Exploding The Phone

www.explodingthephone.com

Bibliographic Cover Sheet

db491

Title	**The Investigation and Prosecution of Electronic Toll Fraud Cases**
Date	1978-04-07
Author(s)	Schmidt, Walter P.
Abstract	Overview of investigation and prosecution of electronic toll fraud cases
Keywords	Blue box; black box; cheesebox; cheese box; red box; Walter Schmidt; Kenneth Odell; Donald Garland Odell; Donald Deval Heater
Notes	Includes United States Court of Appeals Memorandum regarding Odell case
Source	Bob Ginnings

paper given by Walt Schmidt in Atlanta, Ga at ASIS training session on April 7, 1978

THE INVESTIGATION AND PROSECUTION

OF

ELECTRONIC TOLL FRAUD CASES

CONTENTS

GLOSSARY OF TERMS AND ABBREVIATIONS

USED IN DOCUMENTATION OF ELECTRONIC TOLL FRAUD

AMA — Automatic Message Accounting — The equipment used to record on continuous tapes the details of customer-dialed calls required for billing purposes. AMA and CAMA and LAMA refer to the same general type of equipment.

ANI – Automatic Number Identification — Equipment located in a local central office to automatically identify the calling subscriber's number.

Auxiliary Tape Recorder — The magnetic tape recorder which is utilized with and controlled by the Dialed Number Recorder.

Black Box — The black box is named for the color of the first one found. It varies in size and usually has one or two switches or buttons. Attached to a telephone line, it provides free toll calling to that line. The black box user tells individuals to place toll calls to him, then operates the switch or button, causing a non-charge condition to be recorded on the telephone company's billing equipment.

Blue Box — The blue box, named for the color of the first such device found, varies in size and has either 12 or 13 buttons or switches on its face. The blue box can be directly attached to a telephone line or acoustically coupled by placing it directly against the receiver.

A blue box user usually calls a toll-free long distance number to gain access to the switching network. Disconnecting the first call with a 2600 Hz tone from the blue box, the user feeds in the number he wants in multi-frequency tones. Telephone Company billing records show only the free toll call and not the subsequent call made by the blue box user.

Central Office — (CO) — The switching equipment in a building that provides exchange telephone service for a given geographical area.

Cheese Box — An electronic toll fraud (ETF) device which inter-connects two telephone lines, each having different numbers but terminating at the same location. There is a "No-charge" condition on the calls placed to the cheese box, if used in conjunction with a black box.

Customer Toll Dialing — The dialing of toll telephone calls by the subscriber. It is generally referred to as Direct Distance Dialing (DDD).

Digit — Usually one of the symbols 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 and sometimes letters.

DDD — Direct Distance Dialing — Toll service that permits customer to dial their own long distance calls.

DNR — Dialed Number Recorder — The Dialed Number Recorder is attached to the suspect blue box user's line to document blue box activity. Documentation exists in the form of recording on paper tape the application of 2600 Hz tones and the digits dialed in Multi-Frequency Signaling Tones along with any digits dialed by the suspect's telephone. Upon the application of 2600 Hz tone, the Dialed Number Recorder turns on an auxiliary tape recorder to record on magnetic tape the blue box tones and to establish completion of the call.

ETF — Electronic Toll Fraud — The fraudulent obtaining of "free" telecommunications service by use of either a Blue Box, a Black Box, a Red Box, a Cheese Box or other types of electronic devices.

Hz — Hertz — International standard unit of frequency. Replaces and is identical to, the older unit of "cycle per-second."

Intercept — Calls made to an unassigned or nonworking telephone number which are directed to a recorded announcement and/or an operator.

"800" — IN-WATS — Inward Wide Area Telephone Service is one which is used to provide "Toll Free" calling to the IN-WATS subscriber.

MF — MULTI-Frequency Tones — Used to signal a called number on the toll network. Each digit is represented by combinations of 2 of 6 possible different frequencies.

NNX Code or NXX Code — The first three digits of the telephone number.

Numbering Plan Areas (NPA) — Geographical areas in the United States, Canada, and the Caribbean each of which is assigned a distinctive three-digit number called an area code. NNX or NXX codes are not duplicated within an area, making it possible for each subscriber to be assigned an individual ten-digit number unlike any other in any area. IN-WATS listings are indicated by the NPA of 800.

Off-Hook — The condition that indicates the active (busy) state of a subscriber's line.

On-Hook — The condition that indicates the idle state of a subscriber's line.

ONI — Operator Number Identification — Identification by an operator of a calling subscriber's number.

Operator Code — A code that normally is dialed only by an operator to reach the various toll operators, such as 121 for inward, 131 for information, etc.

Probable Cause Device — A device attached to the suspect blue box user's line to register every time a fraudulent call is placed.

Red Box — An electronic toll fraud device which is coupled acoustically to the transmitter on a single slot coin telephone to permit imitation of the tones representing coin deposits in the coinbox, thus achieving "no charge" on toll calls.

Reorder — A low interrupted tone that indicates all switching paths are busy, all toll trunks are busy, equipment blockages, unassigned code dialed, or incomplete registration of digits.

SF — Single Frequency of 2600 Hz tone.

Signalling — A Method used to convey on the toll network the status of a call (off-hook, on-hook, ring, reorder, answer, etc.) or to convey the called number (by use of tones corresponding to digits).

Subscriber's Line — A term used to denote the pair of wires connecting the subscriber's telephone with the central office.

Tariff — The published rates, charges, rules, and regulations governing the provision of communications services.

Toll Call or Message — A completed call to a point outside the local service area, generally referred to as a "long distance" call.

Operator Completed — A toll message placed through an operator and ticketed and timed by her.

Customer Dialed — A toll message dialed by the customer and recorded by automatic equipment.

Customer Dialed — Operator Serviced — A toll message dialed by the customer and serviced by an operator.

Trunk — A communications link between local or toll central offices.

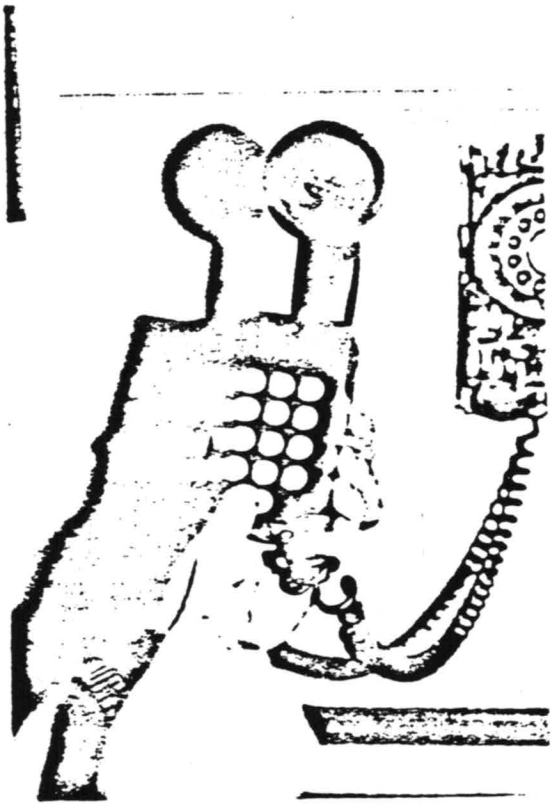
Universal Directory Assistance — NPA-555-1212 — A service furnished by the Telephone Company to provide long distance customers with assistance in finding subscriber listings of telephone numbers.

ELECTRONIC TOLL FRAUD DEVICES

There are several different types of electronic equipment which may be generally classified as ETF devices. The most significant is the "blue box". The characteristics of each type of device are discussed below.

Blue Box

The "blue box" was so named because of the color of the first one found. The design and hardware used in the blue box is fairly sophisticated, and its size varies from a large piece of apparatus to a miniaturized unit that is approximately the size of a "king-size" package of cigarettes.



The blue box contains 12 or 13 buttons or switches that emit multi-frequency tones characteristic of the tones used in the normal operation of the telephone toll (long-distance) switching network. The blue box enables its user to originate fraudulent ("free") toll calls by circumventing toll billing equipment. The blue box may be directly connected to a telephone line, or it may be acoustically coupled to a telephone handset by placing the blue box's speaker next to the transmitter of the telephone handset. The operation of a blue box will be discussed in more detail below.

To understand the nature of a fraudulent blue box call, it is necessary to understand the basic operation of the Direct Distance Dialing (DDD) telephone network. When a DDD call is properly originated, the calling number is identified as an integral part of establishing the connection. This may be done either automatically or, in some cases, by an operator asking the calling party for his telephone number. This information is entered on a tape in the Automatic Message Accounting (AMA) office. This tape also contains the number assigned to the trunk line over which the call is to be sent. The assigned trunk number provides a continuity of information contained on the tape. Other information relating to the call contained on the tape includes: called number identification, time of origination of call, and information that the called number answered the call. The time of disconnect at the end of the call is also recorded.

Although the tape contains information with respect to many different calls, the various data entries with respect to a single call are eventually correlated to provide billing information for use by accounting departments.

The typical blue box user usually dials a number that will route the call into the telephone network without charge. For example, the user will very often call a well-known

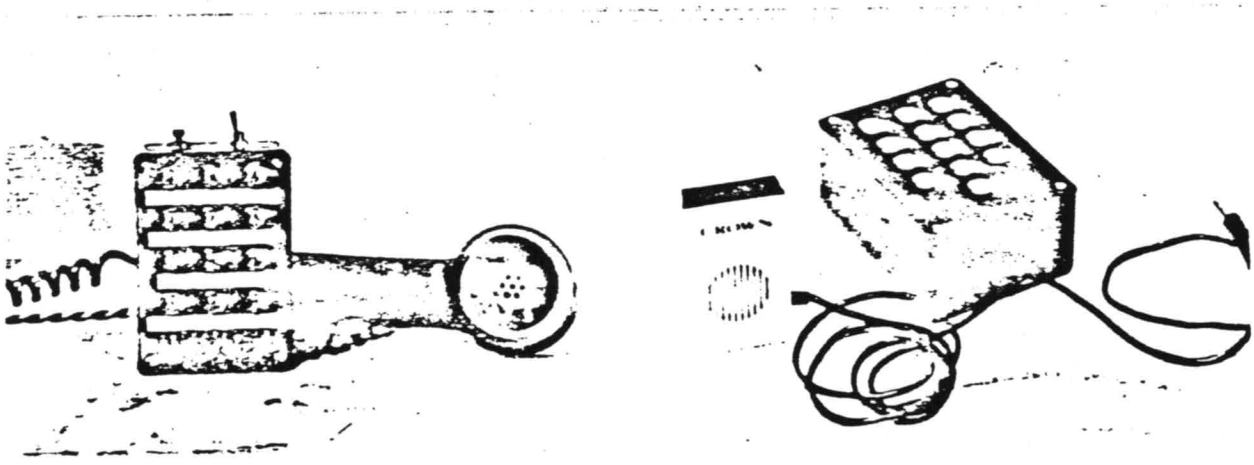
INWATS (toll-free) customer's number. The blue box user, after gaining this access to the network and, in effect, "seizing" control and complete dominion over the line, operates a key on the blue box which emits a 2600 Hertz (cycles per second, abbreviated hereafter as "Hz") tone. This tone causes the switching equipment to release the connection to the INWATS customer's line. Normally, the 2600 Hz tone is a signal that the calling party has hung up. The blue box simulates this condition. However, in fact the local trunk on the calling party's end is still connected to the toll network. The blue box user now operates the "KP" (key pulse) key on the blue box to notify the toll switching equipment that switching signals are about to be emitted. The user then pushes the "number" buttons on the blue box corresponding to the telephone number being called. After doing so, he operates the "ST" (start) key to indicate to the switching equipment that signalling is complete. If the call is completed, only the portion of the original call prior to the emission of 2600 Hz tone is recorded on the AMA tape. The tones emitted by the blue box are not recorded on the AMA tape. Therefore, because the original call to the INWATS number is toll-free, no billing is rendered in connection with the call.

Although the above is a description of a typical blue box operation using a common method of entry into the network, the operation of a blue box may vary in any one or all of the following respects:

(a) The blue box may include a rotary dial to apply the 2600 Hz tone and the switching signals. This type of blue box is called a "dial pulser" or "rotary SF" blue box.

(b) Entrance into the DDD toll network may be effected by a pretext call to any other toll-free number such as Universal Directory Assistance (555-1212) or any number in the INWATS network, either inter-state or intra-state, working or non-working.

(c) Entrance into the DDD toll network may also be in the form of "short haul" calling. A "short haul" call is a call to any number which will result in a lesser amount of toll charges than the charges for the call to be completed by the blue box. For example, a call to Birmingham from Atlanta may cost $.80 for the first three minutes while a call from Atlanta to Los Angeles is $1.85 for three minutes. Thus, a short



haul, three-minute call to Birmingham from Atlanta, switched by use of a blue box to Los Angeles, would result in a net fraud of $1.05 for a three-minute call.

(d) A blue box may be wired into the telephone line or acoustically coupled by placing the speaker of the blue box near the transmitter of the telephone handset. The blue box may even be built inside a regular Touch-Tone® telephone, using the telephone's pushbuttons for the blue box's signalling tones.

(e) A magnetic tape recording may be used to record the blue box tones representative of specific telephone numbers. Such tape recording could be used in lieu of a blue box to fraudulently place calls to the telephone numbers recorded on the magnetic tape.

All blue boxes, except "dial pulser" or "rotary SF" blue boxes, must have the following four common operating capabilities:

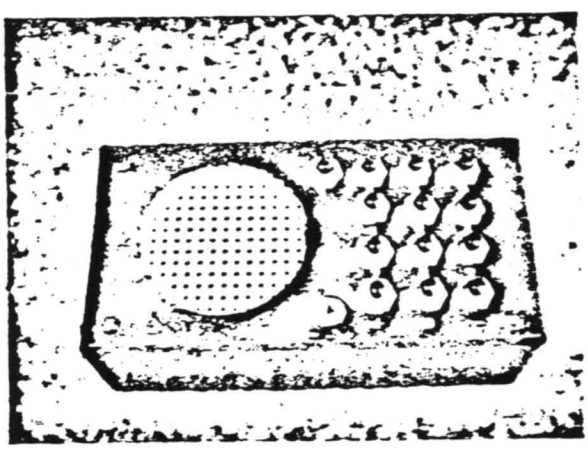
(a) It must have signalling capability in the form of a 2600 Hz tone. This tone is used by the toll network to indicate, either by its presence or its absence, an "on-hook" (idle) or "off-hook" (busy) condition of the trunk.

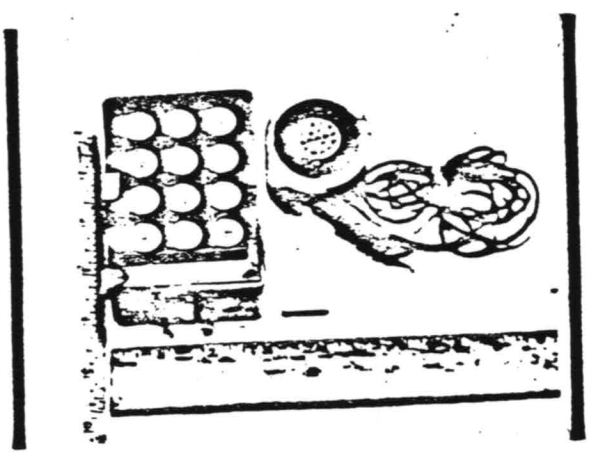
(b) The blue box must have a "KP" key or button. "KP" is an abbreviation for a "Key Pulse" tone that unlocks or readies the multi-frequency receiver at the called end to receive the tones corresponding to the called telephone number.

(c) The typical blue box must be able to emit multi-frequency tones which are used to transmit telephone numbers over the toll network. Each digit of a telephone number is represented by a combination of two tones. For example, the digit 2 is transmitted by a combination of 700 Hz and 1100 Hz tones.

(d) The blue box must have an "ST" key. "ST" is an abbreviation for a "start" signal which consists of a combination of two tones that tell the equipment at the called end that all digits have been sent and that the equipment should start switching the call to the called number.

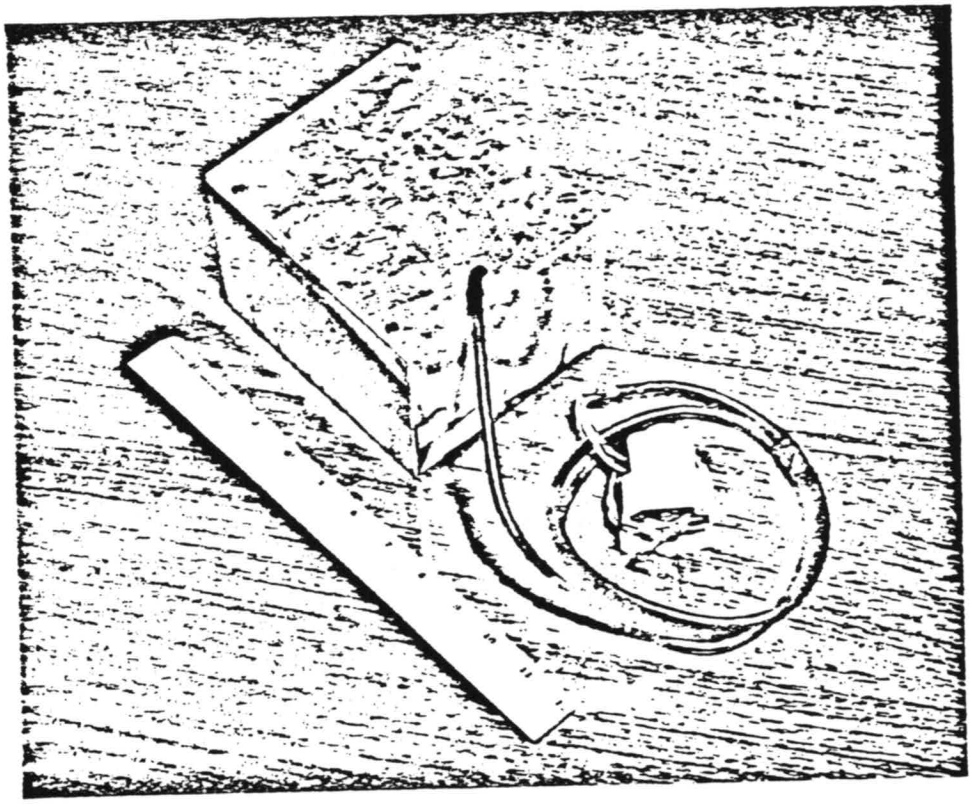
The "dial pulser" or "rotary SF" blue box requires only a dial with a signalling capability to produce a 2600 Hz tone.

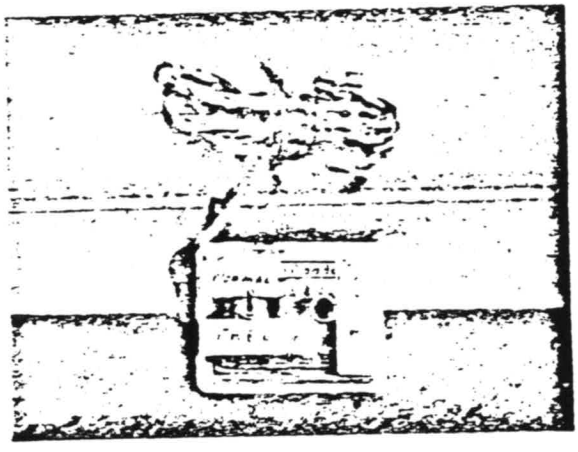


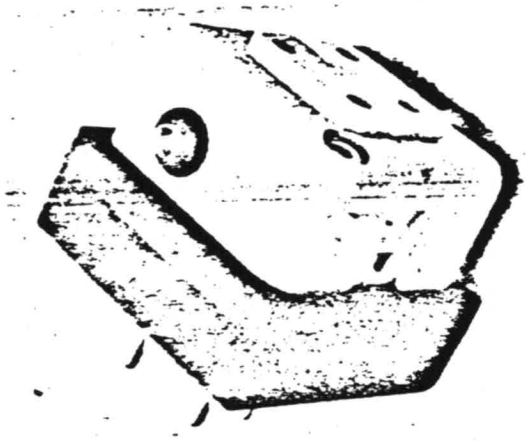


Black Box

This ETF device is so-named because of the color of the first one found. It varies in size and usually has one or two switches or buttons.



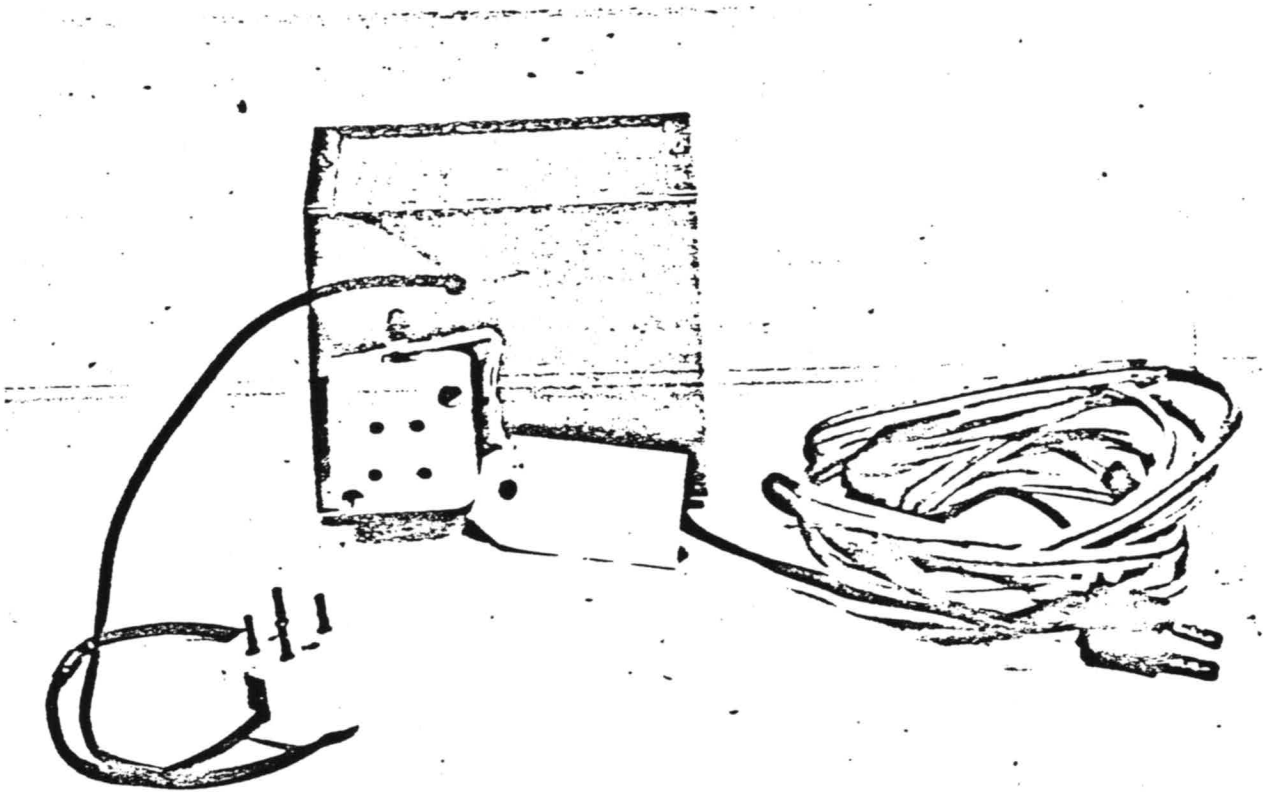




Attached to the telephone line of a called party, the black box provides toll-free calling to that party's line. A black box user informs other persons beforehand that they will not be charged for any call placed to him. (For example, bettors calling from a coin telephone will get their coin back.) The user then operates the device causing a "non-charge" condition ("no answer" or "disconnect") to be recorded on the telephone company's billing equipment. A black box is relatively simple to construct and is much less sophisticated than a blue box.

Cheese Box

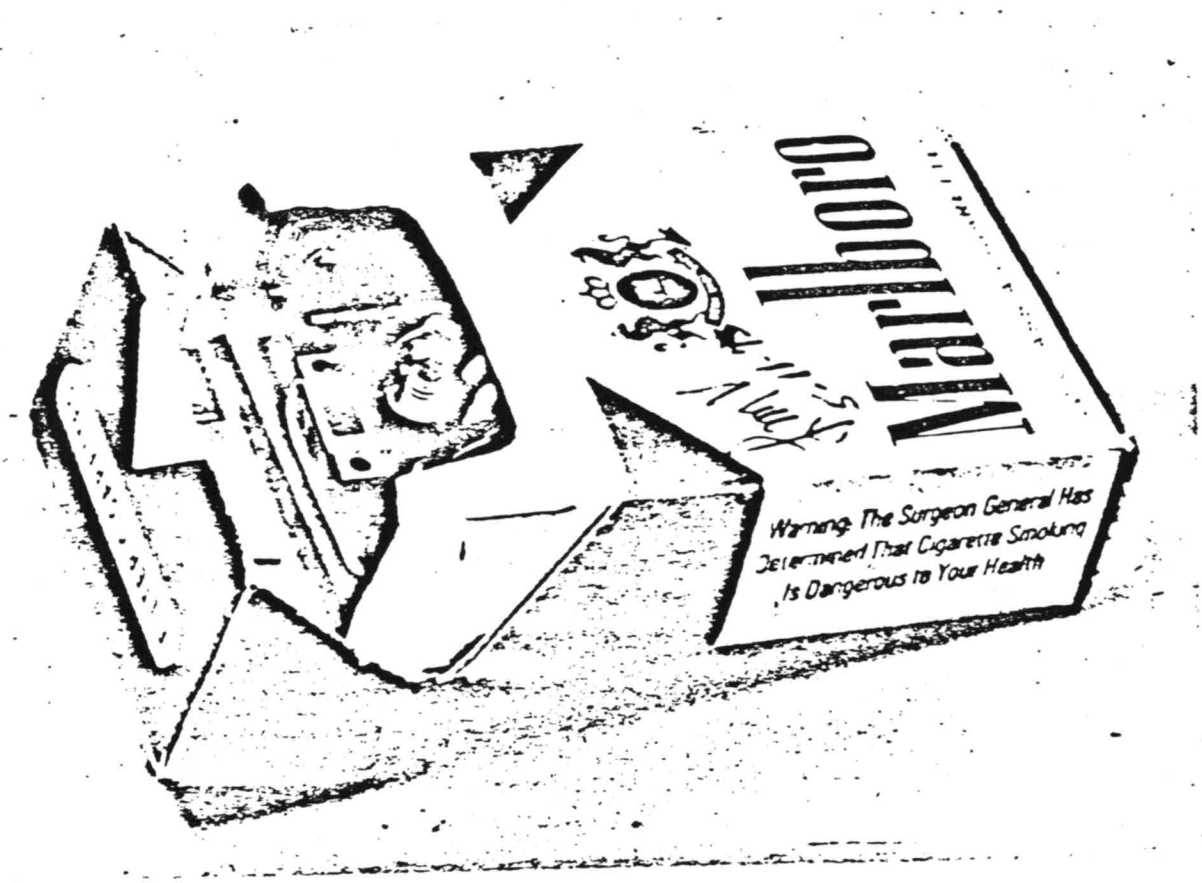
This device is so-named for the container in which the first one was found. Its design may be crude or very sophisticated. Its size varies; one was found the size of a half-dollar.



A cheese box is used most often by bookmakers or bettors to place wagers without detection from a remote location. The device inter-connects two telephone lines, each having different numbers but each terminating at the same location. In effect, there are two telephones at the same location which are linked together through a cheese box. It is usually found in an unoccupied apartment connected to a telephone jack or connecting block. The bookmaker, at some remote location, dials one of the numbers and stays on the line. Various bettors dial the other number but are automatically connected with the bookmaker by means of the cheese box interconnection. If, in addition to a cheese box, a black box is included in the arrangement, the combined equipment would permit toll-free calling on either line to the other line. If a police raid were conducted at the terminating point of the conversations — the location of the cheese box — there would be no evidence of gambling activity. This device is sometimes difficult to identify. Law enforcement officials have been advised that when unusual devices are found associated with telephone connections the telephone company security representatives should be contacted to assist in identification.

Red Box

This device is coupled acoustically to the handset transmitter of a single-slot coin telephone. The device emits signals identical to those tones emitted when coins are deposited. Thus, local or toll calls may be placed without the actual deposit of coins.



INVESTIGATIVE PROCEDURES

This section reviews the investigative procedures used by Security Departments. It should be noted that, to a great extent, these procedures reflect those used by Bell System companies and many independent telephone companies.

Most of the discussion will concern blue box investigations because of the frequency of the blue box cases referred to law enforcement officials for prosecution.

The Security Department may initially discover evidence of ETF activity. This may result from an analysis of calling patterns to particular numbers. Such analyses may reveal abnormal calling patterns which possibly are the result of ETF activity. Moreover, cases of suspected ETF are referred to the Security Department from the various operating departments, from other telephone companies, or from law enforcement officials as a result of their investigation of gambling or other criminal activities. In some instances, detection and identification of a calling station originating suspected blue box tones can be provided by use of a special non-monitoring test equipment.

If initial indications are that there is a substantial possibility that a blue box is being used on a particular line, the Security Department determines certain information about the line. The name of the subscriber to that line is identified, and an inventory is made of the line and station equipment being provided to him. A discreet background investigation (record) is conducted to establish the subscriber's identity. After this preliminary data is gathered, ETF detection units are installed on the suspected line to establish "probable cause" for further investigation. If the "probable cause" equipment indicates repeated ETF activity on the line, other equipment is then installed to document such activity.

The "probable cause" equipment ascertains the existence or non-existence of ETF activity on the line by indicating the presence of multi-frequency tones on the subscriber's end of the line which would not be present in normal usage. The "probable cause" device registers each time a blue box call is placed. It is associated with a built-in peg-count meter to register each and every application of 2600 Hz tones in single-frequency (SF) signalling and/or 2600 Hz tone followed by KP tones used in multi-frequency (MF) signalling. As previously stated, such tones should not normally be present on the line.

If "probable cause" is established, other detection, identification and documentation equipment is installed. The primary equipment being used is the dialed number recorder (DNR), coupled with an auxiliary tape recorder. The DNR is activated when the suspect subscriber's telephone goes "off-hook" and prints on paper tape the following information concerning the call: the date and time of the call and the digits dialed over the suspect subscriber's line. Moreover, the DNR records on the paper tape an indicator of the presence of 2600 Hz tones on the line and the presence of multi-frequency signalling tones on the subscriber's line. The auxiliary tape recorder is activated only after the presence of 2600 Hz tone on the line is detected by the DNR (indicating the use of a blue box). Once the tape recorder is activated, it records the tones being emitted by the blue box, other signalling tones, and the ringing cycle on the called end. It also records a minimum amount of ensuing conversation for the purpose of (1) establishing that the fraudulent call was consummated and (2) establishing the identity of the fraudulent caller. The timing duration of the tape recorder is pre-set. A time of one-minute (including pulsing, ringing and conversation) is the standard setting; however, if the blue box user

is suspected of making overseas calls, the timing may be set for two minutes because of the greater time required by the blue box user to complete the call. Upon termination of the call, the DNR automatically prints the time of termination and the date. It should be pointed out that the presence of 2600 Hz tones plus multi-frequency signalling tones on a subscriber's line positively establishes that a blue box is being used to place a fraudulent call because such tones are not normally originated from a subscriber's line.

Once the raw data described above is gathered, the Security Department collects and formulates the data into legally admissible evidence of criminal activity. Such evidence will establish: (1) that a fraudulent call was placed by means of an ETF device, (2) that conversation ensued, (3) that the fraudulent call was placed by an identified individual, and (4) that such call was not billed to the subscriber number from which the blue box call originated. The evidence which is then available consists of documents and also of expert witness testimony by telephone company personnel concerning the contents of those documents, the operation of the blue box, and the operation of the detection equipment.

(Note: Similar techniques are used in the investigation of other forms of ETF.)

PRESENTATION OF EVIDENCE TO PROSECUTORS

The evidence accumulated by the Security Department is carefully reviewed by the Legal Department for the purpose of determining whether sufficient evidence exists to warrant the presentation of the evidence to law enforcement officials. If the evidence does warrant such action, it is presented under appropriate circumstances to the proper law enforcement officials. In all cases where prosecution is recommended, a professionally investigated and documented summary of the case will be prepared and presented by the Security Department to the prosecutor's office. Each case recommended for prosecution will be prepared as completely as possible, usually necessitating little or no pre-trial investigation for the prosecutor. The summary of the case will include the following:

(a) A background of the case with details of the defendant's activities and a summary of all pertinent investigative steps and interviews conducted in the course of the investigation.

(b) Identification of witnesses.

(c) Synopsis of pertinent points to which each witness can testify.

(d) Description of all documents and items of evidence and the suggested order of proof showing the chronology of events. The physical evidence presented will normally consist of one or more of the following: magnetic tapes from the auxiliary tape recorder, paper tapes from the DNR, worksheets and notes prepared in connection with the analysis of each fraudulent call, the suspect's toll billing records covering the period during which the fraudulent activity occurred, computer printouts which established probable cause or a statement of the source of the "probable cause", and telephone company records of equipment being provided to the suspect.

(e) Upon request, the law applicable to the case.

Other pertinent Company records will be furnished under subpoena or demand of lawful authority. If an arrest or search warrant is sought, the Security representatives will cooperate fully and furnish affidavits required to support the application for the issuance of such warrants. Although the Security representatives cannot execute such warrants, nevertheless, upon request, such representatives will accompany the executing officers to assist in the identification of any suspected ETF equipment found. The Security representative will also be available to suggest pertinent areas for interrogation of the persons suspected of engaging in the fraudulent activity.

APPLICABLE LAW

The cases presented herein have been selected to demonstrate: (1) that ETF activity is proscribed by both federal and state law, and (2) that the investigative procedures used by security personnel have been approved by the courts.

It is not practical to discuss in detail the provisions of the statutes. However, the citations of those statutes proscribing ETF activity are as follows (the full test of these statutes is contained in the Appendix):

FLORIDA: §§ 817.481, 817.482 F. S. A. California § 502.7 P.C.

GEORGIA: Code § 26-1807

NORTH CAROLINA: G. S. §§ 14-113.4, 14-113.5

SOUTH CAROLINA: Code § 16-565.1, 16-565.2

The discussion of federal law which follows includes precedents concerning admissibility of evidence which are equally applicable to prosecutions in state courts.

The applicable federal statute is Title 18 U. S. C. § 1343 (the "Fraud by Wire" statute, hereafter simply referred to as "§ 1343"):

> *"Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication, in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice shall be fined not more than $1,000 or imprisoned not more than five years, or both."*

Because of the wording of the statute, it was argued that § 1343 was applicable only to "schemes" to defraud third persons to whom communications were directed by means of wire, radio, or television. It was argued that the statute was not applicable to mere schemes to obtain free telephone service. Those arguments and contentions have been uniformly rejected by the courts. See Brandon v. United States, 382 F.2d 607 (10th Cir. 1967); United States v. Freeman, 373 F.Supp. 50 (S.D. Ind. 1974); United States v. Shah, 371 F.Supp. 1170 (W.D. Pa. 1974); United States v. DeLeeuw, 368 F.Supp. 426, 427 (E.D. Wisc. 1974); United States v. Jaworski, 343 F.Supp. 406 (D. Minn. 1972; United States v. Beckley, 259 F.Supp. 567, 571 (N.D. Ga. 1965). In Scott v. United States, 448 F.2d 481 (5th Cir. 1971), cert. denied, 405 U.S. 921, 92 S.Ct. 955, 30 L.Ed.2d 791 (1972), the defendants were charged under § 1343 with fraudulently charging toll calls to third parties without permission. In a footnote, the Court of Appeals said:

> *"Although the matter was not raised by appellants, this court has given careful consideration to whether 18 USCA § 1343 covers a scheme to defraud the telephone company of revenues for interstate telephone service. That question has been answered in the affirmative. Brandon v. United States, 10 Cir. 1967, 382 F.2d 607; United States v. Beckley, N.D. Ga. 1965, 259 F.Supp. 557; United States v. Hanna, S.D. Fla. 1966, 260 F. Supp. 430, rev'd on other grounds, 5 Cir. 1968, 393 F.2d 700 [such reversal being set aside upon rehearing and convictions affirmed, 404 F.2d 405 (1968), cert. denied, 394 U.S. 1015, 89 S. Ct. 1625, 23 L.Ed.2d 42 (1969)]. There is no case to the contrary. We agree that the statute embraces the conduct charged here." 448 F.2d at 583 n. 5.*

Blue box usage has been expressly held to be proscribed under §1343 in United States v. DeLeeuw, supra, and in United States v. Jaworski, supra. See also United States v. Freeman, 373 F.Supp. 50 (S.D. Ind. 1974).

When telephone calls are illegally placed, the telephone company has the right, and indeed the duty, to investigate such illegal activity. Sections 202 and 203(c) of the

Communications Act of 1934, as amended [47 U.S.C. §§ 202, 203(c)] provide that no carrier may discriminate between its customers by extending preferential treatment to any of them. Knowingly to allow ETF perpetrators to receive free service would constitute such discrimination. Further, each communications carrier is enjoined, under pain of criminal penalty, not to neglect or fail to maintain correct and complete records and accounts of the movements of all traffic over its facilities (47 U.S.C. § 220). Each carrier is also required to collect the federal excise tax levied upon each toll call (26 U.S.C. § 4251). These duties were acknowledged by the court in Hanna v. United States, 404 F.2d 405, 407 (5th Cir. 1968), cert. denied, 394 U.S. 1015, 89 S.Ct. 1625, 23 L.Ed.2d 42 (1969), and in United States v. Beckley, 259 F.Supp. 567, 571 (N.D. Ga. 1965).

In recognition of the telephone company's duty to investigate such unlawful activity, the courts have sanctioned the right of the company to survey, monitor and tape record fraudulent calls. In fact, there is no other sufficient way to obtain the necessary evidence of the unlawful activity except by means of a minimum amount of monitoring and recording. Such activity by the Company is not violative either of § 605 of the Communications Act of 1934, as amended (47 U.S.C. § 605, hereafter referred to as "§ 605") or of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. § 2510 ff., hereafter referred to as "Title III"). Moreover, because governmental officials are not involved in the gathering of the evidence by Company officials, there is no abridgement of Fourth Amendment Constitutional guarantees. See Burdeau v. McDowell, 256 U.S. 465, 41 S.Ct. 574, 65 L.Ed. 1048 (1921). With respect to the particular investigative procedures described herein, the Ninth Circuit, in an unpublished Memorandum Decision, has reached a similar conclusion. United States v. McDaniel et al., No. 73-3618, 74-1146, decided July 17, 1974 (copy attached).

It has long been the law that a wrongdoer cannot shield his illegality behind § 605. The landmark case was United States v. Sugden, 226 F.2d 281 (9th Cir. 1955), aff'd per curiam, 351 U.S. 916, 76 S.Ct. 709, 100 L.Ed. 1449 (1956). The Sugden case was preceded by several other decisions, including United States v. Gris, 247 F.2d 860, 864 (2d Cir. 1957) and Casey v. United States, 191 F.2d 1 (9th Cir. 1951), rev'd on other grounds, 343 U.S. 808, 72 S. Ct. 999, 96 L.Ed. 1317 (1952). In Casey, the Court of Appeals stated:

> *"The protections of the Act were never intended for, nor do they cover, . . . communications which are themselves illegal." 191 F.2d at 4.*

Similar conclusions were reached in Hanna v. United States, 404 F.2d 405 (5th Cir. 1968), cert. denied, 394 U.S. 1015, 89 S.Ct. 1625, 23 L.Ed.2d 42 (1969); Brandon v. United States, 382 F.2d 607 (10th Cir. 1967); Nolan v. United States, 423 F.2d 1031 (10th Cir.), cert. denied, 400 U.S. 848, 91 S. Ct. 47, 27 L.Ed.2d 85 (1970). More recent cases affirming this principle are United States v. DeLeeuw, 368 F.Supp. 426 (E.D. Wisc. 1974); United States v. Shah, 371 F.Supp. 1170 (W.D. Pa. 1974); and United States v. Freeman, 373 F.Supp. 50 (S.D. Ind. 1974).

In each of the above cases, the action of the telephone company in reasonably monitoring and recording the defendants' fraudulent conversations was approved, and the evidence thus obtained was ruled admissible.

In 1968, Title III was enacted. It amended § 605 by adding the prefatory words "Except as authorized by Chapter 119, Title 18 . . . ." The proscriptions of § 605, to the extent applicable at all, were subordinated to the provisions of Title III. Section 2511(2)(a) of Title III provides an exemption for the activities of a communications carrier

performed for the purpose of protecting the rights or property of the carrier. That section reads:

> *"(2)(a) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication . . . ."*

It should be noted that § 2511(2)(a) permits the carrier to intercept and disclose the fraudulent communications. United States v. Freeman, 373 F.Supp. 50, 52 (S.D. Ind. 1974). This interpretation is further strengthened by the Congressional history of the statute which makes it clear that the telephone company may lawfully intercept communications in the course of gathering evidence of toll fraud. See Senate Report No. 1097 of the Committee on the Judiciary, dated April 29, 1968. On page 93 of that Report (2 U.S. Cong. and Adm. News, 1968, at 2182) is stated:

> *"Paragraph (2)(a) provides that it shall not be unlawful for an operator of a switchboard or employees of a common carrier to intercept, disclose or use wire communications in the normal course of their employment while engaged in any activity which is a necessary incident to the rendition of this service or the protection of the rights or property of the carrier. It is intended to reflect existing law (United States v. Beckley, 259 F.Supp. 567 (DCGA. 1965)). . . ."*

Also of significance is 18 U.S.C. § 2510(5)(a) which excludes from the statutory definition of "electronic, mechanical or other device":

> *"Any telephone . . . instrument, equipment or facility, or any component thereof . . . (ii) being used by a communications common carrier in the ordinary course of its business . . ."*

Section 2510(4) defining the term "intercept" expressly provides that the aural acquisition of the contents of the wire communication must be through the use of a "device" to be unlawful. Legislative history contained on page 90 of Senate Report No. 1097 (2 U.S. Cong. and Adm. News 1968 at 2178-79) reiterates the unqualified language of § 2510(5)(a) that a telephone company's equipment used "in the ordinary course of its business" is excluded from the definition of "device". It would appear clear that equipment (such as DNR's, peg-count registers, magnetic tape recorders, monitoring equipment, and the like) used by security agents or plant personnel of a telephone company in detecting and gathering evidence of toll fraud is being used by the telephone company in the ordinary course of its business for the protection of the Company's rights or property.

Several recent cases, referred to supra, have approved specifically the investigative techniques used by telephone companies in ETF cases and have held that such techniques do not violate Title III.

In United States v. DeLeeuw, 368 F.Supp 426 (E.D. Wisc. 1974), the defendant sought to suppress evidence obtained by telephone company security personnel during a blue box investigation. A dialed number recorder (DNR) was attached to the defendant's line which recorded the digits dialed following the application of a "blue box frequency" tone to the line. An auxilliary tape recorder automatically recorded a one-minute conversation of defendant which ensued after application of the tone.

The court first found that the procedures used by the telephone company did not violate § 605. The court noted that § 605 (as amended in June 1968 by Title III to include in its first sentence, relating to common carriers, the words "except as authorized by Chapter 119, title 18, United States Code . . .") referred, in effect, to § 2511(2)(a)(1) of Title III which declares lawful telephone company interceptions and disclosures necessary

for the rendition of service or to protect Company rights and property. The court held that in this case the Company's action

> *". . . in attaching a 'blue box' detector to the defendant subscriber's line, which device recorded the numbers dialed, and conversations had on such line in only those instances where a 'blue box' frequency was actually applied thereto, constituted the type of nonrandom monitoring for the protection of property which is sanctioned by 18 U.S.C. § 2511(2)(a)(1)." 368 F.Supp. at 428.*

A similar result was reached in United States v. Shah, 371 F.Supp. 1170 (W.D. Pa. 1974). There the telephone company had used a DNR and an auxiliary tape recorder automatically activated by the presence on the subscriber's line of 2600 Hz tone. The recording was limited to the first minute of conversation, and the monitoring lasted for only seven days. The court held that such procedures were authorized by § 2511(2)(a). The court reviewed a number of cases decided prior to the enactment of Title III and re-emphasized that when there were "reasonable grounds for belief" by the telephone company that a person was using its lines to place illegal calls, monitoring of such calls could be instituted as "the only reasonable means of protection for the phone company" and did not violate § 605.

Further, the court found that the telephone company had sufficient preliminary information (from printouts) in its possession to warrant the reasonable conclusion that an electronic device was being used to circumvent its billing equipment. The court held that the defendant, by so using the telephone in a manner contrary to that to which he was entitled as a regular subscriber, was "deemed to have consented" to the monitoring of his calls. 371 F.Supp. at 1176. The company, by limiting its monitoring to 60 seconds for each call and to seven days for the total scope of monitoring, was adjudged to have monitored only to the extent reasonably necessary to identify the maker of such unauthorized calls. Since the right to monitor was not abused, the court acknowledged that the Company could lawfully turn over the tape recordings and other evidence to federal authorities for purposes of prosecution under 18 U.S.C. § 1343.

In United States v. Freeman, 373 F.Supp. 50 (S.D. Ind. 1974), the defendant's alleged use of a blue box was discovered by the telephone company by means of a DNR of substantially the same kind used by Southern Bell. On the basis of the evidence obtained through the DNR, a search warrant was obtained by law enforcement officials; and a blue box was found. Finding specifically that the use of a blue box is within the proscriptions of § 1343, the Court went on to hold that the investigative techniques used by the telephone company did not violate either § 605 or Title III.

Finally, in its memorandum decision (attached hereto) in United States v. McDaniel et al., the Ninth Circuit Court of Appeals, in a blue box case, also held specifically that the telephone company's investigative techniques did not violate either § 605, Title III, or the Fourth Amendment to the United States Constitution. In this case, the monitoring by the telephone company lasted only six days.

APPENDIX

Contains text of following:

Model Indictment

18 U.S.C. § 1343

47 U.S.C. § 605

18 U.S.C. § 2511(2)(a)

18 U.S.C. § 2510(5)(a)

§§ 817.481, 817.482 F.S.

Ga. Code § 26-1807

N.C.G.S. §§ 14-113.4, 14-113.5

S.C. Code § 16-565.1, 16-565.2

Memorandum Decision by United States Court of Appeals for the Ninth Circuit in United States v. McDaniel et al.

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF _____

_____ DIVISION

UNITED STATES OF AMERICA,	)	Criminal No. _____
	)	18 USC 1343
v.	)	
	)	
_____	)	INDICTMENT

The Grand Jury Charges:

(a) That on or about the dates hereinafter specified, in the County of _____, in the District of _____, _____(Name), unlawfully, knowingly, and intentionally did devise a scheme or artifice to defraud and obtain money by means of false or fraudulent pretenses, and did transmit or cause to be transmitted by means of wire communications in interstate or foreign commerce, signals or sounds for the purpose of executing such scheme or artifice which resulted in depriving Southern Bell Telephone and Telegraph Company, _____(Location), of their charges. The said scheme consisted of utilizing or causing to be utilized an electronic device, commonly referred to as a "blue box", to avoid telephone call billings.

(b) That on or about the _____ day of _____, 19____, in the County of _____, in the District of _____, _____(Name), for the purpose of executing the aforesaid scheme and artifice to defraud, and attempting to do so did transmit and cause to be transmitted in foreign commerce by means of a wire communication, that is, a telephone communication, between _____ in the State of _____, and _____, certain signs, signals and sounds all in violation of Title 18, United States Code, Section 1343.

18 U.S.C. § 1343

"Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than $1,000 or imprisoned not more than five years, or both."

47 U.S.C. § 605, as amended

"Except as authorized by chapter 119, Title 18, no person receiving, assisting in receiving, transmitting or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpoena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority. No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is broadcast or transmitted by amateurs or others for the use of the general public, or which relates to ships in distress."

18 U.S.C. § 2511(2)(a)(1)

"It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights of property of the carrier of such communication: Provided, That said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks."

18 U.S.C. § 2510(5)(a)

"(5) 'electronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire or oral communication other than - -

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;"

§§ 817.481, 817.482 Florida Statutes

817.481 Credit cards; obtaining goods by use of false, expired, etc.; penalty

◆ ◆ ◆

(2) It shall be unlawful for any person to avoid or attempt to avoid or to cause another to avoid payment of the lawful charges, in whole or in part, for any telephone or telegraph service or for the transmission of a message, signal or other communication by telephone or telegraph or over telephone or telegraph facilities by the use of any fraudulent scheme, means or method, or any mechanical, electric, or electronic device.

(3)(a) If the value of the property, goods, or services obtained or which are sought to be obtained in violation of this section is one hundred dollars or more, the offender shall be deemed guilty of grand larceny.

(b) If the value of the property, goods, or services obtained or which are sought to be obtained in violation of this section is less than one hundred dollars the offender shall be deemed guilty of petit larceny.

817.482 Possessing or transferring device for theft of telecommunications service; concealment of destination of telecommunications service

It shall be unlawful for any person knowingly to:

(1) Make or possess any instrument, apparatus, equipment or device designed or adapted for use for the purpose of avoiding or attempting to avoid payment of telecommunications service in violation of section 817.481, Florida Statutes; or

(2) Sell, give, transport, or otherwise transfer to another, or offer or advertise to sell, give, or otherwise transfer, any instrument, apparatus, equipment, or device described in subsection (1), or plans or instructions for making or assembling the same; under circumstances evincing an intent to use or employ such instrument, apparatus, equipment, or device, or to allow the same to be used or employed, for a purpose described in subsection (1), or knowing or having reason to believe that the same is intended to be so used, or that the aforesaid plans or instructions are intended to be used for making or assembling such instrument, apparatus, equipment, or device.

(3) Any person who shall make or possess, for purposes of avoiding or attempting to avoid payment for long distance telecommunications services, any electronic device capable of duplicating tones or sounds utilized in long distance telecommunications shall be guilty of a felony of the third degree punishable as provided in § 775.082, § 775.083 or § 775.084.

(4) Any person violating the provisions of subsections (1) and (2) is guilty of a misdemeanor of the first degree, punishable as provided in § 775.082 or § 775.083.

(5) Any such instrument, apparatus, equipment, or device, or plans or instructions therefor, referred to in subsections (1), (2), and (3), may be seized by court order or under a search warrant of a judge or magistrate or incident to a lawful arrest; and upon the conviction of any person for a violation of any provision of this act, or § 817.481, such instrument, apparatus, equipment, device, plans or instructions either shall be destroyed as contraband by the sheriff of county in which such person was convicted or turned over to the telephone company in whose territory such instrument, apparatus, equipment, device, plans or instructions were seized.

Georgia Code § 26-1807

26-1807. Theft of services. — A person commits theft of services when by deception and with the intent to avoid payment he knowingly obtains services, accommodations, entertainment, or the use of personal property which are available only for compensation.

North Carolina G.S. 14-113.4, 14-113.5

§ 14-113.4. Avoiding or attempting to avoid payment for telecommunication services. — It shall be unlawful for any person to avoid or attempt to avoid, or to cause another to avoid, the lawful charges, in whole or in part, for any telephone or telegraph service or for the transmission of a message, signal or other communication by telephone or telegraph, or over telephone or telegraph facilities by the use of any fraudulent scheme, device, means or method.

§ 14-113.5. Making, possessing or transferring device for theft of telecommunication service; publication of information regarding schemes, devices, means, or methods for such theft; concealment of existence, origin or destination of any telecommunication. — It shall be unlawful for any person knowingly to:

(1) Make or possess any instrument, apparatus, equipment, or device designed, adapted, or which is used

a. For commission of a theft of telecommunication service in violation of this Article, or

b. To conceal, or assist another to conceal, from any supplier of telecommunication service or from any lawful authority the existence or place of origin or of destination of any telecommunication, or

(2) Sell, give, transport, or otherwise transfer to another or offer or advertise for sale, any instrument, apparatus, equipment, or device described in (1) above, or plans or instructions for making or assembling the same; under circumstances evincing an intent to use or employ such apparatus, equipment, or device, or to allow the same to be used or employed, for a purpose described in (1)a or (1)b above, or knowing or having reason to believe that the same is intended to be so used, or that the aforesaid plans or instructions are intended to be used for making or assembling such apparatus, equipment or device.

* * *

South Carolina Code § 16-565.1, 16-565.2

§ 16-565.1. Avoiding or attempting to avoid payment of telecommunications services. — Any person who knowingly avoids or attempts to avoid, or causes another to avoid, the lawful charges or payments, in whole or in part, for any telecommunications service or for the transmission of a message, signal, or other telecommunication over telephone or telegraph facilities:

(1) By charging such service to an existing telephone number or credit card number without the authority of the subscriber thereto or the lawful holder thereof;

(2) By charging such service to a nonexistent telephone number or credit card number, or to a number associated with telephone service which is suspended or terminated, or to a revoked or cancelled credit card number;

(3) By use of a code, prearranged scheme, or other similar strategem or device whereby such person, in effect, sends or receives information;

(4) By rearranging, tampering with, or making connection with any facilities or equipment of a telephone company, whether physically, inductively, acoustically, or otherwise; or

(5) By the use of any other fraudulent means, method, trick or device; is guilty of a misdemeanor and shall, upon conviction thereof, be fined not more than one thousand dollars or imprisoned not more than one year, or both.

§ 16-565.2. Making or possessing device, etc., which can be used to violate § 16-565.1. (1) Any person who knowingly makes or possesses any device or any plans or instructions for making the same which can be used to violate the provisions of § 16-565.1 or to conceal from any supplier of telecommunication service the existence, origin or destination of any telecommunication shall be guilty of a misdemeanor and shall, upon conviction, be fined not more than one thousand dollars or imprisoned not more than one year, or both.

(2) Any magistrate may issue a warrant to search for and seize any such device upon application supported by oath of the complainant which shall set forth the facts upon which the application is based, specifically designating the place and the object of the search or seizure. Any such device seized under warrant or as an incident to a lawful arrest shall after conviction of the owner or possessor thereof be destroyed by the sheriff of the county in which such person was convicted.

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee,	)	
	)	No. 73-3618
	)	No. 74-1146
vs.	)	(Consolidated)
ROBERT PAUL McDANIEL KENNETH ODELL, DONALD GARLAND ODELL and DONALD DEVAL HEATER,	)	MEMORANDUM
	)	(Filed July 17, 1974)
Defendants-Appellants.	)	

Appeal from the United States District for the District of Oregon

Before: KOELSCH and WRIGHT, Circuit Judges, and PALMIERI,* District Judge.

The convictions of appellants Robert Paul McDaniel and Donald Farland Odell for conspiracy to commit wire fraud (18 U.S.C. § 371), and of appellants Kenneth Allen Odell and Donald Deval Heater for conspiracy to commit wire fraud and wire fraud (18 U.S.C. §§ 371 and 1343), are affirmed.

Evidence of appellants' fraudulent "blue-box" calls obtained by the phone company's electronic sensing and recording device was properly admitted. There is no statutory basis for excluding the evidence. Contrary to appellants' contention, 47 U.S.C. § 605 has no application to this case. The first sentence of § 605 does not apply to the security officer who made the recordings. Bubis v. United States, 384 F.2d 643, 646-447 (9th Cir. 1967). And the remainder of § 605, as amended, covers only radio communications. United States v. Baxter, 492 F.2d 150, 166-67 (9th Cir. 1973). Moreover, 18 U.S.C. § 2511(2)(a) (i) authorizes the interception and disclosure of wire communications by the phone company under the circumstances here presented. The monitoring conducted was reasonably limited in duration — illegal calls were recorded for only six days. Compare Bubis, supra (three months excessive), with United States v. Kane, 450 F.2d 77, 84 (5th Cir. 1971) (four days a reasonable period).

* The Honorable Edmund L. Palmieri, United States District Judge for the Southern District of New York, sitting by designation.

Nor is there a constitutional reason for excluding the evidence. The phone company's monitoring of illegal calls placed on its own lines was not state action, and as there was no governmental participation in gathering the evidence, Fourth Amendment standards (particularly a warrant requirement) are inapplicable.

Finally, the search warrant was properly executed. A reasonable reading of the two affidavits presented to the magistrate indicates that the limitation on execution contained in the first affidavit was (sic) implicity discarded because of the subsequent events recited in the second affidavit, and was not intended to condition the execution of the second search warrant.

The judgements are affirmed.

ADDENDA

In March, 1975 the United States Court of Appeals rendered a quite significant opinion in United States v. Clegg, 509 F.2d 605 (5th Cir. 1975). In that decision, the Court reaffirmed its prior opinion in United States v. Hanna, 404 F.2d 405 (1968), cert. denied, 394 U.S. 1015 (1969), which upheld the lawfulness of methods used by telephone companies to gather evidence of the commission of electronic toll fraud.

More importantly, the Court concluded that the evidence gathered by the telephone company was not tainted by government participation in, or preknowledge of and acquiescence in, a private party's (electronic) search and seizure of a type which the government itself, under the circumstances, could not have undertaken. The Clegg investigation was conducted in conjunction with a coordinated, multi-state investigation by a number of telephone companies of various blue box manufacturers, distributors and users. The F.B.I. was engaged in a parallel but separate investigation.

Against defendant's allegations that the telephone company's actions violated his Fourth Amendment rights, the Court stressed that the telephone company gathered its evidence against the defendant wholly independently of law enforcement officials, especially in the area of limited voice recording (of the opening salutations of the conversations of illegally-placed calls). The Court sustained the conviction under 18 U.S.C. § 1343, finding that the telephone company had neither acted jointly with, nor under the direction and control of, law enforcement authorities during the gathering of such evidence.

Another recent decision also upholds such investigative methods. In People v. Mahoney, 47 C.A.3d 699, 122 Cal. Rptr. 174 (1975), the California Court of Appeals not only approved such methods but also approved the telephone company's reinstallation of blue box detection equipment, after initial disclosure of evidence to law enforcement officials, to verify the continuing nature of defendant's fraud, thereby providing some fresh evidence to support the application for a search warrant.

In an as yet unreported decision, United States v. Glanzer, No. 75-1359, June 17, 1975, the United States Court of Appeals for the Ninth Circuit upheld the telephone company's investigative techniques against attack under the Fourth Amendment and Title III. A copy of the text of the Glanzer opinion is attached.

In a decision of the Connecticut Court of Common Pleas, State v. Cutler, No. CR3-19517, April 10, 1975, also approving such techniques, the Court said:

> "Put in its simplest perspective, the position of the defendant in this case seems to be as follows: He may employ the use of sophisticated electronic equipment for the purpose of defrauding the telephone company and depriving it of its lawful tariff for the use of its equipment, but the telephone company may not be heard to complain or attempt in any way to prevent him or protect its property rights, and if it should do so by the use of its own sophisticated equipment, the defendant cries 'foul'. If this is the law, the same shall have to be declared by some court other than this one."

Finally, in the recent decision of Unites States v. Sorota, 515 F.2d 573 (5th Cir. 1975), the Court of Appeals sustained the District Court's finding that its comparison of the brief salutation on the telephone company's voice recordings with a voice exemplar of the defendant was sufficient, in light of all the other evidence, to establish that the defendant made the calls in question.

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Appellee, v. KENNETH W. GLANZER, Appellant.	)	No. 75-1359 Filed June 27, 1975

OPINION

Appeal from the United States District Court for the Western District of Washington, at Seattle.

Before: CARTER, GOODWIN, and KENNEDY, Circuit Judges.

PER CURIAM:

Kenneth W. Glanzer was convicted of fraudulently using an electronic device ("blue box") to bypass telephone billing equipment in violation of 18 U.S.C. § 1343.

Glanzer challenges the receipt into evidence of transcripts of telephone-company-wiretap tapes. He contends that the telephone company's surveillance and tapings violated his Fourth Amendment rights, and that the tapes should not have been received into evidence because segments thereof had been destroyed. Neither point is well taken.

The Fourth Amendment questions are fully answered by the recent decision in United States v. Clegg, 509 F.2d 605 (5th Cir. 1975). The electronic surveillance of Glanzer's

telephone traffic, like that of Clegg, was accomplished by telephone-company technicians without governmental assistance or participation. This type of telephone-company security activity not only does no violence to rights protected by the Fourth Amendment, but is specifically authorized by statute. See 18 U.S.C. 2511(2)(a)(i).

The tapes were fragmentary, but the evidence showed that the telephone company did not undertake to monitor all of Glanzer's telephone traffic. The company chose to concentrate on facts relevant to the circumvention of its billing system rather than upon the total content of the wire traffic. Glanzer has failed to suggest any reasonable hypothesis upon which more complete monitoring or preservation of monitored traffic could have helped his defense, and we can think of none. There was no error in receiving the challenged tapes.

The assertion that the evidence was insufficient to support the conviction is frivolous, as is the assertion that Glanzer was entitled to an instruction on a so-called lesser included offense. The only lesser offense suggested, a misdemeanor under 47 U.S.C. § 220(e), is committed when an individual makes a false entry in records that a regulated communications carrier is required by law or regulation to maintain. The misdemeanor is not only not "included", it is not related to Glanzer's offense.

Affirmed.