of their communications.

2. (c) The blue box, black box, and red box can be used to make free calls. The cheese box merely transfers incoming calls to another line.

3. (c) The use of false credit card numbers usually occurs in pay phone booths. When a fraudulent call is discovered, the telephone company may request the police officer to respond to the telephone booth to make an arrest.



*Have you read...*



*Crime by the Numbers.* National District Attorney's Association, 1972.

*A helpful guide through the intricacies of investigation and prosecution of telephone credit card and third number billing fraud cases.*