



Exploding The Phone

db700

www.explodingthephone.com

Bibliographic Cover Sheet

Title **A Summary of Telecommunications Fraud from 1980 Until Present**

Publication *Pacific Bell Corporate Security*

Date 1992-03-25

Author(s) Venn, John E.

Abstract History of telecommunications fraud from 1980-1992. Touches briefly on electronic toll fraud.

Keywords Blue Box; Black Box; John E. Venn; Pacific Telephone

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.

San Francisco, March 25, 1992

J. A. LUZIER, Director-Revenue and Collection Management:

Dear Jackie,

Telecommunications fraud probably began with the introduction of telephone service, taking advantage of some weakness built into the first telephone system. Over the years fraud has migrated from one system weakness to another, migrating when the system weakness is corrected or as another type of fraud becomes more attractive. Telecommunications fraud has often been compared to the air in a balloon, in that when you push on a balloon there is a visible dent but the air mass is the same, the air has just migrated from the point of pressure.

Fraud-Early 1980s

Several different types of telecommunications fraud were being committed in the early 1980s. The most notable types of fraud were Electronic Box, Calling Card, Third-Number-Billing, Feature Group A (FGA) and Feature Group B (FGB). Computers were proliferating and the first instances of computer assisted code "Hacking" were noted.

ELECTRONIC BOX FRAUD

"Electronic Box" fraud is a term used to describe a type of fraud that employed a device (usually built into a box) which took advantage of a weakness built into the telephone system to make/receive free telephone calls. Electronic Box fraud includes, but is not limited to; "Blue Box" fraud, (used to place calls by defeating supervision on single frequency trunks); "Black Box" fraud, (used to receive toll free calls by blocking or resisting the passage of Direct Current and providing a means to trip ringing); and "Red Box" fraud, (duplicates the frequencies produced by coin telephones to indicate the denomination of coins deposited for calls). "Blue" "Black" and "Red" boxes were so named because of the color of the first device seized.

Initially Electronic Box fraud, committed in a Pacific Bell area (when detected) was investigated by one of the four Technical Investigators. The cases usually involved telecommunications

surveillance on the suspect's line, the service of a search warrant and prosecution. The sentence imposed by the court was usually not severe. The losses attributed to Electronic Box fraud were small when compared to losses currently suffered due to subscription fraud.

Successful investigations did not deter Electronic Box fraud. Blue Boxes were mass produced outside the United States and were sold to eager purchasers on both the East and West coasts. Most users began using the Blue Boxes at coin telephones which made apprehension unlikely.

MESSAGE FRAUD

Calling Card fraud (the fraudulent use of another's Calling Card) and Third-Number-Billed fraud (billing a call to another subscriber's telephone number without the subscriber's permission) were usually committed by individuals wishing to place free telephone calls. Calling Card fraud and Third-Number-Billed fraud were usually grouped together and called "Message fraud". Message fraud was often committed from military bases, college campuses, bus terminals, and just about any other location where persons, far from home, would congregate.

In the early 1980s Pacific Bell Security had two managers, twelve investigators and four clerks assigned to investigate fraud. The investigators worked on Message fraud which included Calling Card Fraud and Third-Number-Billed fraud. The investigators were responsible for investigating, rebilling and collection. The duties of the Message fraud investigators were similar in nature to those of a collection agency investigator. Four of the above investigators were responsible for investigating network fraud (Electronic Box fraud) and the facilitation of court ordered services for law enforcement agencies.

Message fraud cases were referred to Pacific Bell Security by the Message Investigation Bureau when the cases met a predetermined criteria. Many of the referred cases were not workable for a number of reasons and were immediately "Z'd" or closed. The remaining cases were worked and at some point either rebilled or closed without rebilling. Due to the lack of any real evidence, few message fraud cases ever resulted in any prosecution.

Losses due to Calling Card fraud were reduced with the introduction of calling thresholds and verification. Verification of Third-Number-Billed calls from coin telephones deterred that type of fraud.

FEATURE GROUP A & B FRAUD

Shortly after the first alternative long distance company offered Feature Group A (FGA) service Pacific Bell Security was advised of FGA fraud. FGA (and later FGB) service was established to allow subscribers access to long distance carriers other than AT&T. A customer used FGA service as follows: the customer

JUN 20 1985 02:18 PM PACIFIC BELL CORPORATE SECURITY P.4/8
dialed a local number (which connected the subscriber to the long distance carrier's network), received a distinctive tone, dialed a PIN assigned by the carrier to the subscriber and then dialed the terminating number. If the customer had dialed a valid PIN the call would complete. If the customer had used an invalid PIN the call would not complete.

FGA (FGB) companies were not aware of which telephone number was originating a call, they would only know which PIN was being used to bill the call. Since, initially FGA (FGB) companies used very short PINs (some only four digits) it was a simple process to program a computer to attempt every possible PIN and at some point the computer operator would possess every working PIN currently assigned by the company.

At first the computer criminals (commonly referred to as "Hackers") used the stolen codes for their own personal telecommunications needs but eventually began sharing the stolen codes with other hackers via computer bulletin boards.

MISCELLANEOUS FRAUD

A number of other types of telecommunications frauds were committed during the early 1980s. A few are: mobile telephone fraud, silver box fraud, code calling, coin refund fraud, clip-on fraud, boiler room fraud (subscription fraud) and various types of network fraud.

Divestiture Until Present

On January 1, 1984, AT&T divested and the regional telephone companies, including Pacific Bell, became separate Local Exchange Companies (LECs). The long distance fraud that we used to investigate because we were a part of AT&T would now be investigated based upon contracts with AT&T (we also were investigating on behalf of FGA and FGB companies under the 175T Tariff).

Electronic Box fraud cases were still being investigated for AT&T, on a contract basis, but due to mechanical fixes, with less and less frequency.

Two fixes were employed to slow and ultimately stop Blue box fraud. The first was short term and involved the installation of 2600 Hz filters on trunks leaving central offices. The second, a long term solution, was technological changes in network signaling which eliminated signal frequency signaling.

Black Box fraud was significantly deterred by network changes which caused an off-hook telephone line to time out after a few seconds.

Red Box fraud has been deterred by modern coin telephone sets which can detect whether coins are deposited or not.

CELLULAR TELEPHONE FRAUD

Cellular telephone service was becoming very popular and right on its heels was cellular fraud. The initial design of cellular systems made fraud easy to commit. There was not positive verification and a fraud suspect could use any number not currently programmed in to a "bandit" list and the call would go through.

Two numbers are required to place a cellular call. A telephone set identification number and a number assigned to the telephone user (and programmed into the set). Early cellular telephones were manufactured with an identification number built into the set which could not be removed without destroying the telephone set. Later cellular telephones were manufactured with changeable set identification numbers. Unscrupulous cellular installers were then able to program the identification number and assigned cellular number of a valid subscriber into another cellular telephone which could then be sold to a co-conspirator. The legitimate cellular subscriber would then be billed for the call.

Positive verification systems and other security enhancements have helped deter some cellular fraud but fraud continues to plague the cellular industry.

AT&T CONTRACTED MESSAGE FRAUD INVESTIGATORS

AT&T initially contracted with Pacific Bell Security for one full-time fraud investigator and subsequently contracted for a second investigator. The fraud investigators were responsible for working on message fraud cases and other cases as directed by AT&T Security.

The second investigator was added in 1988. At that time Technical Investigations had five Senior Investigators assigned to investigate network abuse, investigate on behalf of contracting common carriers and to provide court ordered assistance to law enforcement; two Assistant Investigators assigned to work AT&T Message fraud; and one Security Specialist assigned to various office duties necessary to support the Senior and Assistant Investigators.

"ORGANIZED CRIME" FRAUD SCHEMES

Two fraud schemes were identified which impacted AT&T, Pacific Bell and other common carriers. They were the "Tony White Scam" and "Call/Sell Operations".

The "Tony White Scam" is perpetrated by persons who call legitimate telephone company subscribers and purport to be AT&T or Pacific Bell Security investigators investigating Calling Card Fraud. The criminal usually tells the subscriber that they have thousands of dollars in calls on their (subscriber's) bill to some foreign country. The criminal then asks for the

subscriber's PIN number. Subscribers often are talked into parting with their PIN number. P.6/9

Call/Sell operations are lucrative "organized crime" operations intent on selling fraudulently obtained telephone service to willing buyers at coin telephone locations.

Call/Sell operations are organized as follows:

1. Person(s) obtain the means to place fraudulent long distance telephone calls. These criminals use several different methods to obtain the means to place free calls; a few are: computer hacking, "Tony White Scam", looking over a person's shoulder at a coin telephone, obtaining PBX codes from business employees, obtaining fraudulent service through the telephone company (subscription fraud), etc.
2. Person(s) buy the means to make fraudulent calls from the above person(s), and then resell the means to co-conspirators at coin telephone locations, which are in areas where persons who have relatives in foreign countries congregate.
3. Person(s) sell the means to make fraudulent telephone calls to knowing buyers for a fraction of what the telephone company would charge for the call. Further, due to the fact that Calling Card numbers and PBX DISA (discussed below) numbers have a short fraud life, criminals at coin telephones will often sell those numbers as well.

Pacific Bell Security utilized a number of deterrent methods to attack the "Tony White Scam" and Call/Sell schemes. A few of which were: a number of individuals committing the "Tony White Scam" were arrested based upon Security's investigation, one individual while making several "Tony White" calls; Security worked with a television reporter to complete two separate news series on Call/Sell fraud; Security worked with Pacific Bell Media Relations to publicize the "Tony White" scheme and Call/Sell fraud; Pacific Bell Security has worked with several police departments to make "sweeps" at coin telephone locations, resulting in the arrest of over 300 suspects who were selling or buying fraudulent phone calls. Nevertheless, the "Tony White" and Call/Sell fraud schemes have increased.

These two schemes are popular for a few reasons. They are very lucrative, easy to commit, there are no start-up costs and there is little likelihood of apprehension or prosecution.

SUBSCRIPTION FRAUD

Subscription fraud used in conjunction with Call/Sell fraud was first noted in California during an intelligence gathering investigation in Los Angeles. A Pacific Bell Security

Investigator and an AT&T Security Manager were visiting coin telephone locations (in an undercover capacity) attempting to purchase Calling Cards. They were approached by an individual who offered to sell them a call to anywhere in the world, but he stated he would have to place the call through his associate. The Investigator was able to obtain the telephone number of the associate and later was able to determine that the telephone service had been obtained under a fictitious name for the purpose of committing fraud.

Subscription fraud is not a new type of fraud. It has been used in boiler room operations for years. What is new is organized subscription fraud rings, such as those who commit Call/Sell fraud or who perpetrate the "Middle East Subscription Fraud" scheme (which will be discussed later).

Persons intent on committing subscription fraud usually rent one or more residence/business locations (rent and deposit usually paid in cash) and then apply for telephone service under a fictitious name. They often will obtain matching name and Social Security number in order to pass our verification system (used by the Business Offices). The service ordered usually will include: Call Waiting, Three-Way-Conference Calling, and one or more Calling Card numbers.

Subscription fraud suspects usually will wait a week or so and order additional service. Further, when the telephone company becomes aware of the large volume of calls originating from the subscription fraud site and a Service Representative calls, a suspect will attempt to dissuade the Service Representative from taking any immediate action. Subscription fraud suspects will offer to come to the Business Office and pay or provide identification (anything to stall a disconnect). This allows the suspect to rent another location and prepare to move upon disconnection of the telephone service by the telephone company.

MIDDLE EAST FRAUD

Certain parts of the Middle East cannot call other parts of the Middle East directly. For example, a person in Israel cannot call any of the Arab neighbors directly. In order to place calls economically from one Middle Eastern country to another, telecommunications criminals triangulate calls through the United States.

Persons in the Middle East go to locations that are advertised in newspapers and other periodicals. The locations are equipped with numerous telephones. Persons are asked for the telephone number they wish to call. An employee of the person orchestrating the Middle East scheme places a call to a subscription fraud location in the United States, usually using a stolen Calling Card number or some other fraudulent method. A person in the United States (at the fraudulent site) places the call to the terminating number by using the Three-Way-Conference Calling feature. The person placing the call from the Middle

P.8/9
East pays the person at the originating location. The money from the calls is given to the person orchestrating the scheme who subsequently pays the employees.

THE "AMIGO" CASE

The first "Middle East" scheme discovered operating in Pacific Bell territory was known as the "Amigo" scheme. The Amigo scheme was investigated by a Pacific Bell Senior Investigator and, based upon his investigation, a Search Warrant was served. Three people, including the ring leader ("Amigo"), were arrested. "Amigo" was a nickname given to the ring leader when he was operating in Texas, allegedly where he started the illegal scheme. "Amigo" is from Middle Eastern descent. The loss suffered due to Amigo's ring was estimated at 10 million dollars, but since the time of the arrest the estimate has increased.

There have been several "Middle East" subscription fraud operations identified since "Amigo".

Subscription fraud is difficult to investigate and it is even more difficult to find a law enforcement agency to prosecute the case. Pacific Bell has taken a number of steps to deter subscription fraud, including Positive ID, a system to track special feature usage to the Middle East, and more aggressive disconnects for suspected fraud or non-payment, etc. Subscription fraud is very lucrative and there is little risk of arrest.

PBX

Private Branch Exchange (PBX) fraud takes advantage of poor system design or failure to use adequate security features in some PBXs. The most often compromised feature of a PBX is Direct Inward Switch Access (DISA). DISA is used by businesses to provide economical long distance service to their employees who are away from the office. To use DISA, an employee usually calls a local or toll free number, which is answered by the PBX DISA feature. The employee then inputs a number assigned to the employee by the business. The employee next hears a stutter dialtone and can then dial any number that could normally be called from the business location.

Telecommunications criminals migrated to PBX fraud when long distance companies increased the security on their FGA and FGB systems. Businesses were not aware of the telecommunications fraud threat to their systems and usually did not take adequate precautions to protect their systems. Some businesses did not even use employee codes, they would just have dialtone sitting waiting for any caller to use.

The first major PBX fraud discovered in California was perpetrated by a college student from Pakistan who was residing in an apartment in Los Angeles. The student had five telephone lines in his apartment which he had connected to a homemade

JUN 28 '93 02:20 PM PACIFIC BELL CORPORATE SECURITY P.9/9
conferencing board. Other students would call his apartment and he would place their call for them, fraudulently, through a company's PBX's DISA feature. The criminal kept very accurate records (so he could bill his customers) and through the records, it was established that he had been responsible for a half-million dollars in fraud.

Today, it is not unusual for a business to suffer a half-million or even a million dollar PBX fraud loss in a month.

Computer criminals are able to use the programs, initially used to discover FGA and FGB PINs, to discover DISA codes.

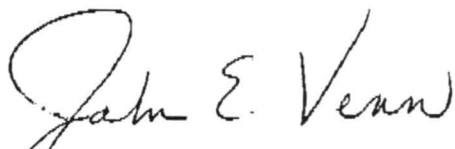
Pacific Bell Security currently assists businesses that suffer PBX fraud when we are served with proper legal process (Pacific Bell is not a victim). Further, Security assists Pacific Bell Marketing by consulting with the Marketing Representatives and their customers on PBX security.

CONCLUSION

Currently, Technical Investigations is staffed as follows: one Manager, four Senior Investigators and two Assistant Investigators. The group spends about 90 to 95 percent of its time on the facilitation of court ordered services for law enforcement. The remainder is spent on Pacific Bell investigations and contracting common carrier trap, number search or Dialed Number Recorder service.

This paper is a summary of the significant fraud schemes encountered by the Pacific Bell Security Division over the last twelve years. It would take a book to cover, in detail, the fraud schemes discussed here or the numerous other schemes not discussed.

Fraud migrates for a reason. It migrates to system weaknesses which allow the fraud suspect to commit the maximum amount of fraud, with the least amount of effort, with little or no risk of apprehension or prosecution. When a fraud scheme meets the above criteria, no amount of investigation will deter it, only system improvement has been and will continue to be effective in combating it.



JOHN E. VENN
Manager-Technical Investigations