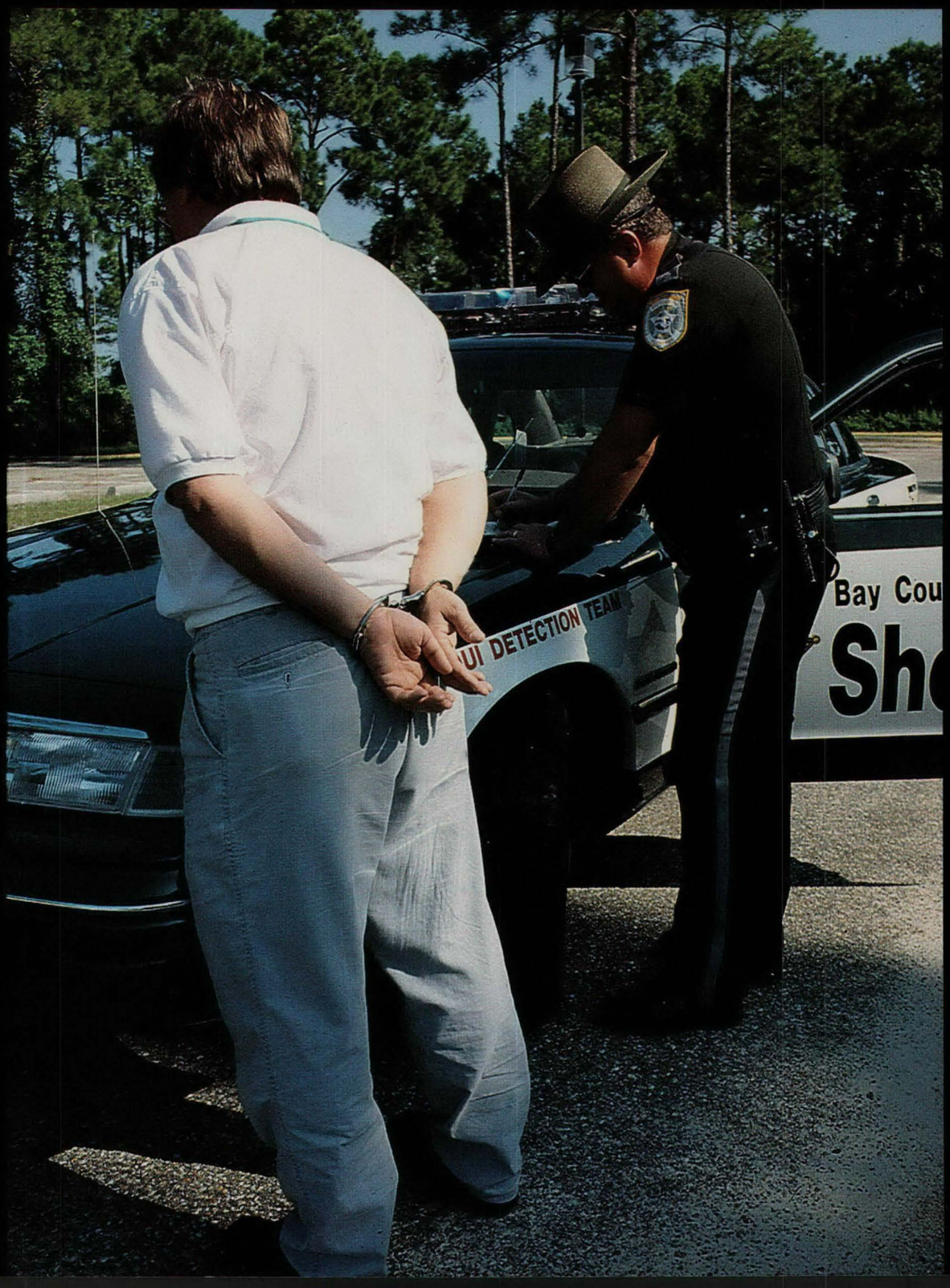
U.S. Department of Justice
Federal Bureau of Investigation

May 1998

FBI Law Enforcement BULLETIN

Investigative Detention



May 1998
Volume 67
Number 5

**United States
Department of Justice
Federal Bureau of
Investigation
Washington, DC
20535-0001**

**Louis J. Freeh
Director**

The *FBI Law Enforcement Bulletin* (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 935 Pennsylvania Avenue, N.W., Washington, D.C. 20535-0001. Periodical postage paid at Washington, D.C., and additional mailing offices. Postmaster: Send address changes to Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Madison Building, Room 209, Quantico, VA 22135.

Internet Address
leb@fbi.gov

Cover photo
© K.L. Morrison

Send article submissions to Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Madison Building, Room 209, Quantico, VA 22135.

FBI Law Enforcement BULLETIN

Features

Departments

ISSN 0014-5688 USPS 383-310

Telecommunications Fraud
Opportunities for Techno-Criminals

By JOHN T. O'BRIEN, M.S.

Photo © Photodisc

The 1990s have been called the communications decade. New communication systems spring up seemingly overnight, and existing systems have expanded rapidly. This has been a great convenience and even a lifesaver for many citizens. At the same time, it has created opportunities for fraud.

Whether they use false information to establish customer accounts or employ technologically sophisticated means to steal account information, techno-criminals target both innocent citizens and telecommunications carriers with a variety of fraudulent schemes. Yet, despite the advanced technology used by some offenders, law enforcement agencies can combat these crimes using traditional methods. Successful resolution of cases involving telecommunications fraud often depends on partnerships with service providers, combined with an understanding of the nature of the crimes.

Telecommunications Systems

The communication systems in the greatest demand by consumers are cellular telephone and personal communication services (PCS). Although cellular telephone and personal communication services differ in their technology and the regulatory requirements, the two terms often are used interchangeably. Both are portable methods of communication between a moving subscriber and the landline telephone system. In both services, subscribers use a portable handset to establish a connection through a cell site. The cell site serves as a base station for a specific geographic area called a cell. In a large city, a cell may cover only a few blocks. In a rural area, one cell may encompass several square miles. As

a moving subscriber travels from one cell to another, the connection automatically transfers to the new cell site.

Types of Fraud

Cellular telephone and PCS fraud can be divided into low-tech fraud and high-tech fraud. Subscription fraud is the least sophisticated and the most common form of fraud. One consulting firm estimated that subscription fraud accounts for 80 percent of all PCS fraud.[1] Individuals establish service using false credentials, including their names, social security numbers, credit references, and salary information. They use the service but never pay for it. The carrier eventually disconnects the service but never recovers the costs or lost revenue.

Though disconnected by the home carrier, these individuals can continue to place calls by doing so from outside the home carrier's service area. The time delay between the delivery of this roaming service and the report of the service to the home carrier makes this type of fraud, called roaming fraud, possible. Roaming fraud proves especially costly because the home carrier remains responsible for paying the charges owed to the carrier that provided the roaming service. All cellular telephone and PCS carriers will be required to provide nationwide roaming service by June 1999. This will create greater opportunities for roaming fraud.

The most prevalent form of high-tech fraud is cloning fraud. Individuals acquire legitimate account information either by outright theft from a carrier or by on-the-air interception. On-the-air interception of account information is possible whenever a cellular or PCS telephone is turned on, even if it is not being used.

Armed with someone else's account numbers, the thief programs them into a cellular or PCS telephone, creating a clone of the legitimate phone. After the home carrier has disconnected the service, the user may continue to place calls by using roaming service, thus committing roaming fraud.

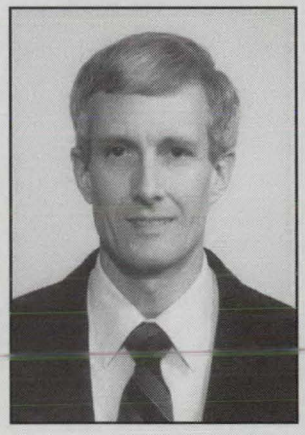
Any cellular telephone or PCS network is vulnerable to low-tech fraud. The vulnerability of a cellular or PCS network to high-tech fraud depends on the technology the carrier employs.

Vulnerability to High-tech Fraud

Most cellular telephone carriers use advanced mobile phone service (AMPS). AMPS transmits an unencrypted analog frequency modulated (FM) signal, which can be intercepted with any FM receiver, such as a scanner. Scanners manufactured or sold in the United States normally block these frequencies; however, they can be modified, often as easily as removing one or two wires. A television set with an ultrahigh frequency tuner (UHF) also can be modified to receive cellular telephone frequencies. As a result, AMPS technology is especially vulnerable to cloning fraud and eavesdropping.

Cellular telephone carriers in larger cities employ a second-generation cellular telephone technology called time division multiple access (TDMA). It digitizes the subscriber's account information and voice and turns them into a high-speed stream of binary digits. A telephone using TDMA technology transmits its digitized

> ***"Subscription fraud is the least sophisticated and the most common form of fraud."***



Special Agent O'Brien serves in the FBI's Washington, D.C. office.

information only during an assigned time slot a mere several thousandths of a second long. These binary digits sent in intermittent bursts of incomplete information make TDMA less vulnerable to cloning fraud and eavesdropping. The carrier also may encrypt the signal, adding even more security.

Some TDMA carriers do not completely cover their service areas. In these areas, subscribers use dual-mode telephones that transition to AMPS if TDMA is not available. When this happens, the telephone becomes more vulnerable to cloning fraud and eavesdropping.

Personal communication services carriers use one of several different technologies on their networks. The two most common are global system for mobile communications (GSM) and code division multiple access (CDMA). In GSM communications, a subscriber's account information and voice are digitized and transmitted during an assigned time slot. The account information is stored in a subscriber identity module (SIM). The SIM is either a postage-stamp size, which remains inside the telephone, or a credit-card size, which the user inserts before making a call and removes afterward.

When a subscriber initiates a telephone call, the GSM network challenges the SIM in a process known as authentication. If the SIM responds correctly, the GSM network connects the call. GSM calls are encrypted using information stored in the SIM.

Experts believe that GSM remains immune to cloning fraud. Even if an individual obtained legitimate account information by outright theft, the expense and effort required to counterfeit a SIM probably would not prove cost-effective for the thief. However, recent reports indicate that some enterprising individuals have developed a way to counterfeit SIMs using a laptop computer and other peripheral equipment.[2]

> ***"...techno-criminals target both innocent citizens and telecommunications carriers with a variety of fraudulent schemes."***

In theory, GSM should be immune to roaming fraud, as well because a GSM carrier can require that the home system verify every challenge and response of a roaming subscriber. In practice, however, authenticating every roaming call adds considerable nonbillable communications to an already-overloaded network. As a result, some carriers do not require home system verification. Without it, a fraudulent subscriber can continue to use roaming service even after being disconnected by the home carrier.

CDMA, the second type of PCS technology, makes unauthorized reception difficult. CDMA first digitizes the signal then adds the subscriber's code to these digits. Only a CDMA receiver with the subscriber's code can receive the transmission. CDMA transmits subscriber information over the same band of frequencies at the same time but uses unique codes to differentiate subscribers.

Although it offers an inherent degree of privacy, CDMA is not considered secure unless the signal also is encrypted. Many carriers who employ CDMA technology plan to incorporate encryption into their services. Still, after several weeks of effort, the research team from a consulting firm that specializes in cryptography broke the encryption scheme used in CDMA and TDMA.[3] Nevertheless, CDMA is considered protected against unauthorized interception of account information and conversations.

The Cost of Fraud

The Cellular Telecommunications Industry Association (CTIA) estimated that PCS and cellular fraud cost carriers $440 million in 1994, $650 million in 1995, and $710 million in 1996.[4] Fraud can be divided into hard fraud, that is, the actual dollars a defrauded carrier loses, and soft costs, which represent revenues the carrier cannot collect from fraudulent subscribers.

When a call is routed from a cellular or PCS carrier's network to a recipient's home or business telephone, it is carried by the local telephone company. The cellular or PCS carrier pays a local interconnect charge for this service. In addition, the home carrier pays wholesale roaming charges when one of

its subscribers uses roaming service in another carrier's service area. Wholesale long-distance charges also apply to calls carried by a long-distance carrier.

The carrier normally bills a subscriber for a monthly service charge plus retail airtime charges. If the subscriber uses roaming service or places long-distance calls, the carrier bills these charges, as well. All of these charges represent revenues the carrier cannot collect from fraudulent subscribers.

Fraud Detection

Given the high cost of fraud, carriers employ various fraud-detection measures. Usually software-based, these programs attempt to identify fraudulent subscribers and cloned telephones. Some fraud-detection software creates a profile for a legitimate subscriber. It then monitors the subscriber's activity and compares it to the profile. If actual use deviates significantly from the profile, the system generates an alarm and notifies the carrier's loss-prevention or security personnel.

Other software monitors activity and flags certain calls—such as simultaneous calls from the same subscriber, high call counts, calls to or from pay telephones, calls to or from suspicious locations, and calls at suspicious times of the day. Exceeding a predetermined threshold generates an alarm and notifies security personnel.

Fraud Prevention

Carriers also institute various fraud-prevention measures to prevent a fraudulent subscriber from completing a call. These methods usually are hardware-based. Most carriers can provide subscribers with a four-digit personal identification number (PIN), which users must enter to complete a call. Some AMPS carriers transmit the PIN and the account information over different frequencies to make it more difficult for thieves to intercept and use the PIN.

Authentication also serves as a fraud-prevention measure, and a growing number of carriers are employing the technique. However, authentication is not available for AMPS.

Radio frequency (RF) fingerprinting detects subtle characteristics of the radio signals transmitted by cellular telephones. It can recognize the differences between the signals transmitted by a legitimate phone and a clone. The network can prevent a cloned phone from completing a call. Carriers can exchange RF fingerprints to allow a carrier outside the home service area to recognize a legitimate roamer from a clone.

Investigation

Criminals, particularly organized-crime associates and drug dealers, have grown increasingly wary of law enforcement's ability to monitor their telephone activity. Many of them want cloned phones for security. Other criminals step forward to meet the demand, offering cloned phones for sale or programming a customer's phone for a fee. Law enforcement personnel should remain alert for source information indicating that someone is providing cloned phones.

Fraudulent Programmer

Clinton Watson of San Jose, California, wrote a software program that allowed fraudulent subscribers to program account information into cellular phones. After receiving an unusually large number of calls at his home from customers using cloned phones, Watson attracted the attention of a local cellular service provider, which contacted the U.S. Secret Service. In April 1994, the Secret Service and the San Jose Police Department executed a search warrant at his home. At the time, he was on probation for a 1988 conviction for cellular telephone cloning. In May 1996, he was sentenced to 5 years in prison, 3 years' probation, and $300,000 restitution for cellular telephone fraud. He also received an additional year in prison for probation violation.

Source: *"They Clone by Night,"* Tele.com, *August 1996.*

Undercover operations have met with some success. In one case, the U.S. Secret Service set up a computer bulletin board system to purchase stolen cellular telephone account information. The sting, Operation Cybersnare, netted suspects who stole millions of dollars worth of data.[5] Storefront operations that sell and program purportedly cloned phones also have proven successful, as did Operation Cellmate. This joint effort between the state attorney's office in Jacksonville, Florida, the U.S. Secret Service, and the Naval Criminal Investigative Service, snared close to 100 suspects, many of whom used the cloned phones they purchased to engage in other illegal enterprises.[6]

In each of these cases, the cellular phone company provided valuable assistance. In fact, most cellular and PCS carriers will work with law enforcement agencies to identify and prosecute fraudulent subscribers. However, telecommunications carriers are not equipped to provide the telephone number and location of a subscriber in real time. Thus, although undercover operations have successfully identified fraudulent subscribers, PCS and cellular carriers usually cannot contact law enforcement agencies quickly enough to catch a fraudulent user in the act. The most cost-effective option is to disconnect the service and absorb the loss.

This situation may change, however. Beginning in April 1998, cellular and PCS carriers will be required to provide public safety agencies with the telephone number and cell site location of a subscriber making a 911 call. By October 2001, carriers will be required to provide the location within 125 meters. These regulations are not meant to serve as fraud-prevention measures; rather, they represent a solution to the growing number of calls to public safety agencies from cellular or PCS subscribers in distress and unsure of their locations. At the same time that these regulations would help pinpoint the location of 911 callers in need of assistance, they would prove helpful for fraud prevention and other law enforcement operations.

With the ability to provide telephone number and location information, the odds of catching criminals in the act and obtaining prosecution and possibly restitution will increase. The effectiveness of this strategy will depend on the relationship between the law enforcement agency and the carrier. Investigators interested in pursuing PCS or cellular fraud cases should contact the carriers in their service areas to determine their interest in establishing liaison and providing referrals.

Two recently introduced pieces of legislation also may help to combat cellular phone fraud. The first, the Cellular Telephone Privacy Act, makes it illegal to use a scanner with the "intent to defraud," specifically to capture a cellular phone's electronic serial number and use it to obtain unauthorized services. The second bill, the Wireless Telephone Protection Act, makes it a crime to use a scanner to capture cellular phone codes. It also asks the U.S. Sentencing Commission to amend sentencing guidelines for cloning.[7] If passed, these two bills may deter individuals from committing fraud.

Conclusion

Demand for cellular telephone and personal communication

Brooklyn Bandits

In July 1996, members of an electronic fraud task force that included U.S. Secret Service agents and New York police officers arrested Abraham Romy and Irina Bashkavich of Brooklyn, New York. Over a 6-month period, the pair allegedly used equipment mounted on the windowsill of their 14th floor apartment to steal account information from more than 80,000 cellular phones in vehicles traveling on the nearby Belt Parkway. A Secret Service official declared the illegal operation the largest ever uncovered by law enforcement.

Source: *Bob Twigg and Carol J. Castaneda, "Pair Held in Largest Cell Phone Ripoff,"* USA Today, *July 3, 1996.*

services continues to grow. In response, service providers use increasingly sophisticated technology to squeeze more conversations into the available frequency bands. At the same time, they must defend themselves and their customers against the increasing number of criminals who seek to exploit weaknesses in the network to commit fraud.

When law enforcement agencies team up with telecommunications companies, they gain insight into the technology used by legitimate and illicit subscribers alike. More important, they form a united front from which to combat the various forms of telecommunications fraud. In doing so, they answer the call of the victims of today's information society. ✦

Endnotes

[1] The Yankee Consulting Group, cited in Tina Metivier, "The Weakest Links," *Wireless World*, January 1997, 40.

[2] Ibid.

[3] Counterpane Systems, cited in Paul Rubin, "Sure It's Secure—But Is It Really Safe?" *Tele.com*, May 1997.

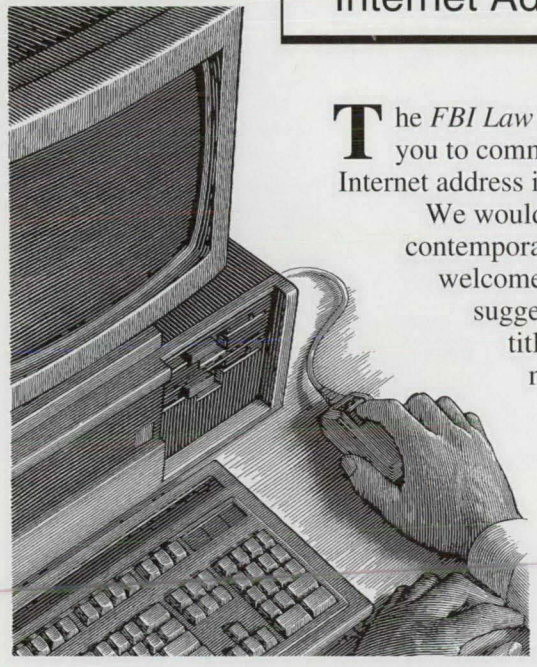
[4] CTIA Wireless Fraud Conference, Orlando, Florida, September 30-October 2, 1997.

[5] "Internet Sting Nets Alleged Hacker Ring," *The Detroit News*, September 12, 1995, [newspaper on-line]; available from http://www.detnews.com; Internet; accessed December 8, 1997; David Shepardson, "Hearing in Cell Phone Sting Sept. 28," *The Detroit News*, September 15, 1995, [newspaper on-line]; available from http://www.detnews.com; Internet; accessed December 8, 1997.

[6] P.R. Beseler, "Operation Cellmate," *FBI Law Enforcement Bulletin*, April 1997, 1-5.

[7] Steve Mansfield, "Don't Send in the Clones," *QST*, November 1997, 16.

The *Bulletin's* Internet Address



The *FBI Law Enforcement Bulletin* staff invites you to communicate with us via e-mail. Our Internet address is leb@fbi.gov.

We would like to know your thoughts on contemporary law enforcement issues. We welcome your comments, questions, and suggestions. Please include your name, title, and agency on all e-mail messages.

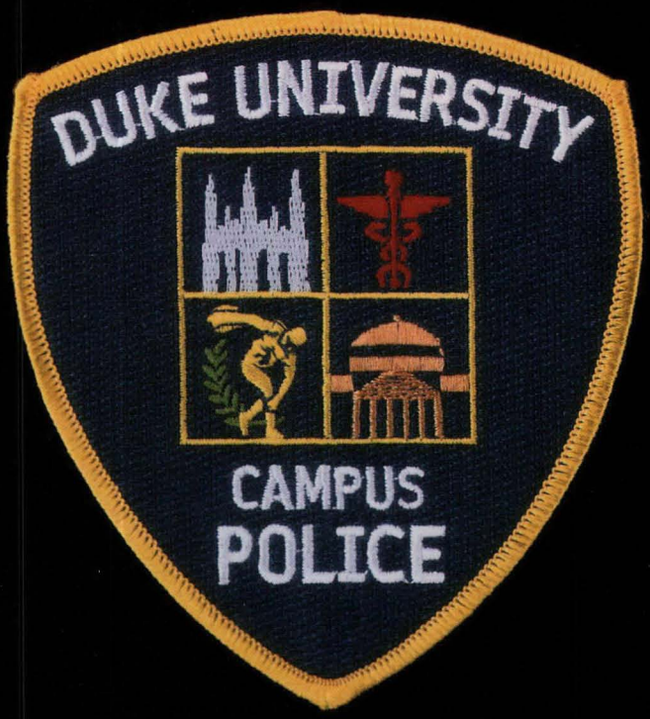
Also, the *Bulletin* is available for viewing or downloading on a number of computer services, as well as the FBI's home page. The home page address is http://www.fbi.gov.

U.S. Department of Justice
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, DC 20535-0001

Periodical
Postage and Fees Paid
Federal Bureau of Investigation
ISSN 0014-5688

Official Business
Penalty for Private Use $300

Patch Call



The patch of the Duke University, North Carolina, Police Department features the Gothic-style Duke Chapel in the upper left quadrant, representing the west campus. Proceeding clockwise is a caduceus, representing the University Medical Center, the Baldwin Auditorium, representing the University's east campus, and a discus player, representing the University's many athletic programs.

The Zuni Tribal, New Mexico, Police Department patch features the tribe's legendary Knife Wing God. The god was once symbolic only to the Zuni Tribal Warriors, but it is now identified with veterans of wars and police officers. The Knife Wing God represents wisdom, strength, and courage.