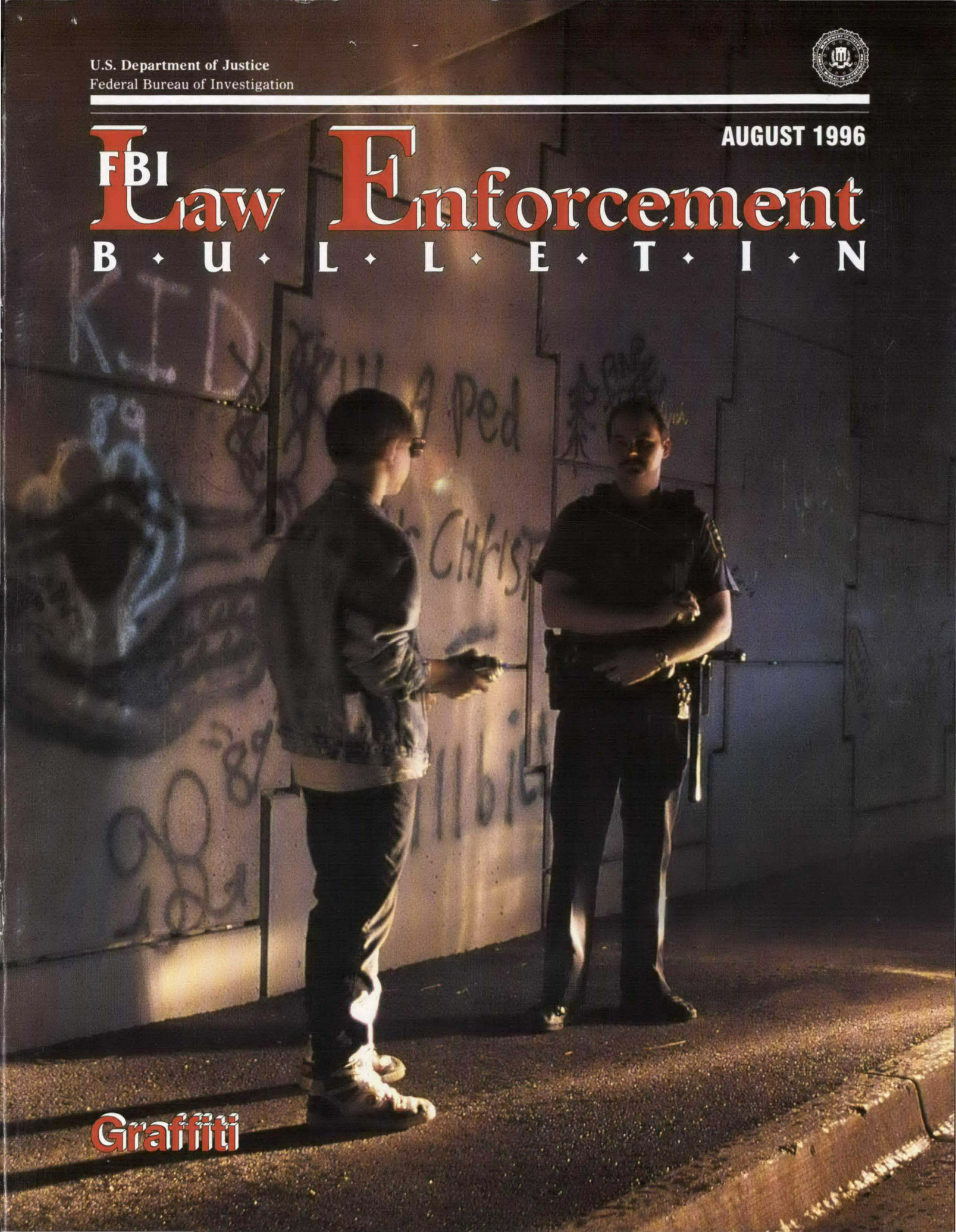
U.S. Department of Justice
Federal Bureau of Investigation

AUGUST 1996

FBI Law Enforcement BULLETIN



Graffiti

August 1996
Volume 65
Number 8

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

**Louis J. Freeh
Director**

Contributors' opinions and statements should not be considered as an endorsement for any policy, program, or service by the FBI.

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget.

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. 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
Kathryn E. Sulewski
Art Director
John E. Ott
Associate Editors
Andrew DiRosa
Julie R. Linkins
Kimberly J. Waggoner
Assistant Art Director
Brian K. Parnell
Staff Assistant
Stephanie L. Lowe

Internet Address:
leb@fbi.gov

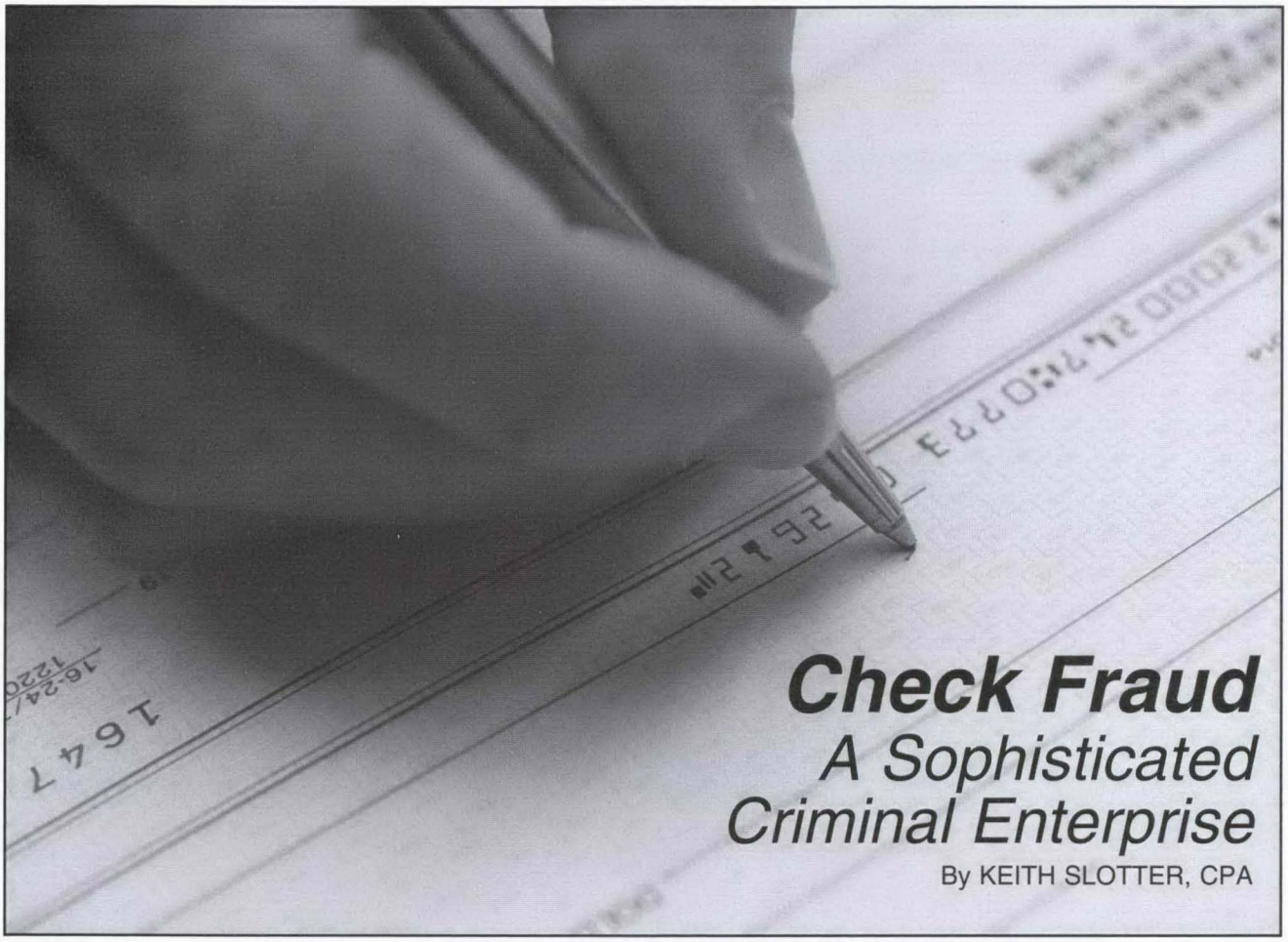
Cover photo ©
Peter Hendrie, Tribute

FBI Law Enforcement Bulletin

Features

Departments

ISSN 0014-5688 USPS 383-310



Check Fraud
A Sophisticated Criminal Enterprise

By KEITH SLOTTER, CPA

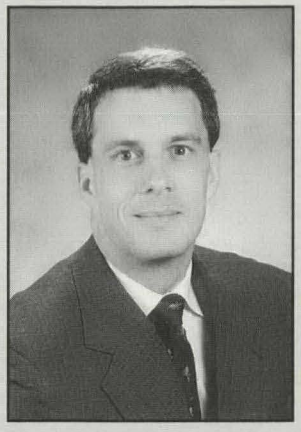
Like waves on the ocean, variations of fraudulent activity keep pounding the shores of the banking industry. Prior to the 1980s, bank fraud schemes generally involved only a few transactions perpetrated by a single individual or small group. Losses averaged less than $100,000 to the victim institution, and law enforcement investigations were fairly routine in nature.

Following deregulation of the savings and loan industry in 1982 and the initiation of more speculative, risky ventures by those in charge of these institutions, a new wave of fraud emerged. During the late 1980s and early 1990s, large-scale frauds perpetrated by institution insiders and those held in trust within the banking industry became prevalent. Law enforcement agencies used massive, task force-oriented investigations to calm the surge of these frauds. As a result, the banking industry as a whole has stabilized and continues to insulate itself from insider abuse.

Conversely, a flood of fraud perpetrated by outsiders, especially organized ethnic groups, has risen dramatically since 1987. Outsider fraud now accounts for more than 60 percent of all fraud against financial institutions.[1] The most prevalent problem in the industry, by far, centers on check fraud, but also involves other counterfeit negotiable instruments, such as traveler's checks, credit cards, certified bank checks, money orders, and currency.

EXTENT OF THE PROBLEM

In its 1994 Check Fraud Survey, the American Bankers Association (ABA) indicated that the volume of check fraud against financial institutions increased by 136 percent from 1991 to 1993. During this same period, dollar losses rose 44 percent, from $568 million to $815 million annually. The country's major financial institutions attribute fully one-half of all check fraud to professional and organized group efforts.[2]



Special Agent Slotter works in the Financial Institution Fraud Unit at FBI Headquarters in Washington, DC.

> ***"New technologies give check fraud perpetrators a wide variety of schemes and devices for committing their crimes."***

Financial institutions do not suffer alone as victims of fraud. For the past 2 years, the Forensic and Investigative Services Division of KPMG Peat Marwick, one of the big six accounting firms, has compiled an annual fraud survey of the 2,000 largest U.S. corporations. These companies reported check and credit card fraud as their most problematic losses during 1994.

The responding companies suffered an average annual check fraud loss of $360,000, an increase of 38 percent from 1993. Alarmingly, over two-thirds of corporate executives believe these losses will continue to mount over the next several years.[3] More than 1.2 million worthless checks are accepted for payment every day.[4]

The technological improvements that have fueled the growth in check fraud schemes have made it difficult for law enforcement to combat the problem. *Forbes* magazine reported on the trend in 1989, stating "...the desktop computer did not create the crime of forgery. All it did was make the tools user-friendly."[5] With the prevalence of laser printers and advanced duplication systems, the production of quality counterfeit checks has become commonplace.

In addition, Congress unwittingly aided the business of duplicating and counterfeiting checks. By passing legislation in 1988, known as Regulation CC,[6] Congress made detecting fraudulent checks even more difficult for financial institutions. This law requires banks to process checks within a 72-hour period and ostensibly provides customers with increased access to deposited funds. While the regulation may have succeeded in making depositor's funds more accessible, it also made passing fraudulent checks easier by giving banks less time to confirm the legitimacy of these transactions.

CHECK FRAUD ORGANIZATIONS

Worldwide, 80 billion checks exchange hands annually; 60 billion of those are written in the United States.[7] As anyone who has mailed a check to the mortgage company 3 days before payday can attest, Americans have become enamored with writing checks and taking advantage of the "float" period, the time during the check-clearing process. Criminal elements within numerous immigrant groups in the United States have analyzed American banking, noting the system's deficiencies and the fact that it affords opportunities for fraud. Presently, organized ethnic enterprises conduct a sizable portion of annual check fraud activity throughout the country.

The Major Groups

The principal ethnic enterprises involved in illegal check fraud schemes include Nigerian, Asian (particularly Vietnamese), Russian, Armenian, and Mexican groups. The majority of the Vietnamese, Armenian, and Mexican organizations base their operations in California, especially in the Orange County, San Francisco, and Sacramento areas. However, they have networked their operations throughout the country, with a number of connections in Chicago, Houston, and Washington, DC.

The Nigerian and Russian groups, with bases in the northern and eastern areas of the country, exhibit more nomadic tendencies. They roam throughout the United States, stop to pass stolen or counterfeit checks, and then move on to new locations. The Russian groups initially established themselves in New York but have extended their activities to Chicago and the West Coast.

Nigerian groups often solicit legitimate identification and account

information to further their check fraud schemes. Recently, law enforcement authorities have noted their interaction with Vietnamese organizations in the Chicago and Houston regions. In the northeast, Nigerian rings have opened numerous investment accounts within various brokerage houses and deposited large sums of money using stolen and counterfeit corporate checks.

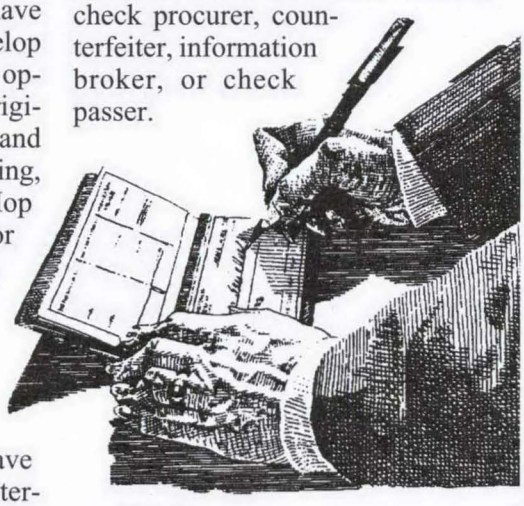
Most West Coast Asian gangs began to organize their bank fraud activities during the 1980s and have continued to expand and develop these sometimes-sophisticated operations. Many such groups originated in Taiwan, Hong Kong, and Vietnam and include the Viet Ching, Big Circle Boys, V-Boyz, Wo Hop To, Wah Ching, and Red Door gangs.[8] Within the Asian gangs, known as triads, the group leader usually holds the title of "master" and oversees all organizational operations.

Current investigations indicate that some Asian groups have been dealing with Russian counterparts, especially to negotiate (deposit or cash) counterfeit currency through the banking system. Recently, members of the Russian Mafia obtained such currency, which was printed in Montreal, Canada, sold to several West Coast Vietnamese factions, and distributed throughout California.

Notably, each of these groups conducts a myriad of white-collar, drug, and violent crimes. The groups perceive check fraud—unlike drug trafficking, extortion, or murder—as a "safe" crime; it carries minimal penalties and a low risk of apprehension.

The Players

Regardless of ethnic origin, groups involved in check fraud maintain certain universal characteristics. Unlike traditional, tight-knit, organized criminal groups, such as La Cosa Nostra, these groups, which may embody several hundred members, usually are loosely organized. Members often network among several organizations. Despite the lack of a rigid hierarchy, members typically fall into one of several roles—leader, check procurer, counterfeiter, information broker, or check passer.



Leaders

Leaders of an organization generally have an extensive criminal history and possess above-average intelligence. Often, they have a degree in business and/or law. These individuals provide the overall direction of the group, as well as expertise in understanding American business and the banking system.

Check Procurers

Check procurers obtain authentic checks, usually by stealing them while employed within a financial institution. Group members then sell or negotiate the stolen checks as is, or they duplicate the checks for future use.

Counterfeiters

Counterfeiters duplicate corporate and payroll checks, traveler's checks, credit cards, certified bank checks, money orders, currency, and other negotiable instruments, as well as personal identification. They usually are well-versed in the use of personal computers, especially in the field of desktop publishing.

Information Brokers

Information brokers gather personal and financial information on legitimate individuals. Using this credible information, associates open new bank accounts, pass counterfeit checks, and secure loans, which they fail to repay.

Check Passers

Check passers actually negotiate stolen and counterfeit checks through the banking system and collect the proceeds to distribute to the group. They often travel throughout the country, opening new accounts and transporting their illicit proceeds. Typically, they negotiate only about 10 percent of a group's illicit checks; the group sells the rest of the checks to other individuals and organizations. Check passers maintain little contact or status within the hierarchy and often are the only members whose ethnic backgrounds differ from the core group.

Ethnic organizations tend to distrust anyone not of their own heritage, making it difficult for law enforcement to infiltrate them. Even though police frequently arrest

Identifying Fraudulent Checks

To recognize check fraud, law enforcement officials must know as much about these instruments as the criminals.

Perforation

Almost all legitimate checks have at least one perforated edge; counterfeit checks are often smooth on all sides.

Federal Reserve Routing and Transit Number

The routing and transit fraction number in the top right hand corner (below the check number) should correspond to the electronically encoded number, known as the MICR, on the bottom center of the check. Fully 98 percent of all fraudulent checks have an incorrect Federal Reserve transit number.

Federal Reserve District and Office

The first three digits in the MICR line represent the state and district office to which the bank is assigned. On fraudulent checks, these numbers often do not correspond appropriately.

Serial Number Match

The encoded check serial number on the bottom left should correspond exactly with the check number in the top right corner.

Check Number

Low numbered checks also indicate potential fraud; 90 percent of all check frauds involving insufficient funds are numbered 101-200.

Source: Frank W. Abagnale, *Document Verification and Currency Transactions Manual*, Abagnale & Associates, 1994.

check passers throughout the country, these street-level criminals generally possess little information concerning upper-echelon group members.

TYPES OF CHECK FRAUD SCHEMES

The variety of check fraud schemes perpetrated throughout the country ranges from depositing single stolen checks to counterfeiting thousands of negotiable instruments and processing them through hundreds of bank accounts. Although it is impossible to summarize all of the check fraud schemes currently operating, three schemes in particular—large-scale counterfeiting, identity assumption, and payroll check fraud—typify frauds being tracked by bank security officials and law enforcement authorities throughout the nation.

Large-scale Counterfeiting

The most notorious groups engaged in large-scale counterfeiting operations are the Vietnamese triads operating out of Orange County, California. Members routinely get jobs within local financial institutions in order to collect master original bank checks, money orders, and corporate/payroll checks for counterfeiting. The triad masters, who often are counterfeit experts with a host of duplication devices, manage the groups' criminal activities.

The groups exchange their counterfeit instruments for cash in a variety of ways. Check passers directly negotiate a portion of the counterfeit documents through financial institutions. They deposit the fraudulent checks, often into new accounts, and withdraw the funds before the bank can complete the check-clearing process and discover the fraud. The transient check passers open accounts in different institutions throughout the country; however, group members within the organizational hierarchy ultimately control their activities from a home base.

In order to minimize their exposure to law enforcement, the counterfeiters sell the majority of their phony goods to third parties for negotiation or further resale. They create most counterfeit checks in $2,000 to $5,000 increments and sell them to black market customers at 5 to 25 percent

of their face value, depending on quality and appearance.

Identity Assumption

Seen in various metropolitan areas, identity assumption schemes often involve Nigerian and Vietnamese criminal organizations. Group members obtain employment or develop sources in local banks and credit agencies so they can acquire otherwise confidential information on bona fide bank customers. The groups then create counterfeit identification, including driver's licenses, social security cards, and credit cards, to assume the innocent person's identity. Under the assumed identity, the criminals open new bank accounts, which they use to deposit fraudulent checks and subsequently withdraw the funds, as well as to secure personal loans and lines of credit.

Once bank accounts have been established, the financial institutions become vulnerable to a variety of frauds. Prior to depositing fraudulent checks and withdrawing the proceeds, the "customer" is likely to obtain a credit card account with a substantial credit line. The perpetrators withdraw funds against the credit line and distribute the money within the criminal organization, along with any bogus loan money they have procured. After withdrawing monies pursuant to the deposit of fraudulent checks, the "customer" leaves town, and the bank sustains a substantial loss.

Such schemes hurt more than just the banks, however. The innocent people whose identities were assumed suffer from ruined credit histories, which may inhibit their future financial activity.

Payroll Check Fraud

A variation of the identity assumption scheme involves placing group members within payroll check-processing companies. These firms compile and distribute payroll checks on behalf of their corporate clients.

The miscreant employees print duplicate payroll checks for various client recipients. They then steal the checks from the premises, and the group duplicates them for negotiation. Concurrently, the group obtains full background identifying data on the client's regular employees, which can be used in future schemes.

> ***"...financial institutions have begun to implement a type of biometric fingerprint identifier...."***

METHODS OF ALTERATION

New technologies give check fraud perpetrators a wide variety of schemes and devices for committing their crimes. Chemical techniques and computers provide the primary means by which criminals manipulate and counterfeit checks.

Chemical Techniques

Legitimate personal checks can be changed easily by chemical means. Similarly, someone well-versed in manipulation techniques can modify corporate checks, traveler's checks, bank checks, and U.S. Government checks with minimal effort.

Chemical alteration is commonly referred to as "check washing." Check washers use a variety of acid-based chemical solutions to erase amount and payee information, while maintaining the integrity of the preprinted information. They then dry the check and inscribe a new payee and a significantly higher dollar amount before presenting it to a bank for payment.

One acid-based solution even allows criminals to revise a check and subsequently destroy the evidence. In this instance, the check washers must move quickly because the chemical solution causes the paper to disintegrate within 24 hours, leaving no supporting evidence of the transaction.

Technology

Today's computer technology makes it relatively simple to counterfeit checks. A counterfeiting operation requires only a laser scanner to capture the image of an original check, a personal computer to make changes, and a quality laser printer to produce the bogus check. The necessary equipment can be obtained for less than $5,000.

Once an original check has been scanned, its data can be manipulated and reprinted with ease. Still, the counterfeiter faces the tough challenges of matching the paper stock used by the check manufacturer; correlating complex color schemes, such as those used on U.S. Government and traveler's checks; and overcoming some of the counterfeiting safeguards currently used by legitimate check printers.

A Typical Scheme

In September, 1994, a San Bernardino County, California, undersheriff received a letter at his residence from an alleged Nigerian businessman promoting a typical fraud scheme. The letter advised that the Central Bank of Nigeria was holding $35 million in U.S. currency, which was due to him as a foreign contractor. This "businessman" was seeking assistance in transferring this money to the United States and needed an American bank account in which to deposit the proceeds. In exchange for his account number and temporary use of the account, the undersheriff was promised 30 percent of the deposited funds for his services.

Source: "Nigerian Schemes Continue," *Intelligence Operations Bulletin*, Office of the Attorney General, California Department of Justice, vol. 53, February 1995.

Yet, counterfeiters can overcome even these hurdles without much difficulty. A number of unscrupulous printers throughout the country offer preprinted checks containing whatever information the customer desires, without bank confirmation or concurrence. Further, today's computers can come very close to duplicating even the most complex color schemes and check safeguards. A counterfeiter's success hinges on knowing that most checks will not be scrutinized closely enough to detect the fraud until they have been cashed and cleared through the banking system.

FRAUD PREVENTION

In order to prevent fraud, check-printing companies offer a variety of counterfeiting safeguards.[9] All such features make attempted alteration detectable in one way or another. Yet, these enhancements are not foolproof and often prove cost-prohibitive to the purchaser. In response, financial institutions have begun to implement a type of biometric fingerprint identifier as a more cost-effective approach.

In early 1995, Bank of America (BOA) in Las Vegas, Nevada, became the first financial institution to use fingerprinting technology to deter check fraud.[10] At BOA, when customers who are not account holders present checks for payment, they must place an inkless fingerprint next to their endorsement. When bank officials identify an attempted fraud, the fingerprinting system provides law enforcement with evidence and background information never before attainable at the onset of an investigation.

This pilot project has garnered impressive results. BOA officials report that the biometric identification system nearly has eliminated check fraud schemes perpetrated by outsiders. It also has reduced the bank's overall fraud by 40 percent.[11]

BOA's success in Nevada has spurred the Arizona Bankers Association to lead a campaign with member financial institutions to implement a similar program. A core group of Arizona-based banks implemented this technology in the fall of 1995. Moreover, BOA officials plan to extend fingerprinting operations to their branches in Texas and New Mexico. A number of financial institutions have expressed a desire to expand the program to new customer accounts, another hotbed for fraudulent checking activities.

During this implementation process, the banks involved have become cognizant of the sociological and privacy concerns underlying such an identification system. Some customers fear the improper use of identifying information. Bank officials stress, however, that no central database of fingerprint information will be maintained and that these records will be furnished to law enforcement only pursuant to suspected criminal conduct.

LAW ENFORCEMENT SUCCESSES

Criminal investigators working negotiable instrument fraud cases, especially involving organized groups, have begun to achieve significant results by using a task-force approach and by promoting effective cooperation with their international law enforcement counterparts. In March 1994, officials from eight federal, state, and local law enforcement agencies in California[12] combined forces to raid a contingent within the Wo Hop To

triad, arresting nine subjects and seizing more than $500,000 worth of merchandise obtained through counterfeiting activities.[13]

The Westminster, California, Police Department's Tri-Agency Resource Gang Enforcement Team, as well as various San Francisco Bay area task forces, has conducted successful raids and arrests targeting Asian criminal organizations involved in check fraud and counterfeiting enterprises.[14] Similarly, the Los Angeles Division of the FBI successfully investigated a local gang involved in a check alteration scheme in which the culprits deposited $600,000 worth of fraudulent checks into accounts at American Savings Bank and subsequently converted the funds to gold krugerrands.

Since its inception in 1992, the Phoenix, Arizona, Financial Institution Fraud Task Force has achieved impressive results in the fight against bank fraud, particularly check fraud. As of March 31, 1996, this task force[15] had indicted 451 subjects with 342 convictions returned.[16] Various FBI field offices throughout the country are studying the success of this particular task force in the hope of establishing similar programs within their jurisdictions.

The Interagency Working Group on Nigerian Crime in Washington, DC, is cultivating cooperation among Nigerian law enforcement agencies to help combat the growing fraud problems associated with these groups. In July 1995, Nigerian authorities raided a Lagos-based organization and arrested numerous locals involved in check fraud and counterfeiting operations. The Royal Hong Kong Police have provided great assistance to U.S. law enforcement in tracking suspects and providing intelligence information on fraudulent operators believed to have migrated to America.

CONCLUSION

Checks can be either stolen, manipulated, or counterfeited. Illicitly obtained checks can be negotiated immediately, altered, or used for future counterfeiting. Generally speaking, only unsophisticated criminals acting alone will immediately negotiate stolen checks by forging the signature. Most organized groups steal checks as a prelude to more enterprising endeavors.

> ***"More than 1.2 million worthless checks are accepted for payment every day."***

Bank security officials and law enforcement agencies concur that the problems associated with check fraud and counterfeit negotiable instruments have reached epidemic proportions. As criminal organizations become more sophisticated in the devices they use, law enforcement also must become more creative and sophisticated in the techniques used in its investigations. To meet this challenge, the battle against check fraud is best fought through cooperation—among agencies, bankers, bank regulators, and the public.✦

Endnotes

[1] FBI Financial Institution Fraud Criminal Referral Statistics for Fiscal Year 1995, September 30, 1995.

[2] American Bankers Association, "1994 ABA Check Fraud Survey," November 30, 1994.

[3] KPMG Forensic and Investigative Services, "1994 Fraud Survey," March 1, 1995.

[4] Frank W. Abagnale, "Document Verification and Currency Transactions Manual," Abagnale & Associates, 1994.

[5] David Churbuck, "Desktop Forgery," *Forbes Magazine*, November 27, 1989, 246.

[6] Expedited Funds Availability Act, 12 U.S.C. § 4001, et seq., passed 8/10/87, enacted 9/1/88.

[7] Supra note 4.

[8] "Asian Gangs Involved in Credit Card Fraud," *Intelligence Operations Bulletin*, Office of the Attorney General, California Department of Justice, vol. 47, December 1994.

[9] Check-printing companies offer a variety of counterfeiting safeguards, such as embossing, artificial watermarks, laid lines, chemical voiding features, warning bands, high-resolution printing, dual image numbering, and security number fonts.

[10] Steven Marjanovic, "Arizona Group Pushes Fingerprinting as a Ploy to Deter Check Fraud," *The American Banker*, July 6, 1995, 10.

[11] Robert Bird, Vice President, Bank of America, San Francisco, California, remarks at meeting of the Bank Fraud Working Group subgroup on Check and Credit Card Fraud, Washington, DC, July 19, 1995.

[12] Participating agencies include the Bureau of Investigation of the California Department of Justice; the Antioch, Oakland, and San Francisco police departments; the U.S. Secret Service; the Immigration and Naturalization Service; and the U.S. Customs Service.

[13] Supra note 8.

[14] "V-Boyz," *Intelligence Operations Bulletin*, Office of the Attorney General, California Department of Justice, vol. 46, November 1994.

[15] The task force comprises law enforcement officials from the FBI; the Phoenix, Tempe, Glendale, Mesa, and Scottsdale police departments; the Maricopa County Attorney's Office; the Arizona Attorney General's Office; and the U.S. Attorney's Office.

[16] Kathryn Brewer, Financial Analyst, Financial Institution Fraud Task Force, Phoenix, AZ., telephone interview with author, April 1996.

Point of View

Overcoming Obstacles
Preparing For Computer-related Crime

By Richard S. Groover

The computer, a jewel of technology, could become the worst enemy of law enforcement agencies across the country. On a daily basis, local law enforcement must deal with a wide assortment of crime situations that, more and more often, involve computers. Local agencies must stay abreast of technology, but in the area of white-collar crime investigations, the computer makes this task difficult.

As explored in the July 1995 *FBI Law Enforcement Bulletin* article titled "Computer Crime Categories, How Techno-Criminals Operate," computers can intersect with crime in a number of ways. But whether computers are the targets of crime, the instruments of crime incidental to criminal acts, or associated with new versions of traditional crime,[1] the day has come when law enforcement must deal with their presence.

Obstacles

When asked about computer-related crime, most local agency heads say publicly that they do not have such problems in their jurisdictions. But the director of the National White Collar Crime Center asserts that agencies across the country might have very serious problems without realizing it. In fact, it might take years for law enforcement to become proficient in dealing with computer-related crime.[2]

Computer technology has become a significant tool for criminals, just as it has for legitimate private businesses. The head of the Department of Justice's Computer Crime Section predicted a marked increase in the number of computer-literate criminals. In the past, fewer than 10 percent of criminals possessed computer skills; by the year 2000, nearly 90 percent will be computer literate.[3] Such a future presents police and sheriff's departments with serious problems if their investigative staffs are not equipped to handle the technologies used by criminals.

Document trails have been replaced by data trails.[4] A lack of training and proficiency in the use of computer hardware and software handicaps investigators. Even the most basic computer use in a crime or in support of criminal activity can become an obstacle to the investigative process if detectives cannot navigate the computer maze.

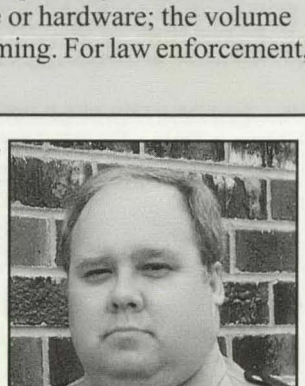
Significant evidence might even remain undiscovered without full investigation of computers found at the scene of a crime or at the disposal of the criminal. If an investigator does not enter the system carefully or properly, data (evidence) can be lost.

Law enforcement administrators historically have encountered significant problems finding individuals who possess technical expertise as well as investigative training. There are experienced investigators and there are knowledgeable computer specialists, but rarely does one person command both sets of skills. In fact, one expert estimates that only 25 to 40 people nationwide fit the bill and could manage an investigative unit.[5]

The absence of properly trained investigators represents only one major element of this problem. Computer companies introduce thousands of new products annually, making it a herculean task to stay knowledgeable about computers and the vast world of software. No one can know how to operate every system.

Moreover, no organization, not even a federal agency, could serve as the repository for all the instructions on all software or hardware; the volume simply would be overwhelming. For law enforcement,

Mr. Groover is a volunteer deputy sheriff with the Hanover County, Virginia, Sheriff's Department and a freelance writer.



even if an agency attempted to be prepared by learning how to navigate the more popular programs, how could it predict which products criminals would use? There are just too many popular programs from which to choose.

Where would local agencies go for help in dealing with unfamiliar computer products? Often, they look to the state police for assistance. Several states have established computer crime support units, but these have not developed sufficiently to make a significant dent in the problem. High costs make it virtually impossible to establish a full support capability.[6]

Nor will rescue come from the federal government. It will be some time before most federal agencies, straining under pressure to train enough employees to handle their own cases, can provide significant assistance to state and local agencies.[7]

Another consideration is the age-old problem of funding. Explaining to city leaders during the budget process that violent crime has increased and must be addressed is easy because violent crime strikes fear in the hearts of citizens.

By contrast, obtaining additional funds for the enforcement of computer-related crimes generally proves more difficult. The public often does not view white-collar or economic crimes as serious, even though such crimes do considerable financial damage to society. Budget providers respond to priorities set by the public. Unfortunately, public apathy toward nonviolent crime prevails, at least until citizens become victims.

Suggested Solutions

For now, local law enforcement agencies can take several steps to deal with this dilemma on their own. First, they must integrate computers into basic training for all officers. The Tempe, Arizona, Police Department has taken a bold step in this direction, issuing a laptop computer, along with the badge and gun, to all graduates of its police academy.[8]

Laptop computers cost approximately $2,500. Considering that police and sheriff's departments spend an average of $25,000 to train and fully equip newly hired officers (excluding salary), issuing a laptop computer to each officer increases training costs by about 10 percent. Faced with escalating costs of computer-related crime, police and city administrators should view equipping officers with laptop computers as a wise investment.

At a minimum, computer training should be paid for and directed by departments. The days have passed when agencies could leave it up to individual officers to learn at home on their personal computers. Such a lackadaisical approach will not head off this mounting crisis.

> **"In the past, fewer than 10 percent of criminals possessed computer skills; by the year 2000, nearly 90 percent will be computer literate."**

Next, agencies must become more computer active across the board. The Williamsburg, Virginia, Police Department, for example, has embraced computers on a daily basis. There, officers enter all incident reports, investigative files, etc., into the computer system, eliminating the need for multiple paper copies. Paper is generated only for summonses and warrants, which require that a copy go to the citizen.[9]

Departments immediately must begin to articulate how behind they really are and express the need for funds. This is difficult. Administrators must admit that they have a problem and need assistance from the local government, something hard for most chiefs and sheriffs to do. But do it they must.

If departments overcome the funding and personnel obstacles, the usual approach to law enforcement careers might need to be reexamined. Normally, police and sheriff's departments rotate staff among the different disciplines in their departments. Such a practice might create well-rounded officers, but it damages the departments' computer expertise.

Computer technological knowledge and training must be comprehensive and continual. Every year, a person's knowledge potentially becomes dated because

the technology changes so quickly. New knowledge builds on old knowledge, and personnel rotation forfeits the continuum of skill needed to deal successfully with computer-related crime.

Local law enforcement agencies also must work together to address the problems associated with computer-related crime. As mentioned, the computer field is too big for one department to handle. Divide-and-conquer tactics offer the only solution.

One jurisdiction can become the expert on one type of hardware and certain software, while a neighboring jurisdiction can specialize in another type. Then, when a computer and its software become evidence, a team can work together to uncover the information critical to the investigation. It took teamwork to make a dent in the drug war; the computer crime war will be no different.

Conclusion

Some local agencies already recognize and understand the emerging enforcement problems posed by computers. Others do not. Some are worried enough to be working on the problem but do not want to disclose just how far behind the criminals they really are. If police and sheriffs will bring this issue to the floor of discussion more often, take definitive steps within their own departments, and work together, the criminals will not be the only group that is 90-percent computer literate for long. ✦

Endnotes

[1] David L. Carter, "Computer Crime Categories, How Techno-Criminals Operate," *FBI Law Enforcement Bulletin*, July 1995, 21-26.

[2] Richard Johnston, Director, National White Collar Crime Center, Richmond, VA, interview by author, September 1995.

[3] Scot Charney, Department of Justice Computer Crime Section, Washington, DC, telephone interview by author, October 1995.

[4] Supra note 1.

[5] Supra note 2.

[6] Supra note 2.

[7] Supra note 2.

[8] Sergeant Toby Dias, Public Affairs Officer, Tempe, Arizona, Police Department, telephone interview by author, December 1995.

[9] Larry Vardell, Chief, Williamsburg, Virginia, Police Department, telephone interview by author, September 1995.

Law Enforcement's New Internet Address

The *FBI Law Enforcement Bulletin's* Internet address has changed. We invite you to communicate with us via e-mail. Our new 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.

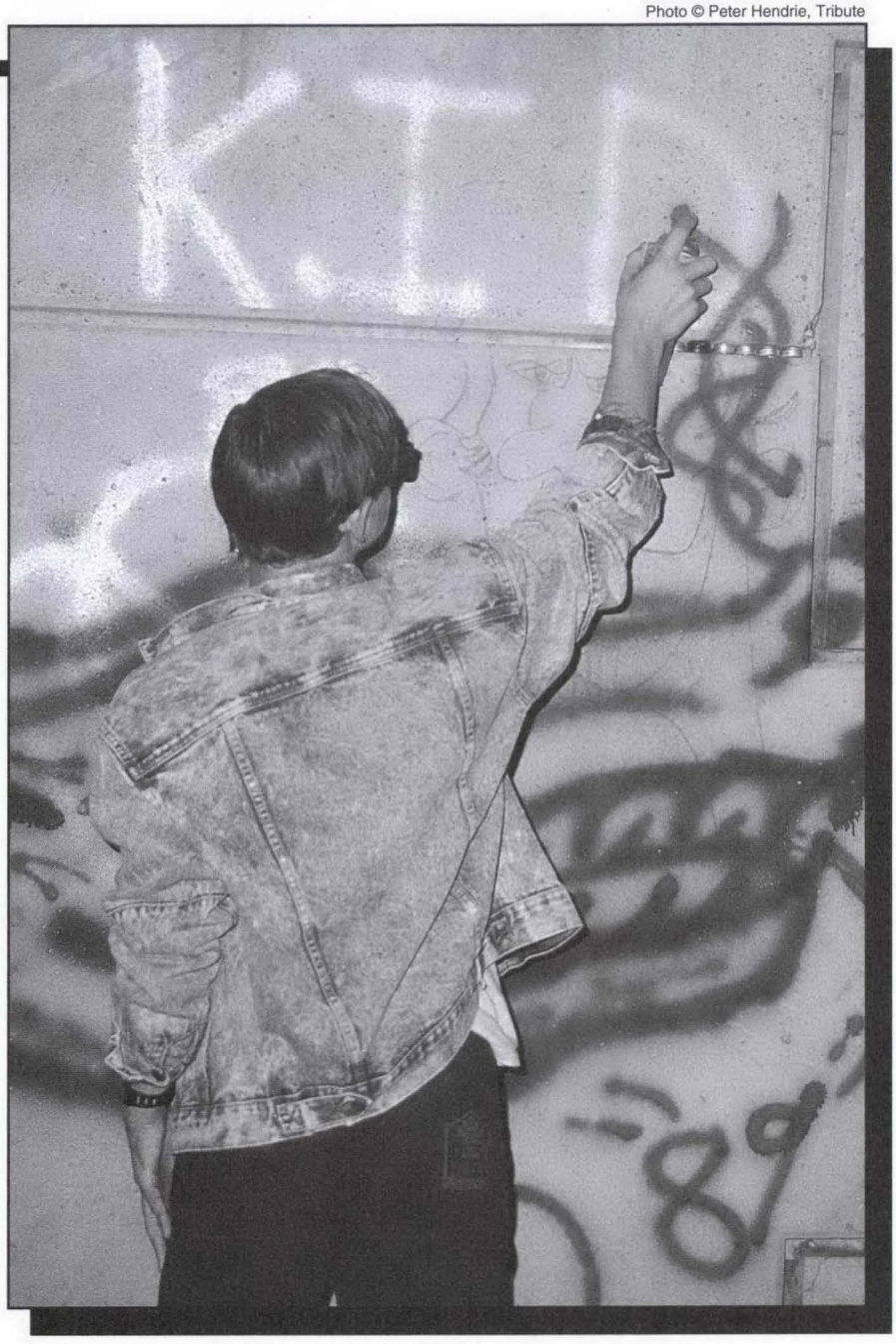
Also, *Law Enforcement* is still available for viewing or downloading on a number of computer services, including the FBI's home page. The home page's address is:

http://www.fbi.gov

Graffiti
Taking a Closer Look

By CHRISTOPHER M. GRANT

Photo © Peter Hendrie, Tribute



Not long ago, the word *graffiti* conjured images of innocent messages, such as "Tom loves Jane," or "Class of '73." Such simple and innocuous scribblings, although occasionally still seen, have become essentially messages of the past. Most of the graffiti that mars contemporary American landscape—both urban and rural—contain messages of hatred, racism, and gang warfare.

Public attitudes toward graffiti tend to fluctuate between indifference and intolerance. On a national level, the criminal justice system has yet to adopt a uniform response to graffiti and the individuals who create this so-called street art. While some jurisdictions combat the problem aggressively, others do very little or nothing at all to punish offenders or to deter the spread of graffiti.

To a large degree, society's inability to decide on a focused response to graffiti stems from the nature of the offense. It could be argued that graffiti falls into the grey area between crime and public nuisance.

If graffiti is considered in a vacuum, such an argument could appear to have some credence. However, it is unrealistic, and ultimately foolhardy, to view such a public offense in a vacuum. There is a growing consensus in communities around the country that the problem of graffiti, if left unaddressed, creates an environment where other more serious crimes flourish and can quickly degrade once low-crime areas.

At a time when law enforcement agencies nationwide are adopting more community-based policing philosophies, administrators are exploring ways to address the basic factors that lead to crime and neighborhood decline. The time has come to take a closer look at graffiti.

WALL WRITING

Graffiti is a general term for wall writing, perhaps humankind's

earliest art form. The crude wall writings of prehistoric times and the highly stylized street art of today's inner-city youths share one common feature: Each stems from a basic human need to communicate with others.[1]

For youths who may not be able to express themselves through other media, such as prose or music, graffiti represents an easily accessible and effective way to communicate with a large audience. Anyone can obtain a can of spray paint and "make their mark" on a highway overpass or the side of a building.

Modern graffiti generally falls into one of three categories—junk graffiti, gang graffiti, and tagging. Junk graffiti messages are not gang-related but often involve obscene, racist, or threatening themes. The line separating gang graffiti and tagging has become blurred in recent years. Tagging, once seen as a nonviolent alternative to more threatening gang activities, is now considered an entry level offense that can lead to more serious crimes, including burglary and assault.[2] In addition, tagging often results in direct gang affiliation. While all types of graffiti threaten the quality of life in affected areas, tagging and graffiti tied to gang activities represent the most widespread and formidable challenges to communities around the country.

GRAFFITI AND THE GANG SUBCULTURE

Tagging

Tagging as a form of graffiti first appeared in the early 1980s and has grown immensely popular in many parts of the country, in both rural and urban areas. A tagger is someone who adopts a nickname, or tag, and then writes it on as many surfaces as possible, usually in highly visible locations. Although spray paint is the most common medium, taggers—sometimes referred to as "piecers," "writers," and "hip-hop artists"—also may use magic markers or etching tools to create their images.

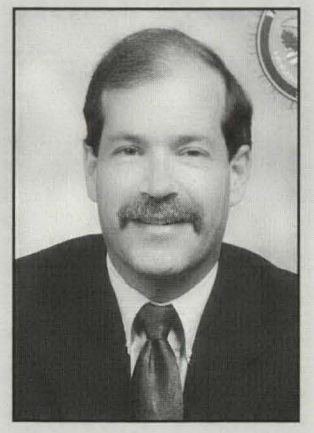
The motivation behind tagging involves fame, artistic expression, power, and rebellion—all integral parts of what has been referred to as the hip-hop culture. Tagging may fill an even deeper void for youths without a strong sense of personal identity. Interviews with taggers reveal a deep desire simply to be known, to create an identity for themselves, and to communicate it to others.[3] The thrill of risktaking also appears to be an underlying motivation for many taggers.

While the images taggers create may not necessarily be gang-related, research shows that most taggers hope to join gangs and use tagging as a way to gain the attention of gang members.[4] The more often their monikers appear in different locations, the more publicity they receive. Consequently, a small number of taggers can cause a disproportionate amount of property damage in a community.

Tagging messages usually resemble handwriting, but may be difficult, if not impossible, to read. Taggers also have been known to invent their own letters or symbols, often adding to the confusion over the message and the author.

Taggers, either vying for the favor of gang members or operating as rogue vandals, use graffiti to:

- Mark or claim territory
- Gain recognition with little fear of arrest
- Threaten or show disrespect to rival gangs or taggers
- Express themselves artistically



Lieutenant Grant serves with the Rapid City, South Dakota, Police Department.

"The criminal justice system has yet to adopt a uniform response to graffiti and the individuals who create this so-called street art."

- Identify a specific gang
- Immortalize dead gang members.

Often, gang graffiti and gang-related tagging serve an additional purpose—communication. In fact, graffiti as a means to communicate territoriality has become a central element of the gang subculture.

Communication and Territoriality

In an article about the increase in area gang violence, a local California newspaper accurately described graffiti as a "crude but effective way for gang members to communicate among themselves, with the community, and with rival gangs."[5] Communication is an important attribute of graffiti that law enforcement and community leaders should understand as they attempt to address the problem. While neighborhood residents and police might see graffiti simply as a blight, gang members and many taggers view it not so much as property damage but as a means to send messages understood within the gang community.[6]

The expressive value of graffiti also forms an important component of gang territoriality. Gangs, and potential gang members, use graffiti to identify and mark their territory. Although the traditional perception of gang territoriality has been altered by increased mobility via the automobile, research of a noted gang expert indicates that gangs continue to "mark, define, claim, protect, and fight over their turf."[7] In fact, territoriality among rival gangs continues to be a major source of gang violence.[8] Graffiti as a primary form of communication and turf identification plays a direct part in feeding this violence.

"...removing graffiti as soon as it appears is the best way to deter further vandalism."

TRUE IMPACT OF GRAFFITI

The threat posed by graffiti to neighborhoods and society in general goes much deeper than territorial gang violence. Community leaders need only consider the reverberating effects of graffiti to understand how a seemingly low-grade misdemeanor can threaten or destroy the quality of life in an entire community.

The monetary damages attributed to graffiti speak for themselves. In 1992 alone, the City of Los Angeles spent more than $15 million on graffiti eradication. This figure does not include the volunteer time devoted to graffiti cleanup or the estimated millions of dollars spent by private businesses taking care of the problem themselves. In addition, the Southern California Rapid Transit District spent $12 million on graffiti removal during the same year.[9]

Denver, Colorado, spends approximately $1 million each year on graffiti cleanup; Sacramento, California, $48,000.[10] According to the National Graffiti Information Network, graffiti eradication costs the public $4 billion a year.[11]

But the financial burden of cleanup is only one aspect of the toll graffiti takes on communities. Graffiti has a more subtle, but no less profound, impact on the aesthetic quality of a community and the psychological well-being of citizens. A January 8, 1992, article appearing in a Los Angeles newspaper examined the impact of graffiti in the city:

> The toll on the population is high—in the millions of dollars to eradicate it, in decreased property values, in the crime experts say it spawns, and in the more intangible psychic costs of living in a city that looks as though it is under siege.[12]

In this same article, James Q. Wilson, UCLA criminologist and framer of the "broken windows" theory, states that signs of disorder in society—such as graffiti, abandoned cars, broken windows, and uncollected trash—frighten law-abiding citizens into avoiding public places. Those places are then left to criminals who further deface them, creating a downward spiral in which the *fear* of crime leads to an *increase* in criminal activity.[13]

The presence of graffiti discourages citizens from shopping or living in affected areas. As established businesses relocate or close, new businesses might be reluctant to move into areas where customers would feel unsafe. As property values decline and law-abiding citizens with resources move, once-thriving neighborhoods can quickly degrade into dangerous places. Thus, the seemingly trivial offense of graffiti ultimately can have devastating consequences for a community.[14]

RESPONSE

Most experts agree that allowing graffiti to remain visible in a community sends a message that this type of behavior is acceptable to residents. Further, allowing graffiti in an area encourages other offenders to degrade the community with more graffiti or other acts of vandalism. As stated in a newspaper article, "...removing graffiti as soon as it appears is the best way to deter further vandalism."[15]

Recognizing the serious threat posed by graffiti, a number of communities across the country have developed programs to respond to the problem. The City of Anaheim, California, is considered a leader in developing innovative programs dealing with taggers and the damage they cause.

The city developed "Adopt-a-Block" and "Wipeout Graffiti" programs and also established a 24-hour graffiti hotline that encourages residents to report graffiti damage, as well as information about suspects. Information leading to an arrest and conviction can net the caller up to $500.

> ***"...the seemingly trivial offense of graffiti ultimately can have devastating consequences for a community."***

The hotline has proven to be quite successful. To date, callers have received more than $16,500 for information provided about offenders. The courts sentence convicted taggers to perform community service that includes graffiti removal.[16] Anaheim also adopted an antigraffiti ordinance that assigns responsibility for the cost of graffiti removal to taggers, prohibits possession of implements used to create graffiti, and requires merchants to keep aerosol spray cans or other implements used to create graffiti out of direct reach of the general public.[17]

In Pittsburgh, Pennsylvania, "Operation Wipe Out" is designed specifically to eradicate graffiti throughout the city. As part of the program, Pittsburgh established an antigraffiti trust fund to pay tipsters for information leading to the arrest and conviction of graffiti vandals.

In Fresno, California, the "Graffiti Action Program" combines city and county resources to provide a graffiti hotline and a mobile graffiti removal unit. In addition, two police investigators focus exclusively on gathering evidence against taggers.

The City of Aurora, Illinois, enacted an ordinance that prohibits minors from possessing cans of spray paint unless they are being supervised by a parent or employer or use the paint as part of a supervised activity at a school or church. City council members in St. Paul, Minnesota, are considering an ordinance that would make it a misdemeanor for a person to possess spray paint or wide tipped permanent-ink markers if their intended use is to deface property.

To enhance graffiti-related investigations, Orange County, California, uses a forensic scientist specializing in handwriting analysis to help identify chronic offenders. Several other localities in California have passed ordinances calling for convicted taggers to perform up to 80 hours of graffiti removal as part of their sentences.

THE FUTURE

Although these approaches represent a step in the right direction, they are reactive measures and do little to address the causes of the graffiti problem. The causes lie deep within the roots of social structure; it will require much more than rollers and paint to correct the problem.

One of the first steps is to educate the public about graffiti—its meaning and its potential impact on a community. Citizens must understand that this type of behavior cannot be tolerated because its insidious nature threatens communities from within.

To deter new graffiti, young people should be taught that their actions can have far-reaching consequences. Law enforcement agencies may consider augmenting drug- and gang-prevention efforts with lessons on graffiti. Students should be advised that damaging property with graffiti is a serious crime and offenders will be punished. As part of the lesson, instructors also may suggest and encourage alternative methods of self-expression.

CONCLUSION

Like prostitution and illegal gambling, people often view graffiti as a victimless crime. But as communities around the country have learned, there is no such thing as a victimless crime. In fact, crimes that do not produce a single, identifiable victim generally have more impact on the entire community.

As a highly visible offense, graffiti represents a particularly menacing threat to the quality of life in a community. The residual effects of reduced property values, lost business, increased gang territoriality, and heightened fear of crime escalate the severity of graffiti-related offenses beyond their impact as visual pollution. Communities that do not develop measures to deter and prevent graffiti now may find themselves confronting more intractable problems in the future. ✦

Rapid City's Graffiti Eradication Project

In the spring of 1995, the Rapid City, South Dakota, Police Department initiated the Graffiti Eradication Project. As part of the program, officers from the department's gang task force respond immediately to sites where gang-related, obscene, or racist graffiti appears. The officers photograph the graffiti and document the incident and location. They then cover the message with spray paint and place the site on an eradication list. Approximately every month, the Graffiti Eradication Team "recovers" all of the sites on the list. The team, headed by personnel from the police department, consists primarily of volunteers from community organizations, service clubs, and church groups.

Results have been impressive. In three formal eradication projects during the spring and summer of 1995, the Graffiti Eradication Team recovered over 100 different sites with paint provided by the Rapid City Parks Department.

Due to its success, the Graffiti Eradication Project has received a very positive response from the community and positive coverage from the local media. Individual citizens and businesses have offered to provide paint and other supplies to further the effort.

Endnotes

[1] Waln K. Brown, "Gangways: An Expressive Culture Approach to Understanding Gang Delinquency," unpublished thesis, (1976).

[2] David Ogul, "Drop Paint Cans, Grab Weapons," *Riverside, California, Press Enterprise*, January 22, 1995.

[3] Dan Korem, *Suburban Gangs* (Richardson, TX: International Focus Press, 1994).

[4] Daniel Scatz, "Graffiti Paint Outs," *FBI Law Enforcement Bulletin*, June 1992, 1-4.

[5] Supra note 2.

[6] Supra note 1.

[7] Arnold P. Goldstein, *Delinquent Gangs: A Psychological Perspective* (Champaign, IL: Research Press, 1991).

[8] Ibid.

[9] Dale Vargas, "New Wave of Graffiti Vandals Making Mark in Capital," *Sacramento, California, Bee*, June 15, 1992.

[10] Ibid.

[11] Supra note 9.

[12] Sheryl Stolberg, "Engulfed in a Sea of Spray Paint," *Los Angeles, California, Times*, January 8, 1992.

[13] Ibid.

[14] Stephanie Slahor, "Fighting Graffiti: Efforts to Stop Visual Terror," *Law and Order*, May 1994, 95-96.

[15] Supra note 12.

[16] Joseph T. Malloy and Ted LaBahn, "Operation Getup Targets Taggers to Curb Gang-Related Graffiti," *The Police Chief*, October 1993, 120-123.

[17] Ibid.

Police Practice

An Alternative To Police Pursuits

By Clyde Eisenberg, M.A.
and Cynthia Fitzpatrick


Photo by Richard Wigh

Hollywood has long glorified the high-speed chase in television and film accounts of police work. Yet, rarely do the action-packed vehicle pursuits portrayed on screen show the tragedy that often accompanies them in real life. Forty percent of all law enforcement pursuits end in a collision, and approximately 290 pursuit-related deaths occur each year.[1]

Within the last decade, vehicle pursuits have become a leading concern to law enforcement administrators throughout the country. Liability issues, coupled with negative media attention, have spurred this concern. In addition, organizations such as Solutions to Tragedies of Police Pursuits (STOPP) now lobby for federal laws to regulate law enforcement pursuits and urge law enforcement agencies to adopt rigid pursuit policies in the name of public safety.[2]

Even without such pressure, many agencies have adopted stringent policies, often only permitting officers to pursue individuals suspected of committing forcible felonies. But this leaves law enforcement administrators to face the dilemma of either allowing non-violent felons to escape or risking property damage, personal injury, or death from pursuits. Both options leave the department open to public criticism and potential lawsuits.

Law enforcement agencies clearly need an alternative to the traditional pursuit. Yet, no single method will avoid all pursuits. Some pursuits occur when the suspect flees the scene of a crime or an already-speeding subject refuses to stop for the authorities. Other pursuits, however, result when an officer identifies a wanted felon and attempts to make an apprehension. When the officer turns on the lights and sirens to indicate that the suspect should stop, the suspect flees and the officer gives chase. The Hillsborough County Sheriff's Office (HCSO) in Tampa, Florida, developed the Vehicle Intercept Program to replace the latter type of pursuit.

What is a Vehicle Intercept?

Vehicle interception rests on the premise that most suspects in vehicles will not flee as long as officers keep their lights and sirens off, thus giving deputies the opportunity to develop a plan of containment. A vehicle intercept uses law enforcement automobiles to block in a suspect's vehicle that is slowing, stopped, or just beginning to move at an intersection, driveway, or parking lot.

Officers position their automobiles according to pre-set guidelines and procedures. A vehicle intercept is not a moving road block, and suspect cars traveling more than 10 miles per hour are not considered viable intercept candidates.

Creation of the Vehicle Intercept Program

In response to a proposal submitted by the authors, the sheriff convened a 10-member committee to examine the vehicle intercept concept and, if it was found plausible, to develop a training module for the department. Sworn personnel from the canine, aviation, training, detective, and patrol bureaus served on the committee. They met over a 1-week period and discussed procedures and guidelines for vehicle intercepts.

The committee also conducted some practical experiments to determine the optimum vehicle positioning for intercepts, taking into account concerns for officer safety, such as cross-fire and possible air bag deployment. The sheriff approved the committee's recommendations, which became part of the HCSO's written standard operating procedure and training curriculum.

Intercept Procedure

Only two categories of drivers qualify for interception—felony suspects and impaired drivers who pose a threat to public safety. Once deputies determine that a vehicle contains a suspected felon or an impaired driver, they do not take any overt action that might alert the occupants of the target vehicle of impending law enforcement action. Deputies refrain from activating emergency equipment and appear to conduct routine patrol while they notify dispatch, giving a description of the target vehicle, current location, direction of travel, and suspected charges.

Next, deputies communicate via radio with other units that can respond to assist. Setting up the intercept requires tactical thinking; officers must consider what intersections and other road conditions lie in the path of the target vehicle that would be conducive to an intercept. Ideally, aviation and canine units would participate, but deputies may execute a vehicle intercept without their assistance. When other units have reached the area and the intercept site has been chosen, the deputies—as many as four units—determine the positions they will take.

Without activating any emergency equipment, the primary blocking unit pulls in front of the target vehicle at the designated location as it slows, is stopped, or is starting to pull away. The primary unit takes a position perpendicular to the target vehicle, with the passenger side facing the suspect's vehicle and the rear axle in line with the front center of the target vehicle.

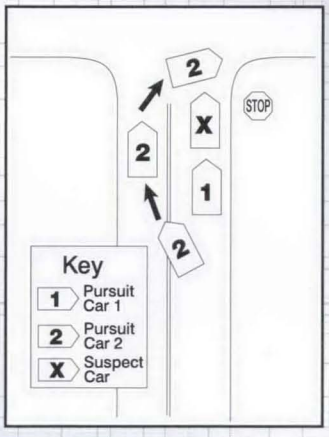
A second police unit simultaneously barricades the rear of the target vehicle. Emergency lights can be activated now. If more than two law enforcement units participate, two can block the rear or one can be deployed facing the target vehicle's driver side door from a distance of 20 to 60 feet.

The deputy operating the primary blocking vehicle stays in the car until other deputies have secured the scene. This precaution prevents potential injury to the

Two-Car Vehicle Intercept

(Same Direction)

As the target vehicle stops at an intersection, police car 1 blocks the rear of the vehicle. Police car 2 moves around to block the front of the target vehicle. Emergency equipment is activated only after the target vehicle has been contained.



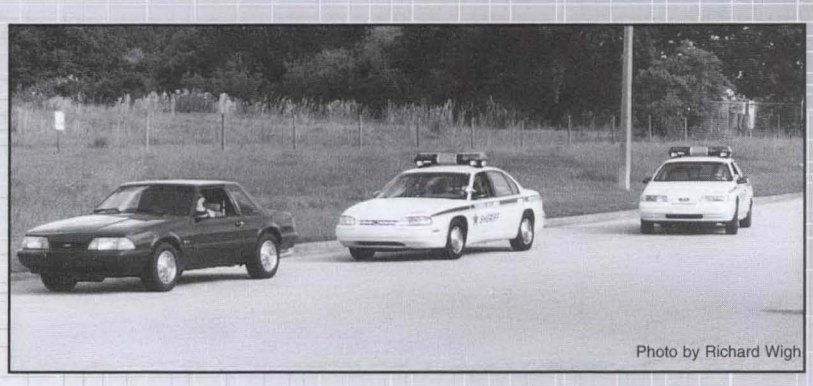


Photo by Richard Wigh

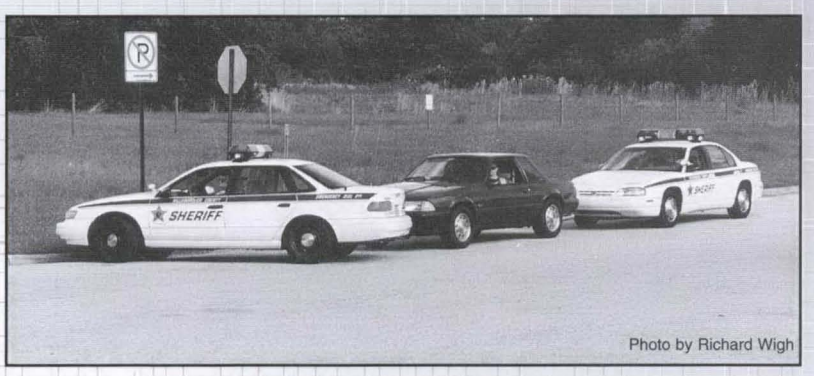


Photo by Richard Wigh

deputy if the target vehicle attempts to break through the block. It also limits the chance of a cross-fire situation developing.

The suspect(s) then are removed from the target vehicle using the high-risk felony stop method or whatever is appropriate for the situation. If the target vehicle breaks through an intercept, deputies respond according to the HCSO's standard vehicle pursuit policy.

Guidelines for Intercepts

The decision to use or participate in a vehicle intercept rests solely with each deputy and does not require supervisory authorization. When deputies decide to intercept a vehicle, they cannot use citizens' vehicles to form any part of the blockade, such as when a suspect stops in a line of traffic. Two-officer patrol vehicles cannot be used as the front blocker due to the potential danger to the officer on the passenger side. Finally, marked and unmarked cars may participate in vehicle intercepts.

Training

Vehicle intercept training consists of a 4-hour module divided into two segments—classroom instruction and practical exercises. The 2 hours of classroom instruction open with a presentation of videotapes and newspaper articles illustrating the critical attention given to police pursuits by the media. Civil liability also is discussed to emphasize the importance of alternatives to high-speed pursuits.

The instructors then present the guidelines and procedures for vehicle intercepts, using diagrams to show vehicle positioning. Audiotapes of radio transmissions during actual intercepts are played and critiqued to give the students a clear sense of how to organize an intercept. Throughout the classroom session, deputies are encouraged to ask questions and voice concerns and criticisms of the program. The aim is to ensure that the students are comfortable with the procedure and to correct any perceived flaws in it.

The second segment consists of practical exercises on the training center's driving pad. Every deputy must complete a minimum of two vehicle intercepts HCSO driving instructors scrutinize and evaluate deputies' driving technique, vehicle positioning, and radio transmissions.

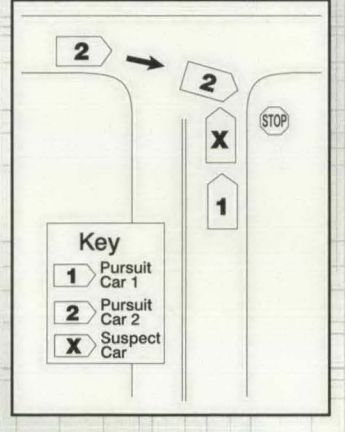
Initial vehicle intercept training for the agency occurred over an 8-month period. From February to October 1995, approximately 700 sworn personnel, including deputies and detectives, completed both segments of the course.

Field Results

As of May 31, 1996, approximately 60 vehicle intercepts

Two-Car Vehicle Intercept
(Perpendicular Approach)

As the target vehicle stops at an intersection, police car 1 blocks the rear while car 2 pulls in front of the target vehicle. Emergency equipment is activated only after the target vehicle has been contained.



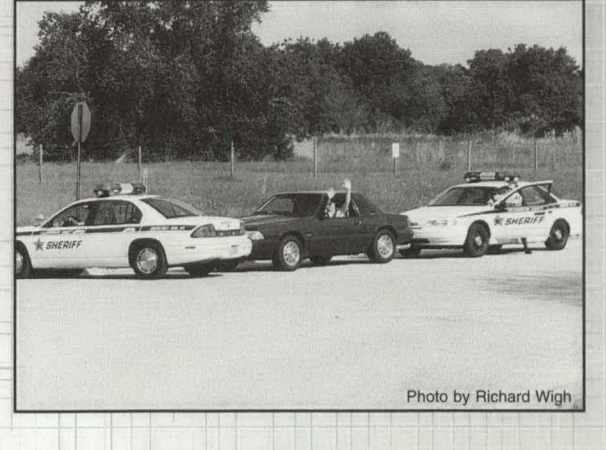
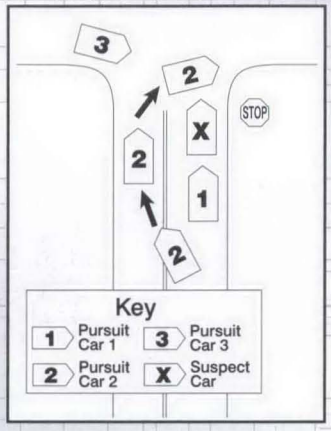


Photo by Richard Wigh

have been performed. Of those, only two vehicles broke through intercepts, one of which resulted in minor injuries to a deputy. It is difficult to calculate precisely how many pursuits these intercepts have prevented; however, HCSO deputies agree that most of the target vehicles would not have yielded to standard law enforcement approaches. Post-pursuit data indicate a 50-percent reduction in pursuits since HCSO deputies were trained in vehicle interception.

Three-Car Vehicle Intercept

As the target vehicle stops at an intersection, police car 1 blocks the rear while car 2 moves to block the front of the target vehicle. Car 3 is angled facing the driver's side of the target vehicle from a distance of 30 to 60 feet. Emergency equipment is activated only after the target vehicle has been contained.



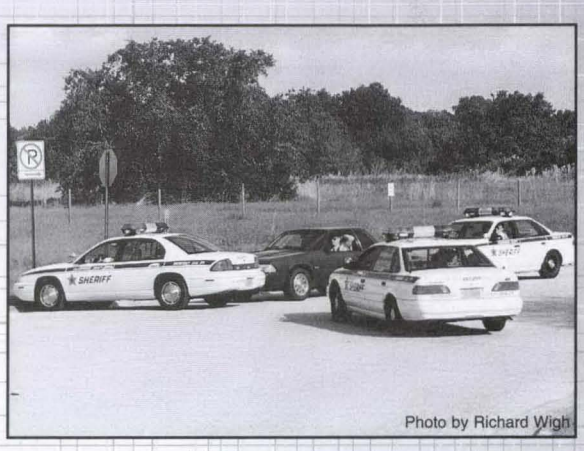


Photo by Richard Wigh

Vehicle Intercept Program Benefits

The Vehicle Intercept Program does not eliminate the need for all police pursuits, but it does provide a viable alternative to many of them. Apprehending suspected felons without protracted, dangerous chases protects the lives and property of the public, the police, and the suspects.

This pursuit alternative also assuages concerns of those who perceive law enforcement as soft on crime when agencies restrict pursuits to suspected violent felons. It demonstrates to them a genuine effort to apprehend all felony suspects in the safest manner possible.

The Vehicle Intercept Program also can generate some positive press coverage. Agencies should not overlook the public relations benefits and should publicize their efforts. Finally, vehicle intercepts result in fewer police pursuits, which translates into fewer liability claims against an agency.

Conclusion

As the nature and frequency of vehicle pursuits have changed in recent years, law enforcement agencies have been forced to reconsider their traditional practices. As demonstrated by the Hillsborough County Sheriff's Office Vehicle Intercept Program, alternatives to pursuits do exist and work. If law enforcement officers rethink the way they approach suspects in vehicles, offenders can be apprehended without the unnecessary endangerment of life and property caused by police pursuits. ✦

Endnotes

[1] P. Thrash, "Police Pursuit Considerations," *Law Enforcement Technology*, vol. 9, 1994, 28-30.

[2] B.L. Dorgan, "The National Police Pursuit Policy Act of 1995," *Congressional Record, Proceedings and Debates of the 104th Congress, First Session*, 141 (97).

Corporal Eisenberg and Corporal Fitzpatrick serve with the Hillsborough County Sheriff's Office in Tampa, Florida.

Canaries In Cages

Responding To Chemical/ Biological Incidents

By LARRY A. MEFFORD, M.P.A.

Photo © AP/Worldwide

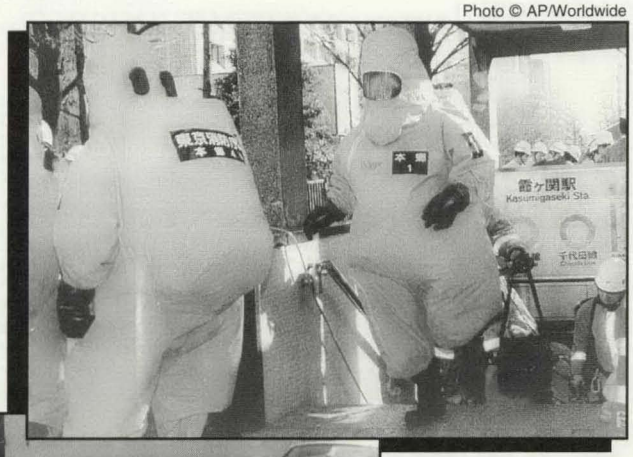


Photo © AP/Worldwide

Scenes from the nerve agent attack that occurred in the Tokyo, Japan, subway system on March 20, 1995.

Consider this scenario. Holiday sales have attracted large crowds to the sprawling suburban mall. Suddenly, as shoppers browse or hurry through the mall, a small bomb explodes in the food court, instantly killing 15 people and severely injuring more than a dozen other men, women, and children.

When the first mall security personnel arrive at the scene, they experience tightness in the chest and difficulty breathing. Dizziness and nausea ensue, and the officers rapidly begin to lose muscular control of their bodies.

The explosive device exposes responding police, fire, and medical personnel to lethal concentrations of a colorless and odorless vapor. Within minutes, more than 50 additional victims are overcome by the fumes lingering in the air. In total, nearly 100 people die in this attack.

Later that night, a major television news organization receives an anonymous telephone call from a man who states that the bomb was a chemical weapon deployed by a known radical organization. Claiming that the incident serves as a warning, he says that similar chemical weapons containing nerve agents have been hidden in populated areas throughout the United States and will be detonated remotely if the U.S. Government does not respond to the group's demands.

Is such a scenario plausible? More than 10 years ago, two foreign affairs specialists speculated that the most dangerous terrorist threat to the United States was not from the use of a nuclear device but from chemical and/or biological warfare.[1] Given the proliferation of the technology and the expanded number of countries capable of manufacturing such weapons worldwide, the specialists' warning rings even more true today.[2]

However, the threat now extends beyond traditional state-sponsored terrorist organizations. The nerve agent attack on March 20, 1995, in the Tokyo, Japan, subway system verifies this threat, and the 12 deaths and 5,500 injured Japanese citizens illustrate the grave danger that chemical and biological weapons pose.

No known domestic or international terrorist elements have signaled a change in tactics from traditional forms of terrorism, such as bombings and kidnappings, to the use of chemical and/or biological (C/B) weapons. Yet, the gravity of the potential use of such weapons, coupled with the capability demonstrated by the perpetrators of the Tokyo subway attack, requires that

American law enforcement agencies be prepared for such incidents. This article describes the threat posed by C/B weapons; the response required by local, state, and federal agencies to C/B incidents; and the statutory basis for investigating and prosecuting crimes involving these weapons.

> ***"For fanatical groups and individuals, the attraction of C/B weapons lies in their relative ease and economy of production..."***

Special Agent Mefford, currently assigned to the San Francisco Division of the FBI, formerly worked in the counterterrorism section of FBI Headquarters in Washington, DC.

THE THREAT

Initially developed to serve on the battlefield, chemical and biological weapons recently have been incorporated into the arsenals of certain criminal and terrorist organizations. Traditionally, a primary law enforcement concern was the procurement (by theft, purchase, or otherwise) of a stockpiled military C/B weapon by someone with criminal intent. However, the series of seven chemical weapon attacks that occurred in Japan between March 5, 1995, and July 4, 1995, clearly demonstrated the danger associated with the spread of C/B weapon technology.

Today, the traditional criminal motivated by monetary gain, or a psychologically unstable yet technically competent individual, could be capable of manufacturing such weapons, whereas in the past, such individuals had to acquire ready-made weapons. Of special concern should be those well-organized and dedicated groups—especially radical domestic and foreign organizations—that foster secrecy, possess ample financial resources, recruit competently trained individuals, and incorporate doomsday or other drastic beliefs.

Both the Japanese and American news media reported widely that the Japanese incidents were perpetrated to ensure that the predictions of a religious cult leader would come true. The chemical weapon attacks allegedly served as an omen for greater disasters, which the Japanese religious cult Aum Shinri Kyo hoped eventually would ignite a world war.[3]

For fanatical groups and individuals, the attraction of C/B weapons lies in their relative ease and economy of production, as compared to other methods of mass destruction. Also, the legitimate civil uses for C/B components (known as precursors) and related technology limit their control and make these substances relatively easy to acquire. This accessibility heightens the threat of C/B weapons being used.

To date, there have been no serious criminal C/B incidents in the United States; however, warning signs have been detected. For example, in 1994, the FBI arrested two individuals who reportedly belonged to an antigovernment, tax protest group in northern Minnesota for possession of a biological weapon. During the trial in St. Paul, the evidence indicated that the subjects had discussed using the lethal toxin Ricin, the substance they were convicted of possessing illegally, to kill certain public officials.

A chemical or biological incident conceivably could take many forms. It could involve the use of military C/B weapons, or an individual or group might attempt to threaten the public by sabotaging an existing stockpile of hazardous materials used for civilian purposes.

In general, the definition of a C/B incident includes any event that might cause mass casualties by the release or use of a hazardous material. This includes:

1) The manufacture or possession of a C/B weapon

2) The dispersal of a C/B agent among the civilian population, herds of livestock, or agricultural crops

3) The contamination of a municipal water or public food supply with a C/B agent

4) The sabotage of a hazardous chemical production or storage facility

5) The destruction or hijacking of a tractor-trailer or railroad tanker containing hazardous chemicals, or

6) The threat to accomplish one of the above.

THE WEAPONS

It is particularly difficult to define precisely what constitutes a C/B weapon because of the extensive legitimate civil uses for the raw materials used to produce them. From a law enforcement standpoint, the central factor in such a definition is the issue of intent. The existence of criminal intent—planning to commit a harmful act using such substances—differentiates peaceful, legitimate manufacturing and research efforts from the production of C/B agents for criminal purposes. Given that distinction, there are three basic types of C/B warfare agents—chemical agents, infectious agents, and toxins.

Chemical Agents

Chemical agents are compounds whose properties produce lethal or damaging effects in people, animals, plants, or materials. They can exist as solids, liquids, or gases and usually are classified by their effects as nerve, blood, choking, or blister agents. Nerve agents, such as tabun and sarin, and blood agents, such as hydrogen cyanide and cyanogen chloride, have particularly lethal effects and can cause death within minutes.

Infectious Agents

Infectious agents that produce illnesses in people are used to create biological weapons. These agents can include numerous bacteria, viruses, or fungi previously known to science, as well as new genetically engineered organisms. The infectious substances in biological weapons can kill or incapacitate large numbers of people. They generally require incubation periods of a few days following exposure before illness develops. Especially lethal diseases include anthrax and the plague.

Toxins

Toxins, unlike infectious agents, cannot reproduce, even though living microorganisms produce them. These poisonous substances require no incubation period, and some can cause incapacitation or death within minutes or hours.[4] Examples of deadly toxins used in biological weapons include botulinum toxins and ricin.

> ***"Televised news accounts showed Japanese police officers...carrying canaries in cages for rapid detection of the presence of chemical agents."***

THE DELIVERY

On their own, poisonous agents do not constitute a weapon. Their incapacitating results only take effect upon dispersal. To be used as weapons, they must be combined with a method of delivery, traditionally found in explosives, projectiles, or aerosol dispensers. Potential delivery systems range from the type of complex systems used in military bombs, mortars, missiles, or rockets to the relatively simple delivery methods, such as was used in the March 20, 1995, nerve agent attack in Tokyo.

In this incident, a small parcel containing several vials of chemicals was wrapped in newspaper and placed on the floor of a subway car. According to witnesses, after crushing the package with his hands or feet, the assailant calmly exited the subway car at the next stop. As the fumes generated by the combined chemicals produced the deadly nerve agent sarin, passengers immediately experienced the effects. As noted, 12 people died in the attack, and 5,500 were injured before Japanese authorities could evacuate and decontaminate the subway.

The criminals responsible for the chemical agent attacks in Japan have experimented with a variety of delivery methods. On May 5, 1995, a paper sack holding several condoms was discovered on fire in a subway station restroom. The condoms reportedly contained a chemical precursor necessary to produce the lethal blood agent hydrogen cyanide. Fortunately, a second bag containing the other chemical precursor had not ignited, thus preventing the lethal chemical reaction.[5]

Two months later, two additional devices also designed to produce hydrogen cyanide were discovered in public restrooms at a Tokyo subway station before the deadly gas had been released. A major news organization reported that perpetrators had equipped both devices with timing mechanisms

designed to remotely release and mix the chemicals.[6]

THE RESPONSE

Televised news accounts showed Japanese police officers in protective C/B suits and masks carrying canaries in cages for rapid detection of the presence of chemical agents. Those reports dramatically illustrate the uniquely dangerous challenge facing public safety agencies that must respond to such incidents.

Major American cities must consider C/B incident contingency plans that incorporate a variety of emergency services capabilities, such as evacuation, medical treatment, containment, decontamination, and criminal investigation and prosecution. These plans should incorporate resources from a variety of agencies, including police, fire, medical, and other emergency services providers assigned to respond to incidents involving mass casualties and/or contaminated environments.

Local and State

Local law enforcement officers probably will be the first responders to any chemical or biological incident. As such, they are responsible for verifying the threat, evacuating affected areas, and attempting to prevent detonation of the C/B weapon, if possible.

If detonation occurs, local authorities must cope with the immediate results of the incident, known as consequence management. This includes saving lives, providing medical treatment to the injured, housing and feeding evacuated citizens, and decontaminating affected areas. Local and state authorities, however, often do not possess expertise in dealing with C/B weapons, which originally were developed by and for the military. Therefore, additional assistance might be needed.

Photo © Mark Ide

Federal

To augment local and state resources in addressing a chemical or biological incident, the FBI has been designated the lead agency for coordinating the federal response. As such, it has developed the Chemical/Biological Incident Contingency Plan.

The plan marshals the appropriate federal technical, scientific, and medical operational support to bolster the FBI's investigative and crisis management abilities. Through this plan, federal agencies provide local authorities with coordinated operational support. This support includes advice regarding technical issues, as well as operational deployment of resources and personnel to the scene.

To activate the federal plan, local police should call the nearest FBI field office, which in turn will coordinate any federal response with FBI headquarters. The FBI's four-step contingency plan incorporates a graduated response to C/B incidents. The four steps are threat assessment, provision of technical advice to the incident manager, deployment of technical personnel and resources to the scene, and marshalling of consequence management resources.

The contingency plan brings together specialized resources drawn primarily from the Department of Defense (DOD), the Department of Health and Human Services (HHS), and the Environmental Protection Agency (EPA). The DOD components provide technical expertise in military weapons systems, including conventional explosives that might be associated with a C/B weapon. DOD also possesses decontamination, sampling, and threat profiling capabilities. HHS and EPA components can monitor, test, and analyze the threat and also provide other specialized medical and laboratory support.

In addition, these agencies might have consequence management responsibilities in the aftermath of a C/B incident. These duties involve taking steps to mitigate the extent of the injuries and damage inflicted. Even though state and local agencies hold the primary responsibility to provide such services, in a potentially catastrophic incident, numerous federal agencies would be available to assist. In addition to those already mentioned, the Federal Emergency Management Agency, the Department of

Transportation, and the Department of Agriculture likely would help, as well as others, depending on the facts of the incident.

The various steps of the plan can be implemented gradually or simultaneously, as dictated by the circumstances surrounding the incident. For example, in case of a credible threat, some emergency arrangements, such as alerting hospital staffs and preparing for evacuation, might be activated, even if the C/B agent has not been released. As a result, both law enforcement and related emergency management actions would combine to handle a credible C/B threat.

The FBI's plan does not address noncriminal hazardous materials cases or the presence of suspicious substances without clear terrorist or other significant criminal implications. It focuses on the law enforcement aspects of a C/B incident, while concurrently addressing the integration of law enforcement and consequence management actions. It is designed to improve the Federal Government's overall ability to augment and effectively assist municipal, county, and state entities in responding to and mitigating the effects of a criminal chemical or biological incident.

THE LEGISLATION

Of course, the effectiveness of any contingency plan hinges on preventing potential attacks before C/B agents can be disseminated. For this reason, an adequate statutory basis for collecting intelligence, seizing evidence, and prosecuting culpable individuals must exist. In terms of weapons of mass destruction, nuclear weapons traditionally have received most of the public's attention, which has resulted in adequate criminal legislation in the nuclear field.[7]

While no similar comprehensive federal criminal legislation has been developed for chemical weapons, pertinent legislation does exist to address biological weapons. A U.S. senator introduced the "Biological Weapons Anti-Terrorism Act of 1989" in May of that year. In justifying the legislation, he stated, "Biological weapons are becoming increasingly easy to make and offer terrorists a simple way to inflict mass destruction. With the recent advances in genetic engineering, this country can no longer afford this potentially disastrous loophole in its criminal code."[8]

> ***"To be used as weapons, [poisonous agents] must be combined with a method of delivery."***

The act took effect in May 1990[9] and makes it illegal to manufacture or possess biological weapons or to assist a foreign country in the development of such a weapon. Additionally, the statute authorizes the U.S. Attorney General to seize and destroy biological weapons. It also contains extraterritorial provisions.[10]

In the absence of other specific legislation, law enforcement agencies still have ways to pursue criminals who brandish these deadly weapons. When C/B weapons are associated with the criminal intent to violate other criminal statutes, a legal method to seize evidence and make arrests exists, as provided for under various state or federal criminal codes. Depending on the circumstances, the FBI might address C/B incidents by applying federal environmental crimes,[11] tampering with consumer products,[12] extortion,[13] or conspiracy[14] laws. State law enforcement agencies can apply other charges, including murder, attempted murder, assault, and extortion.

CONCLUSION

If, as claimed by the anonymous caller depicted earlier, additional chemical weapons containing nerve agents actually had been hidden in populated areas throughout the United States, how would U.S. law enforcement respond? In concert with other law enforcement agencies, the FBI would employ the C/B Incident Contingency Plan. The primary goal always is to prevent dispersal of the nerve agents by proficiently using appropriate intelligence information. Secondary goals include mounting an effective operational response and, thereafter, containing and minimizing the consequences of an incident.

Above all else, chemical and biological incidents require efficient public communication, rapid access to technical and scientific information, and a coordinated effort on the part of all involved agencies. Only through a coordinated and combined effort can law enforcement agencies across the country provide the best

possible protection for the citizens they serve.

With a little luck and a lot of hard investigative work, perhaps no U.S. law enforcement agency will ever have to respond to a lethal nerve agent attack similar to the one described in the opening scenario. With some planning, no agency need be caught unprepared if it does. ✦

Endnotes

[1] Neil Livingstone and Joseph Douglass, Jr., *CBW: The Poor Man's Atomic Bomb* (Washington, DC: Institute for Foreign Policy Analysis, Inc., 1984).

[2] "Chemical Arms: Navy Report Asserts Many Nations Seek or Have Poison Gas," *New York Times*, March 10, 1991, 1.

[3] "Engineer of Doom: Cult Leader Shoko Asahara Didn't Just Forecast Armageddon, He Planned It," *Time*, June 12, 1995, 57.

[4] Congress, Senate, Committee on Governmental Affairs, Hearing by the Senate Judiciary Committee Regarding Biological Anti-Terrorism Act of 1989, 101st Cong., 2d sess., May 17, 1989.

[5] "Aum Reportedly Planted Cyanide Gas Device at Shinjuku Station," *The Daily Yomiuri*, June 14, 1995, 1.

[6] "More Gas Bombs Found in Tokyo Subways," Cable News Network, July 5, 1995.

[7] The Atomic Energy Act of 1954, as amended, 42 U.S.C. § 2011 (1954); and Prohibited Transactions Involving Nuclear Weapons, as amended, 18 U.S.C. § 831 (1948).

[8] U.S. Senator Kohl, Press Release, May 16, 1989.

[9] 18 U.S.C. § 175 (1990).

[10] Extraterritorial provisions of certain federal statutes provide the FBI with the legal jurisdiction to gather evidence and seek U.S. prosecution of defendants for certain actions committed against U.S. citizens overseas.

[11] See especially, the Toxic Substances Control Act, 15 U.S.C. § 2614 (1976); and the Clean Water Act, as amended, 33 U.S.C. § 1319 (1948).

[12] Tampering With Consumer Products, 18 U.S.C. § 1365 (1983).

[13] Mailing Threatening Communications, as amended, 18 U.S.C. § 876 (1948).

[14] Conspiracy to Commit Offense or to Defraud United States, 18 U.S.C. § 371 (1948).

FaxBack Question

How has the Internet helped your agency?

The number of law enforcement agencies establishing home pages or other sites on the Internet has increased dramatically during the past 2 years. As these sites proliferate, agencies are discovering innovative ways to use the Internet to increase interaction with citizens, complement investigative strategies, and streamline department operations. For example, some departments use their home pages to provide recruiting information and electronic application forms that potential candidates can complete via the Internet.

Has your agency developed a home page or similar site (bulletin board, listserv, etc.)?

- If so, how many "hits" does your site receive each month?
- What type of information about your agency do you post?
- What innovative uses has your agency found for its Internet site?
- If your agency has not established a site on the Internet, what factors are hindering such an initiative? Do you believe a site would be beneficial?

Responses will be shared with readers in an upcoming issue of *Law Enforcement*.

How to Respond

Fax response to FaxBack at (703) 640-1474. Responses also may be mailed to the Law Enforcement Communication Unit, FBI Academy, Madison Building, Room 209, Quanitico, Virginia 22135, or sent via e-mail to leb@fbi.gov.

Book Review

To Serve and Protect: A Tribute to American Law Enforcement *by Glenn Gamber and Connie Clark, et. al., produced by the National Law Enforcement Officers Memorial Fund, Inc., Turner Publishing Company, Paducah, Kentucky, 1995.*

The history of American law enforcement is a tale of triumphs and tragedies. *To Serve and Protect* provides a concise but highly detailed account of policing from the colonial era to the present. The narrative traces the progress of American law enforcement from the first night watch established in Boston in 1631 to the chaotic frontier justice of the 1800s, from the reforms of the early 20th century and the rise of professionalism in the 1930s to the technological advances and community-oriented strategies that mark policing today.

The focus of the book, however, is to commemorate the personal tragedies that have accompanied this progress. In addition to providing an updated listing of the names inscribed on the National Law Enforcement Officers Memorial in Washington, DC, the book chronicles the lives and deaths of many of the officers honored there.

The remembered include U.S. Marshal Robert Forsyth, who became the first American law enforcement officer to die in the line of duty when he was shot while serving court papers to two brothers in Augusta, Georgia, in 1794. From Forsyth to J.H. "Cracker" Johnson, a motorcycle officer with the Waycross, Georgia, Police Department, who died from injuries sustained when he was thrown from a moving car by bootleggers in 1931, to Gail Cobb, the first African-American policewoman to die in the line of duty, shot while apprehending a bank robbery suspect in Washington, DC, on September 20, 1974, the stories trace the social changes that have impacted policing during the past 2 centuries. They also serve as a testament to the selfless dedication to duty that characterizes America's law enforcement officers.

Some of the accounts illuminate the lives of officers whose heroism may have been overshadowed by the circumstances surrounding their deaths. Such is the case with J.D. Tippit, an 11-year veteran of the Dallas Police Department, who shortly past 1:00 p.m. on November 23, 1963, became the second person killed by Lee Harvey Oswald. Officer Tippit, a well-regarded patrolman, had stopped Oswald when he observed that the suspicious young man fit the description of the suspected assassin of President John F. Kennedy.

The book also reflects the strange sense of irony that often haunts police work. On the wall of the National Law Enforcement Officers Memorial, J.D. Tippit's name appears next to John Kennedy's—a New York City police officer killed in 1922.

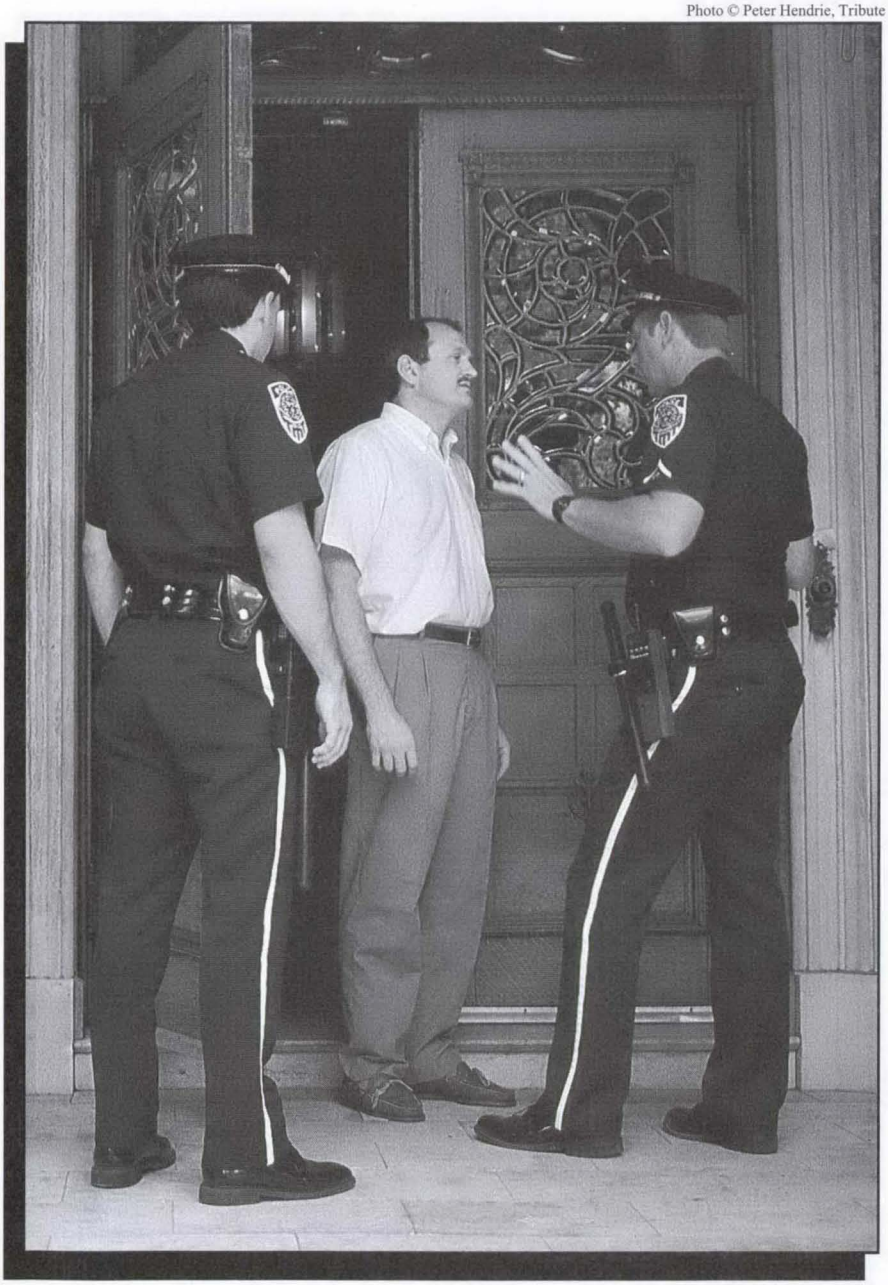
To Serve and Protect pays tribute to America's fallen officers by celebrating their lives and honoring their sacrifices through the remembrances of family members, friends, and fellow officers. The historical context in which the epitaphs appear strengthens the connection of these seemingly distinct tragedies by commemorating the shared sense of commitment that typifies the officers honored at the National Law Enforcement Officers Memorial.

Reviewed by
Andrew DiRosa
Associate Editor
FBI Law Enforcement Bulletin
FBI Academy
Quantico, Virginia

Consent Searches
Guidelines for Officers

By KIMBERLY A. CRAWFORD, J.D.

Photo © Peter Hendrie, Tribute



Consent can be an effective weapon in an investigator's arsenal. When asked for permission to search, individuals with plenty to hide often defy common sense and waive their constitutional right to privacy. Evidence confiscated during a consent search is admissible in a subsequent trial, as long as the officer conducting the search follows the fundamental requirements of the consent to search doctrine and is able to prove the same.

When the Supreme Court decided *Schneckloth* v. *Bustamonte*[1] in 1973, and *United States* v. *Matlock*[2] in 1974, consent as an exception to the fourth amendment warrant requirement became a fairly well-settled principal of law. Of the few questions pertaining to consent searches that remained unresolved following *Schneckloth* and *Matlock*, most were answered by the Supreme Court in the cases of *Illinois* v. *Rodriguez*[3] and *Florida* v. *Jimeno*.[4] However, one question relating to consent searches that remains unanswered by the Supreme Court is whether law enforcement officers can rely on an individual's consent that is given in the wake of another individual's refusal to consent.

This article examines the parameters of the consent to search doctrine established by the Supreme Court in *Schneckloth*, *Matlock*, *Rodriguez*, and *Jimeno*. It then discusses legal and policy considerations for investigators when seeking consent from one person following another person's refusal to consent.

FOUNDATIONS OF THE CONSENT TO SEARCH DOCTRINE

In *Schneckloth* and *Matlock*, the Supreme Court established the two prerequisites for a valid consent to search. Specifically, the Court held that a lawful consent must be given voluntarily and by a person with authority. Moreover, because consent is an exception to the general requirement that searches be conducted pursuant to a warrant, the government bears the burden of proving both of these prerequisites.

When determining the voluntariness of a consent to search, courts use a "totality of the circumstances"[5] test, where all the factors surrounding the consent are examined to determine whether it was a product of the consenter's free will. Using this test, courts have concluded that the following factors do not necessarily render a consent involuntary:

1) The failure to advise an individual of the right to refuse consent[6]

2) The fact that officers had their weapons drawn and had handcuffed an individual prior to asking for consent,[7] and

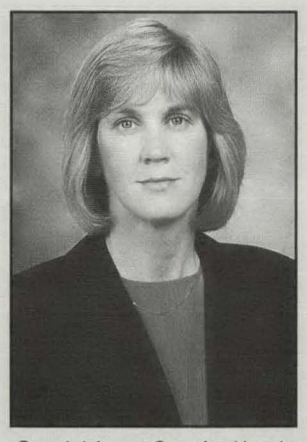
3) The obtaining of consent from a person under the influence of drugs.[8]

Officers should recognize, however, that although these factors do not automatically necessitate a finding of involuntariness, they are factors that courts carefully weigh in the totality of circumstances test to determine the voluntariness of a consent.

The determination of who has lawful authority to consent to a search will depend initially on the object of the intended search. If law enforcement officers want permission to search a person, then only the person to be searched has the authority to consent. If, on the other hand, officers desire to search premises, vehicles, or items of personal property that can be shared by two or more people, the determination of who may consent to the search will require an analysis of who has a fourth amendment right of privacy in the area.[9]

Because consent is a waiver of the fourth amendment right of privacy, only an individual with that right of privacy may consent to a search. The fourth amendment right of privacy, however, is not a function of ownership. Thus, the fact that an individual owns an apartment building does not automatically give this individual a fourth amendment right of privacy in a rented apartment that he can waive by consent.

Rather than ownership, the courts look for lawful access and control when determining authority to consent. If individuals share access and control over an area, there is common authority to consent to search of that area.[10]



Special Agent Crawford is a legal instructor at the FBI Academy.

> ***"...lawful consent must be given voluntarily and by a person with authority."***

REFINEMENTS TO THE CONSENT DOCTRINE

In the two decades that followed the *Schneckloth* and *Matlock* decisions, the Court further refined the parameters of the consent doctrine by addressing two questions of importance to investigators. First, can consent be obtained lawfully from a person with "apparent authority"? Second, what is the appropriate test for officers to determine the scope of a person's consent?

Apparent Authority Ruled Sufficient

In *Illinois* v. *Rodriguez*,[11] the Court created the concept of

apparent authority, which gives law enforcement officers some latitude when attempting to ascertain who has authority to consent to a search. The case arose when police, responding to a domestic complaint, entered an apartment pursuant to the complainant's consent. Once inside, officers arrested Rodriguez and seized a substantial quantity of cocaine and drug paraphernalia that was in plain view.

At a subsequent suppression hearing, the court discovered that although the complainant used a key taken from her purse to unlock the apartment door for the officers, the complainant did not live there at the time of the search. Rather, she and her two children had moved out of the apartment weeks prior to the search and had taken most of their belongings. Moreover, testimony revealed that the complainant's name was not on the lease, she did not contribute to the rent, and Rodriguez did not know that she had a key to the apartment. Based on these facts, the trial court concluded that the complainant had no authority to consent to a search of the apartment and granted Rodriguez's motion to suppress.

On review, the Supreme Court agreed that under the ruling in *Matlock*, the complainant would not have the requisite access or control over the apartment to consent. However, the Court continued its analysis by concluding that a consent may be valid if, at the time of the search, police *wrongly but reasonably believe* that the consenting party possesses common authority over the premises. Thus, the Court created the concept of apparent authority.

In creating the concept of apparent authority, the Supreme Court recognized that the fourth amendment prohibits only *unreasonable* searches and seizures.[12] The Court has held repeatedly that while law enforcement officers do not have to be correct or certain in order to comply with the fourth amendment, they do have to be reasonable.

> ***"Rather than ownership, the courts look for lawful access and control when determining authority to consent."***

In *Rodriguez*, the Court found no justification to depart from this reasonableness standard when determining whether an individual has sufficient access and control over premises to give a valid consent to search. If it is reasonably apparent to officers that the individual giving consent has the authority to do so, then the fourth amendment reasonableness standard is satisfied.

The concept of apparent authority rewards officers who use good judgment and common sense when determining an individual's authority to consent. It is important to note, however, that apparent authority does not relieve officers of their obligation to ask questions and develop information with respect to a consenting individual's access and control. Because the burden of proof remains on the government to establish the reasonableness of the belief that the consenting individual had the authority to do so, it is important for officers to document the efforts they make to gather information regarding an individual's access and control over the property to be searched by consent.[13]

Scope of the Consent

In *Florida* v. *Jimeno*,[14] the Court attempted to clarify the scope of a lawful consent search. The case was initiated when an officer, who had previously overheard Jimeno setting up a drug deal, stopped him for a traffic violation. After issuing a traffic citation, the officer advised Jimeno that he had reason to believe that there were drugs in the car and asked for consent to search. Jimeno indicated he had nothing to hide and gave the officer permission to search. On the passenger side of the car, the officer found a folded brown paper bag that contained a kilogram of cocaine.

After being charged with possession with intent to distribute cocaine, Jimeno successfully moved the trial court to suppress the evidence on the grounds that his consent to search the car did not extend to containers inside the car. On review, the Supreme Court found Jimeno's argument to be an illogical repudiation of the fourth amendment reasonableness standard and held that the "standard for measuring the scope of a suspect's consent...is that of 'objective reasonableness'—what would the typical reasonable person have understood by the exchange between the officer and the suspect."[15]

Applying the "objective reasonableness" standard to the facts in *Jimeno*, the Court concluded that it was reasonable for the officer to believe Jimeno's general consent to search his car included the bag lying on the floor of the car. Therefore, the search was lawful.

The Court's adoption of the objective reasonableness standard for measuring the scope of a consent closed the door on defense attempts to limit searches by arguments that defy logic. Law enforcement officers are not required to consider every conceivable interpretation of a consent prior to carrying out a search. Rather, officers are simply required to give the consent a reasonable interpretation when acting upon it.

If officers identify the specific object of their search when requesting consent to search, the scope of the consent subsequently given is easy to define. A voluntary consent given to search for a specific object allows officers to look anywhere that object reasonably could be concealed. For example, officers who receive consent to search an area for drugs can logically conclude that they may search wherever drugs reasonably could be hidden.[16]

CONFLICTING RESPONSES TO REQUESTS FOR CONSENT

The Supreme Court's decisions in *Rodriguez* and *Jimeno* clarified several consent issues, and by applying a standard of reasonableness, brought consent in line with all areas of fourth amendment law. While the Court has not resolved the often-confronted question of whether a consent is valid if it follows another individuals refusal to consent, lower federal courts have addressed that issue.

Lower Federal Court Decision

In *United States* v. *Morning*,[17] federal law enforcement officers received information from a confidential source that a woman and a man named "Poncho" had a large quantity of marijuana at their residence. Acting on this information, two officers knocked on the front door and advised Morning, the woman who answered the door, that they were conducting a drug investigation and would like permission to search the premises.

> ***"Law enforcement officers are not required to consider every conceivable interpretation of a consent prior to carrying out a search."***

When Morning replied that she would prefer that they get a warrant, the officers asked if anybody else lived in the house. In response, Morning stated that Poncho also lived there and she left to get him. When Poncho came to the door, the officers again stated their purpose in being there and asked Poncho for consent to search. Poncho not only consented to the search but also told the officers where they could find the marijuana.

After the officers searched the residence and found 226 pounds of marijuana, Poncho and Morning were arrested and charged with possession with intent to deliver. In a subsequent motion to suppress, Morning argued that the search of the residence without a warrant could not be justified by Poncho's consent because she had previously denied consent by stating her preference for a warrant. When the trial court rejected Morning's argument, she entered a plea of guilty and preserved her argument for appeal.

On appeal, the U.S. Court of Appeals for the Ninth Circuit first reviewed the facts to determine whether Poncho and Morning had common authority to consent to a search of the premises, using the *Matlock* formula of lawful access and control. Finding that both individuals lived in and shared the very small house in question, the court concluded that there was joint access and control and either party could lawfully consent to a search of the premises.[18]

Next, the court undertook the real question at issue—whether Poncho's otherwise valid consent to search was nullified by Morning's previous refusal to consent. First, the court reviewed the Supreme Court's decision in *Matlock* and quoted the following passage:

> [W]here people have joint access and control over property 'it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.[19]

Emphasizing the Supreme Court's notion of assumption of

the risk, the court concluded that individuals who refuse to consent to a search of an area over which they share access and control do not have a right to expect that those with whom they share will likewise deny their consent. Individuals who refuse to consent may have a fond hope that others will follow suit, but fond hopes are not protected by the Constitution.

Applying this rationale to the facts in *Morning*, the court found that by sharing premises with Poncho, Morning assumed the risk that he would consent to a search of those premises. This assumption was, in no way, affected by Morning's efforts to exercise her own right of privacy by denying consent to search.[20]

The court's reasoning in *Morning* is compatible with that of several other courts that have dealt with the same issue.[21] Courts consistently hold that assumption of the risk precludes a defendant from successfully claiming that fourth amendment rights have been violated when another person consents to a search of a shared area, even when the other's consent follows the defendant's refusal to do so.[22]

Equal Access Necessary to Override Refusal to Consent

Law enforcement officers who conduct a search based on an individual's consent that follows another individual's refusal to consent must be careful to determine that the consenting individual has, at least, equal access and control over the area being searched. Only a consent given by a person with equal or superior access and control over an area can supersede another's refusal to consent.

In *United States* v. *Impink*,[23] for example, a landlord, who had retained the right to access leased premises for the limited purpose of storing a piece of equipment, noticed some suspicious glasses, flasks, and burners on the property. The landlord subsequently notified the police and gave an implied consent to a search of the premises. This consent was followed by the tenant's specific refusal to consent. When 50 pounds of methamphetamine subsequently were found on the premises, the tenant was arrested and ultimately convicted.

Photo © Mark Ide

When this case reached the U.S. Court of Appeals for the Ninth Circuit, the court noted that the landlord's right of access was extremely limited and considerably inferior to that of the tenant. Given the landlord's unequal right of access, coupled with the tenant's refusal to consent, the court held that the search of the premises pursuant to the landlord's consent was a denial of the tenant's fourth amendment rights and suppressed the evidence.[24]

Because only a person with an equal or greater right of access can override another's refusal to consent, law enforcement officers must be careful to develop facts that would allow them to reasonably conclude that the person giving consent has such equal or greater right. Once this reasonable conclusion is drawn, officers can act on the consent, despite the protest of the nonconsenting party.

CONCLUSION

Consent is a viable exception to the fourth amendment warrant requirement when obtaining a warrant is not practicable. The Supreme Court has ruled that the standard for reviewing the lawfulness of a consent search is objective reasonableness, thereby obviating the need for law enforcement officers to be absolutely correct when conducting a search pursuant to a consent. Moreover, the legality of a search following conflicting responses to a request for consent has received approval from the lower courts where the consenting person has, at least, equal access and control over the area being searched.

The overall effect of these recent cases is that consent has become a more valuable investigative tool. Law enforcement officers must always be mindful, however, that the government bears the burden of proving the lawfulness of any consent search. Accordingly, officers who rely on a consent to search must be careful to develop the necessary facts to justify reliance on the consent and to document thoroughly the circumstances surrounding the consent. Where feasible, it also is advisable for officers to consult with a legal advisor prior to conducting a consent search. ✦

Endnotes

[1] 412 U.S. 218 (1973).

[2] 415 U.S. 164 (1974).

[3] 110 S.Ct. 2793 (1990).

[4] 111 S.Ct. 1801 (1991).

[5] 412 U.S. at 227.

[6] *Id.*

[7] *United States* v. *Wilkinson*, 926 F.2d 22 (1st Cir. 1990), *cert. denied*, 501 U.S. 1211 (1991).

[8] *Id.*

[9] 415 U.S. at 171.

[10] In *Matlock*, the Court instructed lower courts to evaluate common authority to consent to a search as follows:

> Common authority is, of course, not to be implied from the mere property interest a third party has in the property. The authority which justifies the third-party consent does not rest upon the law of property, with its attendant historical and legal refinements,...but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.

[11] 110 S.Ct. 2793 (1990).

[12] U.S. Const. amend. IV reads in pertinent part: "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated...."

[13] *See, e.g.*, *People* v. *Kramer*, 562 N.E.2d 654 (Ill. App. 4 Dist. 1990), *appeal denied*, 571 N.E.2d 152 (1991).

[14] 111 S.Ct. 1801 (1991).

[15] *Id.* at 1803-4.

[16] For a discussion of locked containers in the area subject to search, see Crawford, "The Consent to Search Doctrine—Apparent Refinements," *FBI Law Enforcement Bulletin*, July 1992, pp. 26-32.

[17] 64 F.3d 531 (9th Cir. 1995), *cert denied*, 116 S.Ct. 1030 (1996).

[18] The district court actually found that Poncho had "superior authority" over the premises because he resided there full time and paid the bills. *Id.* at 534.

[19] *Id.* at 536 quoting *Matlock*, 415 U.S. at 171 n. 7.

[20] *Id.*

[21] *See, e.g.*, *United States* v. *Sumlin*, 567 F.2d 684 (6th Cir. 1977), *cert. denied*, 435 U.S. 932 (1978); *United States* v. *Hendriz*, 595 F.2d 883 (D.C. Cir. 1979); *United States* v. *Morales*, 861 F.2d 396 (3d Cir. 1988)(fn. 9); *J.L. Foti Construction Co.* v. *Donavan*, 786 F.2d 714 (6th Cir. 1986).

[22] *Id.*

[23] 728 F.2d 1228 (9th Cir. 1984).

[24] *See also*, *United States* v. *Warner*, 843 F.2d 401 (9th Cir. 1988).

The Bulletin Notes

Law enforcement officers are challenged daily in the performance of their duties; they face each challenge freely and unselfishly while answering the call to duty. In certain instances, their actions warrant special attention from their respective departments. *Law Enforcement* also wants to recognize their exemplary service to the law enforcement profession.

Specialist Sommer

Officer White

During the early morning hours, Specialist Gary Sommer and Officer Mark White of the Breckenridge, Colorado, Police Department responded to the scene of a single vehicle accident. The vehicle had careened off the roadway and settled upside down in the rushing waters of the Blue River. Specialist Sommer and Officer White waded into the river and found the unconscious driver trapped by his seatbelt in the vehicle. Observing that the man was turning blue, the officers quickly cut him loose from the seatbelt and carried him to the riverbank. There, they revived the victim by clearing his airway and administering CPR. Responding medical units later transported the man to a medical facility, where he was treated and released. The man probably would have drowned in his vehicle had it not been for the quick, professional response of Specialist Sommer and Officer White.

Deputy Christmas

Deputy James Daniel "Danny" Christmas of the Ware County, Georgia, Sheriff's Department responded to the report of a structure fire at an area residence. When he arrived at the scene and realized that he knew the residents, Deputy Christmas advised the dispatcher to call their workplace to determine if they were at work. Upon being informed that two females might be asleep in the house, Deputy Christmas entered the burning residence and found the women sleeping in a smoke-filled bedroom. As fire began to race across the ceiling of the room, Deputy Christmas awoke the women and led them to safety. He then rescued two puppies from the residence.

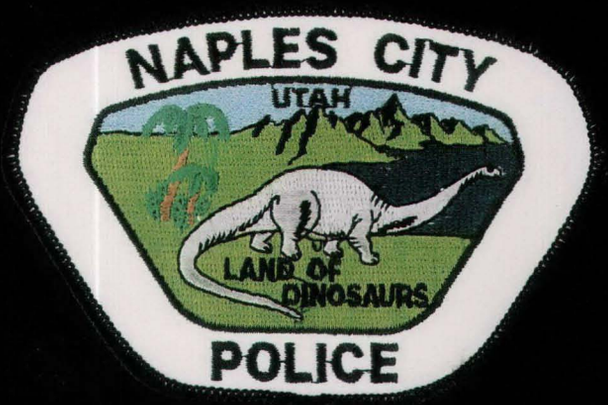
Nominations for the ***Bulletin Notes*** should be based on either the rescue of one or more citizens or arrest(s) made at unusual risk to an officer's safety. Submissions should include a short write-up (maximum of 250 words), a separate photograph of each nominee, and a letter from the department's ranking officer endorsing the nomination. Submissions should be sent to the Editor, *FBI Law Enforcement Bulletin*, Law Enforcement Communication Unit, Quantico, VA 22135.

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

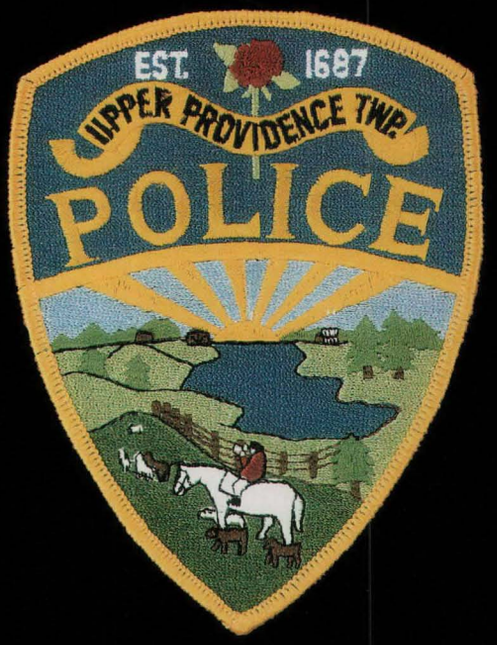
Periodical
Postage and Fees Paid
Federal Bureau of Investigation
ISSN 0014-5688

Official Business
Penalty for Private Use $300

Patch Call



The Naples City, Utah, Police Department patch depicts a brontosaurus walking through a prehistoric landscape. Naples City is home to the Dinosaur National Museum; the area surrounding the city is known as the "Land of Dinosaurs."



The patch of the Upper Providence Township, Pennsylvania, Police Department features a scenic view of the local hunt country. The township, known for its plentiful wild roses, was founded by Quaker settlers in 1687. The area has a strong heritage of fox hunting, horse racing, and steeplechases.