

FBI

FBI WITH EACH ARTICLE

September 1987

Law Enforcement Bulletin

U.S. Department of Justice
National Institute of Justice

107089-

This document has been reproduced exactly as received from the person or organization originating it. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the National Institute of Justice.

Permission to reproduce this copyrighted material has been granted by
FBI Law Enforcement Bulletin

to the National Criminal Justice Reference Service (NCJRS).

Further reproduction outside of the NCJRS system requires permission of the copyright owner.

NCJRS

SEP 24 1987

RECEIVED



107089-
107091

FILM WITH EACH ARTICLE
Contents

September 1987, Volume 56, Number 9

- 107089 Crime Problems 1 **Telecommunications Fraud Devices**
By George N. Aylesworth and Marianne Swan
- 107020 Crime Statistics 5 **Crime in the United States—1986**
- 13 **Book Review**
- Operations 14 **Impact Fees: A Fiscal Response**
By Bruce A. Mills
- 107091 Research 16 **An Introduction to the Serial Rapist: Research by the FBI**
By Robert R. Hazelwood and Ann W. Burgess
- Legal Digest 25 **The Inventory Search (Conclusion)**
By John C. Hall
- 31 **Wanted by the FBI**

FBI

Law Enforcement Bulletin

United States Department of Justice
Federal Bureau of Investigation
Washington, DC 20535

John E. Otto, Acting Director

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law of the Department of Justice. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget through June 6, 1988.

Published by the Office of Public Affairs
Milt Ahlerich, *Acting Assistant Director*

Editor—Thomas J. Deakin
Assistant Editor—Kathryn E. Sulewski
Art Director—John E. Ott
Production Manager—Mark A. Zettler
Reprints—Carolyn F. Thompson

The Cover:

Minneapolis police officer and his canine partner make friends in the community.

The FBI Law Enforcement Bulletin (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Ave., N.W., Washington, DC 20535. Second-class postage paid at Washington, DC. Postmaster: Send address changes to Federal Bureau of Investigation, FBI Law Enforcement Bulletin, Washington, DC 20535.



Telecommunications Fraud Devices

"...it is important for police officers to be aware of, and be able to recognize, TFDs since their use results in losses totaling millions of dollars annually."

EDITOR'S NOTE:

As individuals develop new methods of defrauding telecommunications companies, some devices may be known by different names in different regions of the country. The original "black box" could not produce tones, while some later designs (sometimes referred to as "yellow boxes") do. Some devices even contain electronics to complete both local calls and "blue box" calls.

Police officers, in the regular course of their duties, may encounter devices used to make long distance calls illegally, and at times, may actually come in contact with persons using these devices. Because telecommunications fraud devices (TFDs) are small and are often disguised as other items, recognizing these devices and the illegal activity associated with them is often difficult. Yet, it is important for police officers to be aware of, and be able to recognize, TFDs since their use results in losses totaling millions of dollars annually.

TFDs are often found in conjunction with other criminal activities. In addition to avoiding long distance telephone charges, these devices can also be used to prevent records of telephone calls between certain numbers from being made. For this reason, the de-

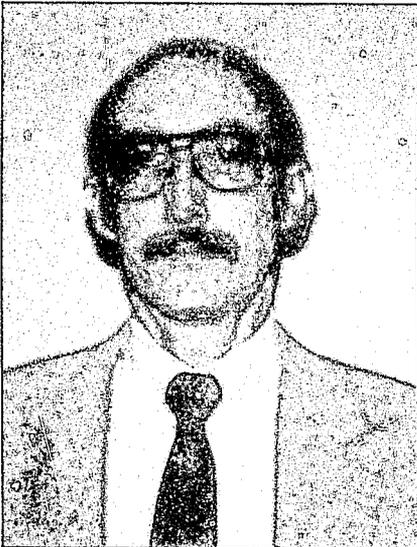
vices are particularly attractive to persons conducting illegal narcotics or gambling operations, as well as those involved in other types of organized criminal activity.

Use or possession of TFDs is prohibited by Federal law.¹ However, there may be local laws with specific provisions on TFDs. For example, it is a crime in Florida for any person to make or possess any electronic device capable of duplicating tones or sounds used in long distance telecommunications, if the intent is to avoid payment for long distance service.² A person convicted of violating this provision is guilty of a third-degree felony.³

Police officers should consult their legal adviser or local prosecuting attorney regarding the appropriate laws to use in the event they encounter a TFD. Other valuable resources for information regarding TFDs are the security offices of local telephone companies, the U.S. Secret Service, which investigates Federal law violations regarding TFDs, and the Communications Fraud Control Association.⁴

There are several key factors in making any case concerning the use, possession, or manufacture of TFDs, commonly known as "blue boxes," "black boxes," or "red boxes." These factors include recognizing the device, establishing possession of the device, and being aware of circumstances that indicate that the device is intended to

By
GEORGE N. AYLESWORTH
Supervisor
and
DET. MARIANNE SWAN
Police Legal Unit
Metro-Dade Police Department
Miami, FL



Mr. Aylesworth



Fred Taylor, Director
Metro-Dade Police Dept.

be used to avoid or attempt to avoid payment for long distance service.

TFDs often look like pocket calculators that may or may not have a functional calculator display. Others simply appear to be metal or plastic boxes with numbered or lettered keys. The configuration of the keys may be similar to that on a touch-tone telephone, a calculator, etc. The symbols on the keys may also vary. Many of the devices will have a small built-in speaker, while others may have a small speaker at the end of a wire leading from the box.

There are devices that resemble TFDs and operate in a similar manner, but are not illegal to possess. One such device is an automatic telephone dialer which can be programmed to reproduce the tones made by a touch-tone telephone. When held to the mouthpiece of a telephone, an automatic telephone dialer will make a connection with the desired number by emitting the appropriate sequence of tones. These dialers, unless altered internally, do not make the same type of tones as TFDs and will not bypass long distance charges. They will make local calls, which is something that the tones produce by a TFD will not do. In fact, one indication that a suspect item is illegal is that it cannot be used to complete a local call. This factor will differentiate a TFD from a legal telephone dialer. There are devices, however, which contain electronics to be both a legal telephone dialer and a TFD. In essence, there are two devices in one box, one being legal and one being a TFD.

The three major types of TFDs used to evade payment of long distance charges have certain characteristics that set them apart from each other and from legal devices and which may assist in identifying them as TFDs.

However, the common factor is that all duplicate tones used in long distance telecommunications.

"Blue boxes" are devices that will originate fraudulent long distance calls from regular or coin-operated telephones. These devices may be relatively large, in which case they will generally be used in a fixed location, or they may be the size of a small calculator or package of cigarettes. Those resembling pocket calculators may actually function as one as well as a telecommunications fraud device. "Blue boxes" are usually equipped with 12 to 15 buttons or switches used to activate the necessary tones. If not designed to be wired directly into a telephone system, the device will have a speaker, either built into the device or attached with a wire, that is used to introduce the required tones into the mouthpiece of a telephone. A "blue box" is used by first making a legal long distance call. Calls on the "800" system, "555" long distance information system, or "short haul" long distance calls with minimal costs are often used to initiate use. Once the initial call is made, the "blue box" introduces a tone into the system which releases the original call and seizes the available long distance line. The caller can then use this "open" line by activating other "blue box" tones to call any number, virtually anywhere, at no cost and with no records being created. Officers should be alert to any suspicious device with a number of buttons or switches, which is either wired to a telephone or found in close proximity to a telephone. A small speaker on the device, or connected to it with a wire, is another factor. At public telephones, persons may be seen manipulating suspicious de-



Detective Swan

vices near the telephone and placing either the device or a small remote speaker up to the mouthpiece of the telephone.

"Red boxes" are devices that are used exclusively with single slot, coin-operated telephones. These devices duplicate the tones created by coins dropping into the telephone when payment is made. The tones signal the switching system of the long distance network that payment has been made and that the long distance connection should be completed. A record of the call will exist in the records of the coin-operated telephone number. "Red boxes," due to their public use, are always small. They are often built into a crush-proof, flip-top cigarette package. The most common type has three buttons for simulation of the tones connected with the three denominations of coins accepted by coin-operated telephones. Some of them have a single button and simulate only the tone associated with quarters. The speaker is self-contained, and when the device is concealed in a cigarette package, the speaker is commonly faced to the front side of the cigarette package, where a number or small holes have been made to allow a clear tone to escape. During use, these devices will be held close to the mouthpiece of the coin-operated telephone.

"Black boxes" are devices that are attached to a telephone line. They vary in size and have one or two buttons or switches. Unlike the other telecommunications fraud devices, the "black box" does not permit free long distance calls to be made from the telephone to which it is connected. Rather, long distance callers to the "black box" equipped telephone will be able to make their calls free of charge. The

"black box" causes the long distance network to react as if the call was not answered and the caller disconnected. Therefore, the caller is not billed and no record is created. Callers from a coin-operated telephone will have their money returned, as is done with a legitimate uncompleted call.

TFDs may be encountered during the execution of a search warrant, and since many resemble legal items, they could be overlooked. In all cases, but particularly where innocent-appearing devices are involved, detection will usually depend on an examination of the device, coupled with a careful observation of all factors surrounding its discovery. Pertinent factors include proximity to a telephone; list of telephone numbers, particularly telephone numbers from other nations, on or near the device; statements made about the device; or information developed during the investigation which produced the warrant.

Another way in which TFDs may be encountered is during a search of a person or vehicle without a warrant, pursuant to some exception to the general requirement for a warrant.⁵ Again, the identification of a suspect device will often depend in part on a compilation of surrounding factors, in addition to the appearance or testing of the device.

Officers may observe persons using TFDs in a public place, which indicates that the person is engaging in illegal activity. Under such circumstances, a police officer would be authorized to temporarily detain the person, as long as there was a reasonable indication that a crime was occurring or had just occurred.⁶ The detention must be for investigative purposes and must be brief.⁷ There are a number

"The key factor in any case involving TFDs is recognition of the devices and the methods of using them."

of factors that could establish the requisite indication of illegal activity to authorize such a temporary detention, e.g., the demeanor of the person (apparent nervousness or furtive actions) and observed use of some type of device held up to a telephone. Once such activities have been witnessed, an officer can approach the individual. Based on the results of this contact, the officer then determines whether further action should be taken. If the person's freedom of action is not significantly restricted by such contact, either explicitly or implicitly, a custodial situation will not result, and any statement the person makes will not be the result of custodial interrogation.⁸ Consequently, such statements, along with other observations made during the contact, could appropriately be used to develop probable cause to arrest and would be admissible as evidence in subsequent proceedings.

"Blue boxes" and "black boxes" are types of TFDs that will be encountered more frequently in residences or offices. As noted previously, these items are often wired into the telephone system. "Blue boxes" are often found in connection with "call-sell" operations. These are operations in which owners of the devices permit other persons to make long distance calls, usually international calls, for a fee that is much lower than the actual long distance rate. These operations may operate around the clock, and the extent of the loss to the long distance carrier may be correspondingly large. "Call-sell" businesses are usually found in areas where there are large concentrations of foreign nationals or recent immigrants.

Personal computers can also be used as TFDs. Computers can be connected to telephone lines by devices

called "modems." These devices vary in size and shape, but will usually be recognizable because they will either have a cradle in which a telephone handset is placed or will connect with common telephone connector wire. As most computers have the capability to generate a wide range of tones, there will be no recognizable "blue box" or "black box" visible. However, documentary items such as personal telephone directories, lists of access codes, or instructions for illegal use may be found in proximity to a personal computer. Personal computers are most commonly used to defraud long distance carriers through their ability to generate an abundance of random numbers and run these numbers in the telephone system until an access code is found. At this time, the computer can break into the long distance network of some carrier and make calls which are either not charged to any account or are charged to another person's account. In any case, as personal computers are not illegal devices *per se* as are the other items previously described as TFDs, it is unlikely that an officer will be able to develop enough information to make an arrest or seizure, based on use of a personal computer as a TFD during an inadvertent encounter or observation of the device. However, if factors exist that create a suspicion of illegal activities, officers who are aware of these potential uses for personal computers could notify the Secret Service or the local telephone company. These agencies may then be able to initiate an inquiry and establish a prosecutable case.

Summary

While there is a comprehensive Federal law prohibiting TFDs and a Federal investigative effort to combat

their illegal use, it is important that local officers be cognizant of TFDs. Local efforts will assist the national effort and have the potential to provide local benefit, because TFDs are often found in connection with other criminal activity. The key factor in any case involving TFDs is recognition of the devices and the methods of using them. TFDs may easily be overlooked if police officers are not aware of the various forms they may take.

FOOTNOTES

¹18 USC sec. 1029.

²Sec. 817.482(2), *Fla. Stat.*

³*Id.*

⁴Communications Fraud Control Association, P.O. Box 23891, Washington, DC 20026. The Communications Fraud Control Association (CFCA) is an organization of security personnel from a large number of telecommunications companies. The association and its members are a valuable source of information and technical assistance to law enforcement officers investigating telecommunications fraud cases. The president of the CFCA provided information which made this article possible, as did the special agent in charge of the New York Office of the U.S. Secret Service.

⁵*Chimel v. California*, 395 U.S. 752 (1969); *United States v. Ross*, 456 U.S. 798 (1982); *New York v. Belton*, 449 U.S. 1109 (1981).

⁶*Terry v. Ohio*, 392 U.S. 1 (1968).

⁷*Id.*

⁸*Oregon v. Mathiason*, 429 U.S. 492 (1977); 50 L. Ed. 2d 714; 97 S. Ct. 711 (1977).