July 1994
Volume 63
Number 7

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

Louis J. Freeh
Director

The *FBI Law Enforcement Bulletin* (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Avenue, N.W., Washington, D.C. 20535. Second-Class postage paid at Washington, D.C., and additional mailing offices. Postmaster: Send address changes to *FBI Law Enforcement Bulletin*, Federal Bureau of Investigation, FBI Academy, Quantico, VA 22135.

Editor
Dr. Stephen D. Gladis
Managing Editor
Kathryn E. Sulewski
Art Director
John E. Ott
Associate Editors
Andrew DiRosa
Julie R. Linkins
Kimberly J. Waggoner
Assistant Art Director
T.L. Wilson
Staff Assistant
Stephanie Plucker

FBI Law Enforcement Bulletin

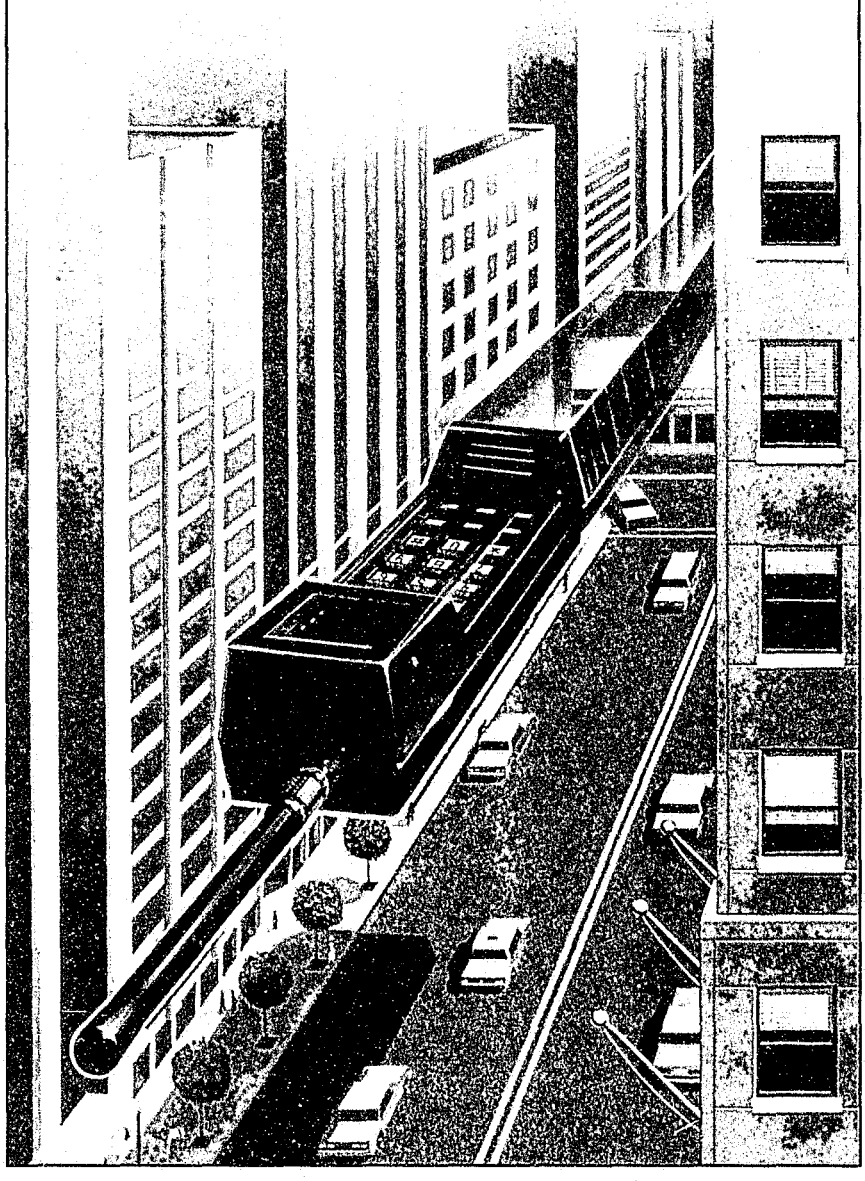
Features

Departments

ISSN 0014-5688 USPS 383-310

Voice-Mail Fraud

By
RONALD R. THRASHER, M.S.



An employee out of town on business phones the employer using the toll-free number. Once inside the voice-mail system, the employee enters a number code that gives access to a dial tone. This allows the caller to make personal, long-distance calls that are ultimately billed to the employer's account. The caller, in fact, commits fraud against the business by using the voice-mail system for personal use.

For many investigators, the use of stolen telephone calling cards and "computer hacking" of telephone billings are familiar offenses. Less known, however, is the fraudulent use of commercial voice-mail services.

Voice mail is the recording callers often hear when they phone a corporate or government office. The recording provides limited instructions on how callers can be connected with an individual, should they need to talk to a real person. More commonly, the recording tells callers how to leave a recorded message in the office's "voice mailbox." These services often include the capability of allowing mailbox holders to phone their own mailbox by dialing a number code (password) to recover messages.

Criminals usually commit voice-mail fraud against businesses equipped with a toll-free (1-800) customer service number that employs one of a variety of voice-mail systems. The fraud takes place when a caller leaves a personal, nonbusiness-related message for another individual within a business' voice mailbox, usually using

the toll-free number, and another individual retrieves the message, again using the toll-free number. The loss is reflected in the long distance calls, many times from overseas numbers, that are charged to the business' or government office's toll-free service.

Fraud Variations

Because telephone long-distance packages offer a variety of customer services, voice-mail fraud has several variations. One type of fraud, detailed in the beginning of this article, occurs when the toll-free service makes available remote access dialing.

Offenders phoning a voice-mail system equipped with remote access dialing can quickly access the code, frequently a four-digit number, through a computer modem. Once they gain access, callers can make personal use of the service to further other criminal enterprises, or to sell the access code for a profit.

The illegal selling of long-distance service is most commonly associated with stolen calling card numbers. Corporations have recorded losses exceeding $1,000 within the first few hours following the report of a stolen corporate calling card.

While the sale and use of remote access dialing codes appears less frequently, this crime is increasing rapidly. The loss to one corporation exceeded $220,000 within the first 13 hours after the fraudulent activation of a remote-access dialing code. Should offenders first access the remote system at the beginning of a 3-day weekend or holiday period, which delays detection, the crime is compounded further.

Offender Profile

A wide range of individuals are likely to commit voice-mail fraud. Young offenders often use voice mail illegally to send chain messages, similar to chain letters of years past. Some individuals simply wish to avoid long-distance charges by leaving and receiving personal messages through the use of a corporation's toll-free voice mail.

Computer "hackers" may attack the system for profit or simply for the thrill of defeating the security safeguards. However, investigators should not envision computer hackers only as college students who break into a security system solely for the challenge of beating the programs. While this still occurs, hackers of all ages usually obtain and enter access codes on computer bulletin boards, newsletters, and specialty magazines as a way of showing off their prowess. This practice gives countless others the means to commit fraud.

Also, it appears that many hackers have become more profit-motivated. Investigations into voice-mail fraud have revealed that these individuals set dollar amounts for access information and then sell the information, usually to other criminals. At times, they auction the information and sell it to the highest bidder.

Of equal interest to law enforcement are hackers who access a system to commit corporate espionage and drug traffickers who are interested in a secure, no-cost message delivery system. These individuals often access voice mail by using a pay phone or stolen mobile equipment to avoid identification through tracing, line identifying, or phone taps.

Investigation

When initiating an investigation into voice-mail fraud,

Lieutenant Thrasher is the Criminal Investigation Commander in the Stillwater, Oklahoma, Police Department.

"Criminals usually commit voice-mail fraud against businesses equipped with a toll-free (1-800) customer service number...."

investigators should first target the mailbox, which often reveals valuable information. They should identify if the fraud was initiated against an existing, seldom-used mailbox or following the installation of a new mailbox. It is also important to know how passwords or number codes are created or changed and if the password to give access to the targeted mailbox was recently changed.

Investigators also need to verify if a computer terminal was used to make a change in the mailbox and if the computer was equipped with a modem. If so, investigators should then determine if access to the computer took place at unusual times (late at night, during lunch, on holidays and weekends, etc.) and who accessed the computer (authorized or unauthorized personnel).

Then, within constitutional parameters, the next step for investigators is to review the voice-mail messages, because many systems record the date and time of incoming messages. Message times can then be compared to toll-free invoices to identify the source and location of incoming calls. While a good avenue for investigators to pursue, this may pose some difficulty if the fraud originates from a public phone or stolen mobile equipment.

Investigators should not overlook possible employee involvement. Indicators of employee involvement include origin and destination of toll calls, time of computer access, password changes, and creation of new mailboxes. Investigators should also look for answers to the following questions:

- Was a system change made, without use of a modem, during the lunch hour, after hours, during a weekend or holiday, or at a time the business was not normally open?

> ***"A wide range of individuals are likely to commit voice-mail fraud."***

- Who would have access to either the computer or the telecommunications system, or both, and had the information or expertise to make the change?
- Who within the organization might be in dire financial straits or living beyond their income and could benefit from the fraud?

Prosecution

Many State statutes define fraud as the obtaining of money, property, or services by trick, deception, or false pretenses. This provides prosecutory authority for communication offenses.

Because voice-mail fraud may cross several jurisdictions, State and local prosecutors should also consider contacting a Federal prosecutor for assistance. Federal authority can be found within Title 18, U.S. Code, Sec. 1343. The code reads, in brief:

> "Whoever, having devised or intended 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 writing, 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. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both."

Prevention

The excessive financial losses traced to voice-mail fraud can be prevented, or at least diminished, when companies take simple precautions. If a business has already been victimized, investigators can offer the following strategies to prevent further losses:

- Monitor abnormal calling patterns and toll-free service costs
- Enhance security and access codes to include more than the standard four digits
- Change codes frequently
- Assign corporate communication security to a single individual

- Make all employees more "security conscious"
- Block system access calls from locations outside the business service area and during those times the business is closed
- Develop a corporate plan in the event communication fraud is suspected, which includes immediate notification to law enforcement and a determination to prosecute offenders
- Guard security passwords and control access numbers
- Remove modem access for administrative system changes.

Conclusion

Communication fraud poses many challenges not encountered by the criminal investigator in more traditional crimes. Although losses attributed to telecommunication fraud reported by long-distance services exceed $1 billion annually, many law enforcement investigators are unfamiliar with voice-mail fraud.

Technological breakthroughs in communication allow the private sector to offer new and advanced products and services. This underscores the importance for law enforcement to recognize communication as a major interest of the criminal entrepreneur. Investigators must, therefore, broaden their knowledge of communication fraud, especially voice-mail fraud, to identify, apprehend, and prosecute the technologically advanced offender. ✦

Crime Data

Crime Decreases in 1993

According to preliminary Uniform Crime Reporting figures, the number of serious crimes reported to law enforcement agencies decreased 3 percent in 1993 when compared to 1992 data. This decrease continued the trend from 1992, when overall crime was down 3 percent from the previous year.

A Crime Index composed of violent and property crimes measures serious crime. Last year, violent crime dropped 1 percent, while property crime decreased 3 percent.

Among the individual violent crime offenses, only murder registered an increase from the 1992 level, one of 3 percent. Forcible rape fell 4 percent, robbery dropped 2 percent, and aggravated assault remained unchanged. For property crimes, arson and burglary each declined 6 percent, motor vehicle theft dropped 4 percent, and larceny-theft fell 2 percent.

Declines in overall Crime Index totals occurred in all regions of the country. The Northeast registered a 5-percent decline; the Midwest, a 3-percent drop; and the South and West, a 2-percent decrease each.

All population groupings experienced Crime Index decreases during 1993. Cities with populations over 1 million recorded the greatest decline, one of 5 percent. The decreases reported by rural and suburban county law enforcement agencies were 3 percent and 2 percent, respectively. ✦

Source: FBI Uniform Crime Reporting Program, Press Release, "Crime Trends, 1993 versus 1992," May 1, 1994.