Doing time on the telephone line.

Print

Title Annotation: *includes related article; phone fraud*
Author: *Anderson, Langford*
Date: *Feb 1, 1990*
Words: *2760*
Publication: *Security Management*
ISSN: *0145-9406*

DOING TIME ON THE TELEPHONE LINE

WHEN 13 PERSONS PLEADED guilty or were convicted last fall of marketing 1,500 stolen long-distance access codes, the estimated loss to the five victimized carriers was $19 million. Trials were held in Honolulu and 14 mainland cities, with sentences ranging from nine to 46 months in prison. The trial of the six remaining defendants in San Francisco that began in December has not reached judgment.

One carrier initiated civil action and received awards in the millions of dollars. While this case is the largest of its type in history, widespread annual theft of services has been plaguing the industry for 20 years, with new versions of crime cropping up as new defenses are introduced.

"The first telecommunications fraud that we noticed consisted of college students wanting to call their families, or their girlfriends or boyfriends, so they started using credit card numbers they had gotten," says Joe Horvat, area manager of the risk management division of Southwestern Bell Telephone Company. "To make a call in those days, you had to go through an operator, who had no way to verify whether the simple code number that was used was valid."

AT&T responded to the rapid growth of phone fraud in early 1971 by beefing up security. "We lost $50 million in Southwestern Bell's territory: Kansas, Missouri, Arkansas, Oklahoma, and Texas," says Horvat, who joined Southwestern Bell 23 years ago and has been in security since 1971.

From 1970 to 1973, US telecommunications security investigators found themselves with work loads of 50 to 100 cases that ranged from losses of a few hundred dollars to $10,000. The Bell System hired former police officers, accountants, and technicians in an effort to blend a variety of useful skills on investigation teams.

At first the plan was to deter abuse by aggresively prosecuting suspects and publicizing student arrests in campus newspapers. Military installations were also targeted. But even with improved credit card coding and other carrier precautions, abusers soon learned how to beat the safeguards.

Along with credit card abuse, several other versions of telecommunications fraud emerged in the early 1970s. Third-number fraud and code calling, particularly popular with large, cross-country trucking firms, began. Drivers left free messages for their companies by giving operators a predetermined name or phrase.

"The caller would ask the operator to place a collect call for a Fred P. Jones III," Horvat recalls. "The call would be refused, but the name was a code that let the company know a driver had a half load in Nashville en route to Kansas City. This would go on 24 hours a day, seven days a week, and the cost in AT&T operator time was incredible."

Electronic fraud devices first appeared in the early 1960s and became widespread throughout the next decade, particularly in the early 1970s. It took a series of innovative technological developments by the Bell System to defeat them. The devices were named for the color of the first boxes seized but later could be found in any color.

Blue boxes, perhaps the best known, allowed users to place free long-distance calls from any telephone. They had 13 to 15 buttons that simulated tones and contained a transmitter acoustically coupled to a telephone or wired to a telephone line. Blue boxes were defeated by a signal channeling enhancement that Bell had been developing for several years.

Black boxes allowed long-distance calls to be received without being billed. If a user knew when a call was coming in, he or she flipped a toggle switch on the box while the phone was ringing. The box did not allow enough current to return to the originating city to trip the billing computer. The computer thought the phone was still ringing when the long-distance call had actually been completed. The changeover from mechanical to electronic switching systems solved the black box problem.

Red boxes simulated aural system tones that counted the coins deposited in a pay phone. Operators thought the correct amount had been received and connected the call. Red boxes were defeated by upgrading central office equipment so it required more precise tones--plus or minus 1 percent error.

IN THE LATE 1970S, NEW COMPLICAtions began to appear. Computer modems were introduced, and a few hackers emerged with handles such as Captain Crunch, Cheshire Cat, Catalyst, and Susan Thunder. With new technological developments, AT&T fraud investigators were able to identify and prosecute hackers.

The divestiture of the Bell System in 1984 brought new entries to the telecommunications industry--mostly long-distance service providers. These new providers lacked the knowledge and defenses that 13 years of investigative experience and engineering development had given the Bell System. For example, some providers used authorization code numbers that consisted of only four to six digits. The codes could be figured out in a few minutes and passed around.

By the mid-1980s, PCs were less expensive and could be equipped with autodialers. Also, many newcomers simply didn't know that running a telecommunications business inevitably involves certain losses, which many of them began experiencing right away.

In 1985, common carriers rarely worked together to combat crime. Local exchange companies (LECs) were not equipped to offer low-cost investigative services, educational support, or billing analysis. Consumers suspecting phone fraud did not have a national number to call for help and could not share information.

That spring, a few managers from the security departments of 15 long-distance and local telephone companies met in San Francisco and created the Communications Fraud Control Association (CFCA), a nonprofit organization that has established itself as a national clearinghouse for telecommunications crime information. One fact is evident from CFCA's programs: widespread cooperation among injured parties gets results sooner and helps conserve vital company resources.

Today's proliferation of desktop computers and accessories gives anyone who wants to make free long-distance calls more opportunities to steal. Fraudulent calls can now be made faster and in greater volume than ever before.

Newer carriers have aggressively sought to minimize their vulnerabilities, much as AT&T did earlier, and they have largely succeeded. The result is that inventive, well-organized phone phreaks--those who try to steal codes to make free long-distance calls, as opposed to hackers, who try to access data bases to get information--are adopting new, potentially more devastating targets.

Last October, an engineer for a Tennessee civil engineering firm with 350 employees discovered that criminals had used the company's private switch to place hundreds of long-distance calls. The switch, called a private branch exchange (PBX), directs incoming and outgoing calls and can connect company sales representatives calling from pay phones with domestic and foreign clients.

The company was billed $3,000 for inbound 800 line use and $12,000 for calls to the Dominican Republic. "I was totally unaware that this could happen," the engineer said.

The scenario is repeated over and over throughout the United States, as long-distance carriers are no longer the only victims of telecommunication services theft.

Losers range from the Tennessee Valley Authority, with its 35,000 employees, which lost $65,000, to Philadelphia Newspapers Inc., owner of the Inquirer and Daily News, which lost $115,000 in one month last fall. The Denver Post and Christian Broadcasting Network also recently lost big money to PBX abusers.

A computer manufacturer based in the Netherlands but with offices across the United States lost $42,000 on its PBX in three weeks. One manufacturer had 43 PBXs compromised across the country, losing $700,000 in one weekend. Another's system was

hit for $300,000 in one month.

In an earlier case, New York City's Department of Human Services lost $750,000. Department employees rigged the organization's switch to make more than 15,000 unauthorized calls to spots in the United States and 50 other countries, particularly Pakistan, Colombia, and the Dominican Republic.

As Horvat summed it up, "If someone with a magic wand could fix all the problems tomorrow, fraud would move to some other vulnerability we don't know about."

Private switches with access codes of only six or seven digits will continue to be attacked. Abusers route long-distance calls overseas, quickly accumulating charges the systems owner has to pay.

Many PBXs are not equipped to detect irregular activities or block fraudulent calls, making them especially vulnerable. If a system is equipped with a remote access feature used by sales representatives, intrusions by outsiders quickly become an expensive nightmare that worsens with each phone bill. This is true even if the only remote access is the maintenance port used by technicians to adjust and repair system software.

Even if direct inward service access (DISA) and remote maintenance ports are protected by authorization or barrier codes, thieves can easily use a variety of tricks to break through defenses. Once they gain access to a system, phreaks usually sell authorization codes to persons most likely to make international calls: illegal aliens and drug traffickers. The sad part of this scam is that system owners are nearly always unaware of vulnerabilities.

SOLUTIONS TO TELECOMMUNICAtions fraud include intelligent software, which is available to help PBX owners identify, screen, and block fraudulent calls. Simply adding digits to access codes is another precaution, because numbers with fewer than 10 digits cannot hold off today's intruders. A number of manufacturers have gone to 14 digit access codes. Some carriers send technical representatives to customers to reprogram systems, upgrade safeguards, and advise owners to shut their systems down at night and on weekends.

Voice mail fraud is another threat. Criminals are easily defeating or by-passing security codes to take over the mailboxes of voice store-and-forward systems, or voice mail--the electronic bulletin boards of the future. Criminals then exchange lists of long-distance codes without the system owners' knowledge.

Phone phreaks are not the only problem. Paying customers also use voice mail systems to commit a variety of crimes, such as coordinating international drug shipments and marketing bankcard numbers, long-distance access codes, and even prostitution.

To protect voice mail systems, owners should assign each mailbox its own code and perhaps set up five- or six-digit passcodes in a tree system. Software is also available

that terminates a call after three attempts have been made on the system and informs callers to try again when they have the correct number. Then it alerts owners that the attempts have been made.

Just increasing access codes to six or eight digits decreases the probability of deciphering them to one in nine million. Adding as many digits as possible, say between 12 and 15, is ideal.

South Dakota-based industry consultant Marc Tobias says voice mail distributors should load randomly generated data file lists of active mailboxes into newly installed systems. He also advises managers to limit the time mailboxes can go unused and to close surplus units.

A new version of voice mail fraud could cause mailbox owners considerable grief. Last October 31, MCI Senior Manager Jenny Grolemund discovered that systems equipped with a feature allowing callers to bypass the greeting message are especially vulnerable to intrusion. Two days later, CFCA's faxed news weekly Fraud Alert warned readers of the vulnerability.

Bandits have also targeted cellular phone carriers, who first noticed in 1986 that fraud losses were rising faster than they had thought possible. Losses of hundreds of thousands of dollars surfaced in three Northeastern cities, then spread quickly to the South and West. Bandits--the thieves of the car phone industry--began exploiting two inherent weaknesses in roamer services when the system became operational in 1983. Roamer services are provided by cellular companies under reciprocal agreement and allow customers to travel from city to city and still use their car phones.

Lists of network abusers, or negative switch files, were particularly vulnerable then, because they could hold only 1,000 numbers. Another problem was that switches that ran the independent service areas throughout the country could not link an owner's identifying number (NPA NXXX) to the serial number embedded in a particular phone.

In 1984, designers saw the need for more sophisticated protection against fraud and installed a few improvements. Electronic serial numbers (ESNs) were embedded in each car phone set, along with the user's mobile identification number (MIN). Both numbers are verified by the local switch and checked against the negative file each time a customer places a call. If anyone tries to alter the ESN, the mobile phone simply stops operating.

Home carriers identified legitimate customers by first determining if the first seven digits, NPA NXXX, were valid. Next, they compared the ESN with the negative file to see if the set had been identified as a bandit.

But if, for example, a customer of a Washington, DC, cellular company drives to New York City, where the service of another provider may be used through reciprocal agreement, only one number can be validated. Roaming bandits can then more easily

use cellular telephones illegally.

Some customers became unwitting bandits by using their phones when another carrier was providing the service. Deliberately dishonest bandits used other people's phones and, because they knew valid numbers, could call free in other cities. They weren't discovered by the service provider until the bill arrived.

More pernicious intruders altered the electronic serial numbers in a phone's RAM chip. Some even installed many numbers. To counter this fraud, cellular companies aged codes by taking them out of circulation if they went unused for a certain period of time.

Even with more sophisticated bandits on the loose than ever before, however, several technical improvements have stymied most intruders. During the first six months of 1986, 21-digit validation systems that can verify ESNs and MINs were installed. Communication between the industry's two clearinghouses was improved, so the rate of successful verification is now at 98 percent. There are now 2.7 million valid cellular users in the United States.

"Losses began dropping a year ago, and there has been even more of a reduction in the past six months," says Carolyn Schott, manager of roaming services for NewVector Group, US West's cellular carrier in Bellevue, WA. "It's funny, the bandits are more creative, but we're losing less money."

Bruce Bangert, general manager of revenue assurance for PacTel Cellular in Irvine, CA, says fraud losses ran about 20 percent during the first six months of 1988. "Now, with bandits needing to be more knowledgeable of the technology, losses have dropped to about 2 percent."

However, Tobias, an attorney and consultant specializing in pay phone security, tells anyone within earshot that customer-owned, coin-operated telephones (COCOTs) are readily being beaten, and that most Americans don't believe stealing from the phone company is a crime.

"If you purchase one of these wonderful devices for $2,000 and install it outside your store, phone phreaks can simply walk up to it and make free calls," says Tobias.

"It may be 45 days before you get the bill and shut it down. Under all US tariffs, the operator is liable for every call. Single phone losses of $25,000 in a month are no longer rare occurrences."

Tobias was recently called to Fort Lauderdale, FL, to help a vendor who had lost $400,000 in calls to Egypt, Bolivia, and Pakistan on his COCOTs--all within three months. "Red boxes, defeated years ago by Bell Laboratory technology, have been replaced by high-tech ingenuity, often carried out by 14-year-old kids," he says. Other vulnerable devices include mobile phones, automatic teller machines, and private pay phone systems available on ships, trains, and airplanes.

Over the next few years, the Integrated Services Digital Network (ISDN) will be gradually employed in fighting fraud. When fiber optics are installed, ISDN uses a digital system to provide a message that includes originating and terminating numbers, the codes used for billing, and transmission protocol. "ISDN's vulnerabilities to fraud will really be unknown until it is employed," says Horvat. "And we won't know where the holes are ourselves until then."

No one is immune to phone fraud. Modern life revolves around the use of the telephone, and it is more important than ever to keep abreast of new forms of abuse and developments in fraud control.

"Information must be shared," says CFCA President Marty Locker. "Today's abusers are well organized and have developed an efficient network to exchange information and share resources."

Clearly, if telecommunications fraud losses are ever to be controlled, security professionals must continue to find ways to stay ahead of abusers. The key to staying ahead is sharing vital information.

Langford Anderson is director of communications for the Communications Fraud Control Association in McLean, VA, and editor of Fraud Alert and The Communicator.