U.S. Department of Justice
Federal Bureau of Investigation

DECEMBER 1996

FBI Law Enforcement B·U·L·L·E·T·I·N

Computer Crime

December 1996
Volume 65
Number 12

**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 an endorsement by the FBI for any policy, program, or service.

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. Periodical 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
Linda W. Szumilo

Internet Address:
leb@fbi.gov

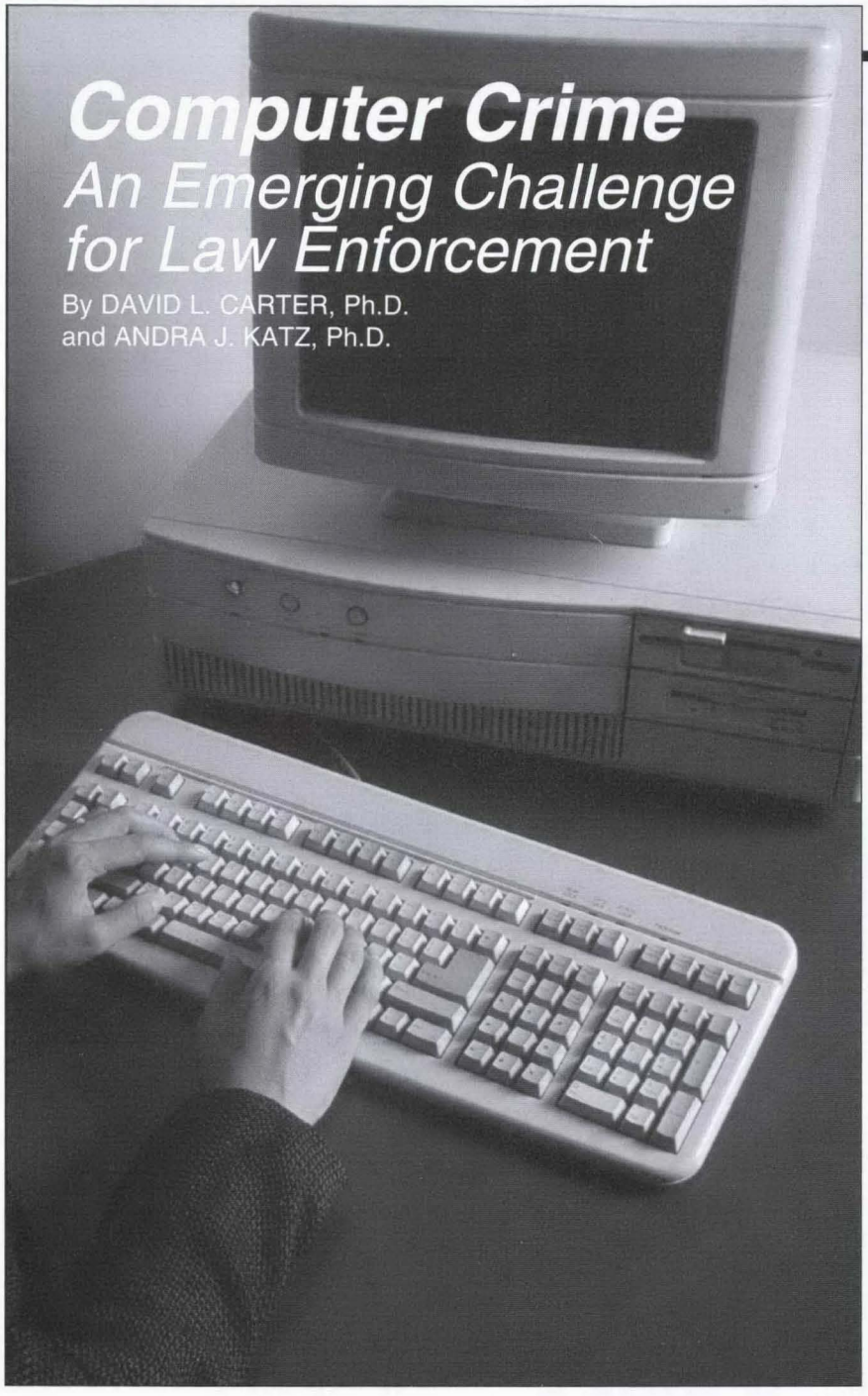
Cover photo ©
Photodisc

FBI Law Enforcement B·U·L·L·E·T·I·N

Features

Departments

ISSN 0014-5688 USPS 383-310



Computer Crime
An Emerging Challenge for Law Enforcement

By DAVID L. CARTER, Ph.D.
and ANDRA J. KATZ, Ph.D.

Law enforcement has withstood many challenges over the years. Prohibition, organized crime, riots, drug trafficking, and violent crime exemplify some of the complex problems the police have faced. Now law enforcement confronts another problem that is somewhat unusual—computer-related crime.

Several factors make this type of criminality difficult to address. Lawbreakers have integrated highly technical methods with traditional crimes and developed creative new types of crime, as well. They use computers to cross state and national boundaries electronically, thus complicating investigations. Moreover, the evidence of these crimes is neither physical nor human but, if it exists, is little more than electronic impulses and programming codes.

Regrettably, the police have fallen behind in the computer age and must overcome a steep learning curve. To make matters worse, computer crime is sometimes difficult for police officials to comprehend and to accept as a major problem with a local impact, regardless of the size or location of their communities.

Futurist Alvin Toffler identified information as the commodity of greatest value as the new millennium approaches.[1] Indeed, the Securing Proprietary Information Committee of the American Society of Industrial Security observed that the value of a company's future lies not in its tangible assets, but in the "intellectual capital" of the business.[2] In most businesses today, intellectual property is kept in computers. As a consequence, the computer has become the target—and sometimes the instrument—of crimes.

We conducted a national study of corporate security directors to explore the environment of computer crime and identify some critical issues facing policy makers in the future. The creation of computer crime units in the Secret Service, Air Force Office of Special Investigations, FBI, and a small number of state and

local agencies shows that law enforcement agencies are beginning to recognize the significance of computer crime. The growth of such groups as the Florida Association of Computer Crime Investigators and the High Tech Crime Investigators Association, as well as the proliferation of computer crime specialists in such agencies as the Royal Canadian Mounted Police, Royal Thai Police, and London Metropolitan Police Department, confirms the rising worldwide awareness of computer crime. Still, as one respondent to this study observed:

> I feel the weakest link is the lack of education in [public] law enforcement relating to computer-technology crimes. The law enforcement community has devoted [itself] to the high priority violent crimes, lumping computer crimes into a low priority status, yet the losses to computer crime could fund a small country.

RESEARCH FINDINGS

While many crimes using computer technology mirror traditional offenses—such as theft or fraud—the technical complexity, speed, and creative avenues by which these crimes occur pose particular problems for detection, prosecution, and prevention. If the trend of computer crime over the last 5 years provides any indication of the future, law enforcement's problems have just begun.

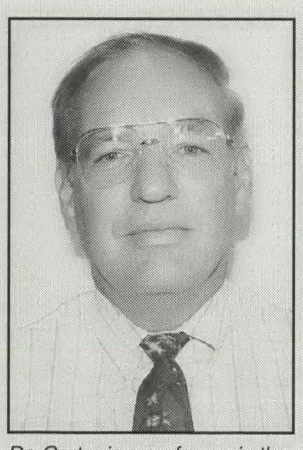
Victimization

The extent of computer crimes appears to be expanding rapidly. A study conducted by the American Bar Association (ABA) in 1987 found that of the 300 corporations and government agencies questioned, 72 (24 percent) claimed to have been the victim of a computer-related crime in the 12 months prior to the survey.[3] The combined estimated losses from these crimes ranged from $145 million to $730 million over the 1-year period.

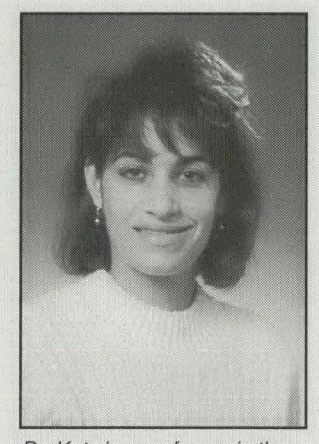
This broad range illustrates the problem in estimating losses. Not only is it difficult to identify and document these crimes, it is even more difficult to place a monetary value on the loss of intellectual property for which the actual value may not be known for months or even years.

Two years later, in 1989, the Florida Department of Law Enforcement (FDLE) surveyed 898 public and private sector organizations that conducted business by computer. Of the 403 respondents, 25 percent reported they had been victimized by computer criminals.[4] The Florida study found embezzlement of funds by employees to be a major source of the crimes. No attempt to estimate losses was made because, according to one of the researchers interviewed, "losses would have been nothing more than a guess."

In perhaps one of the most comprehensive studies, a component of the United Nations Commission on Crime and Criminal Justice surveyed 3,000 Virtual Address Extension (VAX) sites in Canada, Europe, and the United States in 1991 to assess computer security threats and crimes. The results show that 72 percent of the respondents reported a security incident within the previous 12 months, with 43 percent reporting the incident was criminal in nature.[5] By far, the greatest security threats came from employees or



Dr. Carter is a professor in the School of Criminal Justice at Michigan State University, East Lansing, Michigan.



Dr. Katz is a professor in the Administration of Justice Department at Wichita State University, Wichita, Kansas.

other people with access to the computers; however, respondents reported a number of external breeches from crackers[6] telephoning into the systems or accessing via networks.

The ABA and FDLE studies barely mentioned this external threat and gave little attention to it as a growing problem. This is not surprising, however, because predominantly only the military, academics, and researchers used networking in the late 1980s. Access was comparatively limited, and networking technology cost more than it does today. The 1991 United Nations study, however, identified external threats via remote access as a problem that would grow in the years to come.[7] Despite this concern, past research suggests that threats of computer crime generally come from employees, like much of the theft that occurs in retail businesses.

Our study found a trend of victimization that increased significantly over previous studies, with 98.5 percent of the respondents reporting they had been victimized, and 43.3 percent admitting to being victimized more than 25 times. While these numbers seem dramatic, security professionals who reviewed the data expressed surprise at the frequency of *admitted* victimization, not actual victimization.

Consistent with previous studies, employees committed most of the reported crimes. The primary threat came from full-time employees, followed by part-time and contract employees, with computer crackers a close third. The researchers expected this finding because of the correlation between theft and access to computers.[8] However, the important dynamic to recognize is that access is changing dramatically as networking becomes more widespread. As the probability of these crimes increases, so will the public's expectation that state and local law enforcement agencies will be able to respond to and investigate these offenses.

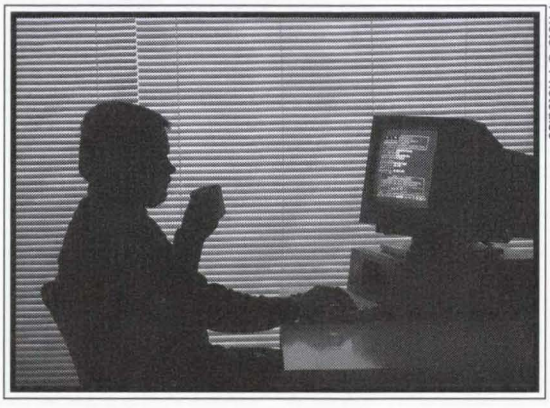


Photo © Photodisc

Theft

Not surprisingly, the fastest growing computer-related crime was theft. However, an interesting facet of this crime supports Toffler's forecast—the most commonly stolen commodity was information. Respondents reported that thieves most frequently targeted intellectual property, which includes such things as new product plans, new product descriptions, research, marketing plans, prospective customer lists, and similar information.

To illustrate one method of information theft, an information security specialist tried an experiment. A major corporate research laboratory used the Internet to search for information on new product plans. In a test of the system, a security specialist illegally accessed the Internet communications of two researchers and recorded their search inquiries and the Internet Uniform Resource Locator (URL) addresses they visited. The specialist then gave the key word search inquiries and URLs to an independent researcher in the same field, who immediately hypothesized the type of product the company was working on and the new dimension of the product under development. When informed of the results, the laboratory researchers confirmed the hypotheses. While this was a security experiment, it illustrates how computer crime can occur.

Our study found a significant relationship between personal use of company computers and increases in intellectual property theft. Personal use of computers ranged from simple word processing to use of spread sheets for personal finances to accessing the Internet. In many cases, employers either permitted or, more typically, overlooked these uses. Perhaps when employees have workstations where they perform personal activities, they begin to view the space as being their own. Consequently, the theft—particularly of intellectual property that has no tangible value—is not as readily perceived as being wrong, thereby making it psychologically easier to commit. In general, victims discovered thefts either by an audit trail showing access to information for which the user had no legitimate

need, by an informant who told the business of the theft, or by external information, such as the actions or products of a competitor, that indicated theft.

A wide body of research shows the value of stolen trade secrets and intellectual property.[9] Historically, thieves obtained such property by compromising employees, photocopying documents, committing burglary, or conducting surveillance of company personnel and practices. Increasingly, however, thieves prefer stealing from computers because it provides more extensive access to more usable information, is easier and more reliable than other methods, and presents less risk of detection and capture.

Our research also revealed a significant relationship between personal use of company computers and employees stealing or attempting to steal money. In most cases, businesses identified employees who tried to steal money before sustaining a loss. It was easier to account for monetary losses, which required some type of electronic transaction, than for intellectual property losses, which simply required copying files. Moreover, businesses placed more security controls on monetary files and monitored them more closely than information files. In addition, businesses generally had fewer monetary files than information files, making cash accounting easier to monitor.

Despite these safeguards, monetary thefts have occurred. In Detroit, Michigan, a small-time computer cracker penetrated a bank's computer system, opened a new account, and methodically transferred small amounts of money into it from existing accounts. The small thefts totaled about $50,000 before being noticed.[10] One of our survey respondents summarized the issue succinctly, "Losses are sometimes very large. We just lost $1 million."

Unauthorized Access to Files

The term "browsing" refers to the practice of obtaining unauthorized access to files just to see what they contain, somewhat akin to a criminal trespass. It is sometimes difficult to ascertain whether a law was broken, a company policy violated, an ethical standard breached, or the behavior simply stemmed from poor judgment. Browsing truly can cover this continuum, depending largely on security controls, customary practices within an organization, and corporate policy governing access to information.

> ***"...computer crime is sometimes difficult for police officials to comprehend and to accept as a major problem...."***

One security professional indicated that most cases of browsing in his company were simply curiosity or "cybervoyeurism" with no malicious intent. He even believed that most hackers were interested in the challenge of breaking into a computer system rather than in committing a theft. Despite the experiences of this individual, our research indicated otherwise.

There were significant relationships between browsing by full- and part-time employees and their attempts to steal both intellectual property and money. While not as strong overall, a significant relationship between browsing and the theft of intellectual property, but not money, also existed. With the growth of networking, a similar analysis in the next two years or so might find different results.

In the case of stealing intellectual property, browsing apparently served as a means to identify the nature of available information, its potential value, and the ability to steal the data. In the case of money, browsers most likely sought to learn the computer system's file structure, determine transaction protocols, locate accounts most susceptible to theft with a lower probability of discovery, and test security for access control and authentication roadblocks. Clearly in both cases, browsing was a significant precursor to criminality.

Traditional wisdom suggests that browsers are more of a nuisance than a threat. However, the data suggest that browsing is an exploratory activity that leads to theft or attempted theft in a significant number of instances. Organizational policy, employee supervision, and security measures should be reviewed to detect and resolve browsing activities.

Virus Introduction

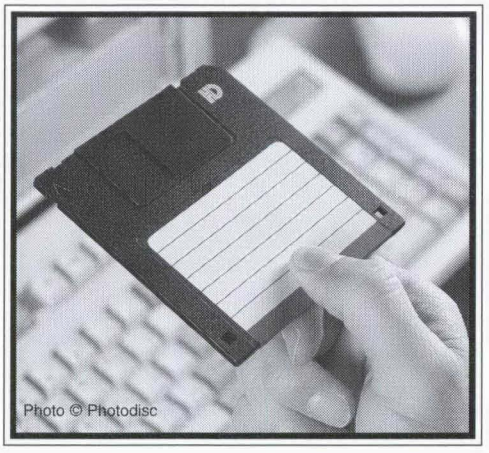
Computer viruses, created for a variety of reasons, can have many different effects, depending on the creator's intent. To illustrate,

several new insidious viruses have been found.

- "Gingrich" randomly converts word processing files into legalese often found in contracts. Victims can combat this virus by typing their names at the bottom of infected files, thereby signing them, as if signing a contract.
- "Clipper" scrambles all the data on a hard drive, rendering it useless.
- "Lecture" deliberately formats the hard drive, destroying all data, then scolds the user for not catching it.
- "Clinton" is designed to infect programs, but it eradicates itself when it cannot decide which program to infect.
- "SPA" examines programs on the hard disk to determine whether they are properly licensed. If the virus detects illegally copied software, it seizes the computer's modem, automatically dials 911, and asks for help.

For those malcontent computer users who seek ready-made viruses, a bulletin board service in France, accessible via the Internet, has a large collection of diverse viruses that can be downloaded and then introduced into a targeted computer. Certainly, the capacity to infect a computer is available, and infections are occurring on an increasing, although not epidemic, basis.

Sixty-six percent of the responding businesses reported viruses had been introduced into their computers over the past 5 years. When tested, the data show significant relationships between virus introduction by crackers who stole (or attempted to steal) both intellectual property and money.



Anecdotal evidence supports this finding, suggesting that crackers would try to destroy any evidence of their presence and their crime and make it harder to detect and investigate a theft or intrusion by introducing a virus. Essentially, the criminals intend the virus to provide a smoke screen for their invasion of the computer.

These findings strongly suggest that in a significant number of cases where computer thefts occur, viruses are introduced. The caveat to investigators is to look for evidence of thefts whenever a virus is introduced via network or modem access.

In addition, part-time employees often covered their theft or attempted theft by introducing a virus into the targeted computer, following the same rationale as for crackers. Interestingly, there was no significant relationship between virus introduction and any behavior by full-time employees, although anecdotal evidence suggests that employees have placed viruses in computer systems for a number of reasons.

According to the National Computer Security Association, the massive terminations and layoffs afflicting the corporate landscape provide an important explanation for the increase in computer viruses. A growing number of employees, believing they have been coldly dismissed after years of loyalty, see inserting a virus into the corporate computer system as a way of striking back.

Notably, to fend off the threat posed by viruses, nearly 83 percent of the respondents reported that anti-virus software had been loaded on company computers. Given that this software is easy to use and relatively inexpensive in comparison with the damage a virus could cause, it is somewhat surprising that all companies do not use virus protection.

While not directly comparable, it appears that the portion of respondents who do not have anti-viral software approximately equals the number who have no Internet connections or external modem access. Presumably, security personnel in these companies have concluded that a virus threat does not exist because the computer has no external connectivity. If so, the researchers emphasize that full-time employees also pose computer security risks. They obviously could—and have—introduced viruses.

Employees might introduce viruses for a variety of reasons, including harassing other employees, seeking retribution, playing with the system (gamesmanship), impeding

commerce, and hiding evidence of thefts. While our study did not measure reasons empirically, interviews and anecdotes shed light on these motivations.

Harassment of other employees, particularly with respect to "company politics," serves as one reason for viruses. If a fellow employee can cause problems to others, particularly in a company where one's success is measured competitively against other employees, then a virus can be a good tool to gain an advantage.

In other cases, employees seek retribution. Those who believe they have been treated unfairly, terminated without just reason, or unappreciated might seek revenge. Introducing a computer virus might fulfill the need for revenge because it can cause significant damage to the company with little chance of the perpetrator's getting caught.

Some employees could be motivated to infect a computer with a virus simply for purposes of gamesmanship. In these cases, the employees typically introduce a virus to play with the system without intending to cause permanent damage, as in the case of the "Clinton" virus. Despite this lack of malice, these employees still inflict some financial loss on the targeted businesses due to lower productivity while the virus is present and the cost of eradicating the problem. Moreover, there could be accidental damage caused by the virus itself or by attempts to remove it.

Another reason for infecting a computer is to impede the commerce of a business. Whether introduced by a cracker working at the behest of a competitor or an employee who has "sold out," a virus intended to impede commerce typically will cause major damage, such as erasing files, mixing information so that it makes no sense, or locking up hardware so that the system's software must be reloaded. In addition to the effects of the virus on the computer system, businesses sustain significant losses from secondary effects: the costs of virus eradication and system repair, operational slowdowns—or even stoppages—while the problem is being resolved, and undetermined losses of market share that might occur as a result of the problem.

> ***"Money and intellectual property have been stolen, corporate operations impeded, and jobs lost as a result of computer crime."***

A final reason for employees to infect computers is to hide evidence of thefts. If a virus erases information, disrupts audit trails, or jumbles information, then losses—even if detected—might be attributed to the virus, not a theft.

As shown, computer viruses can be obtained readily and introduced by employees and crackers alike. Policy makers should take the logical security precautions, anticipating the possibility of viral infection of computer systems. As network connections among computer systems proliferate, the potential for problems will only increase.

Security Countermeasures

In light of these computer crime threats, we asked the respondents about their practices and experiences with a variety of security countermeasures. These included encryption, operations security, cash accounts security, employee training, and firewalls.

Encryption

The analysis shows a significant relationship between file or data encryption and reduced theft of intellectual property. Encryption, therefore, should be considered an important tool for protecting confidential information.

However, encryption tools should be reviewed and changed periodically. Breaches of such systems not only have occurred but also have become somewhat of a game. For example, RSA-129 is a 129-digit number created in 1977 by the developers of an encryption system said to be "provably secure." The creators of the code estimated that it would take 40 quadrillion years to factor the number using the methods available in the late 1970s.

The code's creators recognized that rapidly evolving technology would increase analytic capacities dramatically over the coming years and, in light of this, predicted that the code would remain secure well into the next century. In 1994, a mere 17 years later, a group of 600 Internet volunteers cracked the code.[11] Evidently, technology is challenging traditional assumptions,

including the assumption of long-term security via encryption.

Operations Security

Our study also found that increased operations security led to decreased theft of intellectual property. Operations security includes such measures as monitoring users, creating audit trails of system users, and conducting physical surveillance of users and systems. Physical surveillance, in particular, brought down the incidence of intellectual property theft; however, it also caused an operational problem.

Anecdotal evidence suggests that when security surveillance of computer users increases, employee morale deteriorates, job satisfaction lessens, and employee productivity decreases. It might be difficult to balance the need to use surveillance to reduce intellectual property theft against the potential negative effects of such heightened scrutiny. In all likelihood, the decision will have to be made on a case-by-case basis following an evaluation of the organizational culture and a risk/benefit analysis.

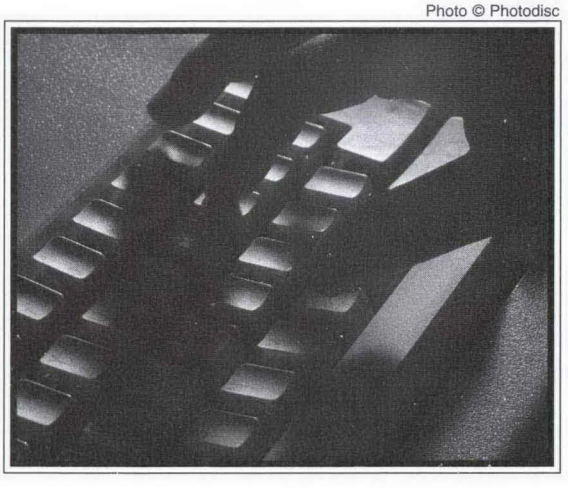
Protecting money, according to the respondents, poses different problems. While the value of intellectual property is difficult to assess, it can be protected more easily through encryption. However, encryption has unique limitations, and computerized cash accounts require different types of operations security.

Cash Accounts Security

The threat of monetary loss is real. In 1994, a Russian cracker unlawfully accessed Citicorp's computers, transferred approximately $40 million, and withdrew some $400,000.[12] Our study found a number of measures required to secure cash accounts, including changing passwords regularly, using numerical access control systems, upgrading authentication software, monitoring employees, maintaining audit trails, and regularly reviewing cash accounts for small losses.

On this last point, we learned that small account balance errors in computer files serve as good indicators that someone has tampered with the accounts. In a rush to commit the crime, the perpetrator is more likely to make small—rather than large—errors and miss them.

Photo © Photodisc



Employee Training

Across the board, increased employee training consistently helped minimize theft. Respondents reported that employee training diminished crimes and computer abuse, such as harassment via e-mail and personal use of business computer systems.

Firewalls

Finally, we tested the use of firewalls as a countermeasure. While different approaches exist, as a rule, firewalls are software controls that permit system access only to users specifically registered with a computer. As users attempt to gain access to the system, they are challenged to ensure they have an authentic password. Typically, users encounter several challenges, known as layers, for added protection.

Although respondents reported widespread use of firewalls, the data showed no significant relationship between this countermeasure and protection of information. Indeed, several respondents' comments suggested that crackers had penetrated their firewalls. A number of security professionals have reported discovering "Password Sniffer" and "Password Breaker" programs downloaded from the Internet by crackers to breach security.

Our study did not examine the sophistication or level of security provided by these firewalls, thus the finding of no significance could be a function of security practice rather than actual effectiveness of the countermeasure. Typically, firewalls are developed to defend against known incursion methods. However, computer criminals are creative and clearly have demonstrated their ability to penetrate many firewall systems. Moreover, when security professionals develop new barriers, crackers approach them like a puzzle, rather than an obstacle.

Essentially, a firewall acts as a sophisticated electronic dam. Unfortunately, once an intruder finds a passage around this barrier, access to critical information becomes much easier.

Some evidence suggests that when systems have firewalls to protect against external intruders, system operators place less emphasis on internal security control, thus exposing the system to abuse by insiders and, once the firewalls have been breached, outsiders alike. To provide effective information system security requires a more holistic, proactive vision supported by the underlying assumption that any countermeasure can be compromised.

CONCLUSION AND RECOMMENDATIONS

As the research shows, computer crime poses a real threat. Those who believe otherwise simply have not been awakened by the massive losses and setbacks experienced by companies worldwide.

Money and intellectual property have been stolen, corporate operations impeded, and jobs lost as a result of computer crime. Similarly, information systems in government and business alike have been compromised, and only luck has prevented more damage from occurring.

The economic impact of computer crime is staggering. British Banking Association representatives estimate the global loss to computer fraud alone as approximately $8 billion each year. To add other losses as previously described brings the total economic effects of computer crime to a level beyond comprehension. As new technologies emerge and another generation of people becomes not only computer literate but also network literate, the problems will multiply.

Researchers must explore the problems in greater detail to learn the origins, methods, and motivations of this growing criminal group. Decision makers in business, government, and law enforcement must react to this emerging body of knowledge. They must develop policies, methods, and regulations to detect incursions, investigate and prosecute the perpetrators, and prevent future crimes. Institutions already have fallen behind the criminals; at this point, the question is not whether they can catch up but whether they can keep the gap from widening.

> ***"The economic impact of computer crime is staggering."***

Just as law enforcement agencies have developed specialized criminal investigative units and prevention programs for crimes of violence and drug abuse, they must initiate similar programs for computer crime. In addition, police departments immediately should take steps to protect their own information systems from intrusions.

Computer crime is a multibillion dollar problem. Technological changes will enable more perpetrators to ply their trade from remote locations. Police managers must plan for this reality and devote resources to deal with the computer crime problem.

Computers have ushered in a new age filled with the potential for good. Unfortunately, the computer age also has ushered in new types of crime for the police to address. Law enforcement must seek ways to keep the drawbacks from overshadowing the great promise of the computer age. ✦

Endnotes

[1] A. Toffler, *PowerShift* (New York: Bantam Books, 1990).

[2] R. Heffernan, Securing Proprietary Information Committee of the American Society of Industrial Security, Committee Presentation at the ASIS Annual Meeting, New Orleans, LA, September 12, 1995.

[3] U.N. Commission on Crime and Criminal Justice, *United Nations Manual on the Prevention and Control of Computer-related Crime* (New York: United Nations, 1995).

[4] Florida Department of Law Enforcement, *Computer Crime in Florida*, unpublished report, Tallahassee, Florida, 1989.

[5] Supra note 3.

[6] This term, which refers to people who break into computer systems without authorization, is preferred to "hackers," which signifies people skilled in writing and manipulating computer code.

[7] Supra note 3.

[8] Supra note 2.

[9] See, for example, supra note 2; B. Tripp, *Survey of the Counterintelligence Needs of Private Industry* (Washington, DC: National Counterintelligence Center and the U.S. Department of State Overseas Security Advisory Council, 1995); and U.S. Congress, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* (Washington, DC: U.S. Government Printing Office, 1995).

[10] "Computer Used to Steal Cash," *Lansing State Journal*, February 5, 1995, 4B.

[11] J. Rosener, *Cyberlaw* (America Online) April, 1994.

[12] J. Rosener, *CyberLaw* (America Online), October, 1995.

Book Review

Understanding Today's Police *by Mark L. Dantzker, Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1995.*

Policing in today's society involves a host of complexities never experienced, even in the recent past. Understanding and articulating these complexities can, at times, prove to be an overwhelming task. Many law enforcement text books that adequately discuss the theoretical aspects of the job fail to shed light on coping with these complexities by applying those theories to everyday policing.

Understanding Today's Police goes beyond theory and offers readers thought-provoking and realistic examples of everyday police work. Throughout the text, the author presents a wide variety of "case in point" discussions depicting examples of real life situations that have occurred in policing, which help illustrate more conceptual points made in the text.

The book begins with an overview of the role of law enforcement in society. This introduction provides the foundation for the remainder of the text by summarizing the various roles of the police and by providing readers with a brief history of American policing. However, as the author makes clear, this historical perspective serves only as a backdrop to the main focus of the text—an in-depth examination of the roles and functions of today's police and the challenges that will face the police of tomorrow.

To encourage readers to think critically about the different components of the discussion, the author includes a "Do You Know" section after each chapter. The questions posed in each of these sections challenge readers to go beyond a surface understanding of the points discussed in the preceding chapter. Many of the questions invite readers to think in terms of how the issues discussed might affect their local agencies.

The author also uses a systems approach to discuss policing. He examines policing from a federal, state, and local perspective. The reader then can dissect and explore components of the criminal justice system at each of these levels.

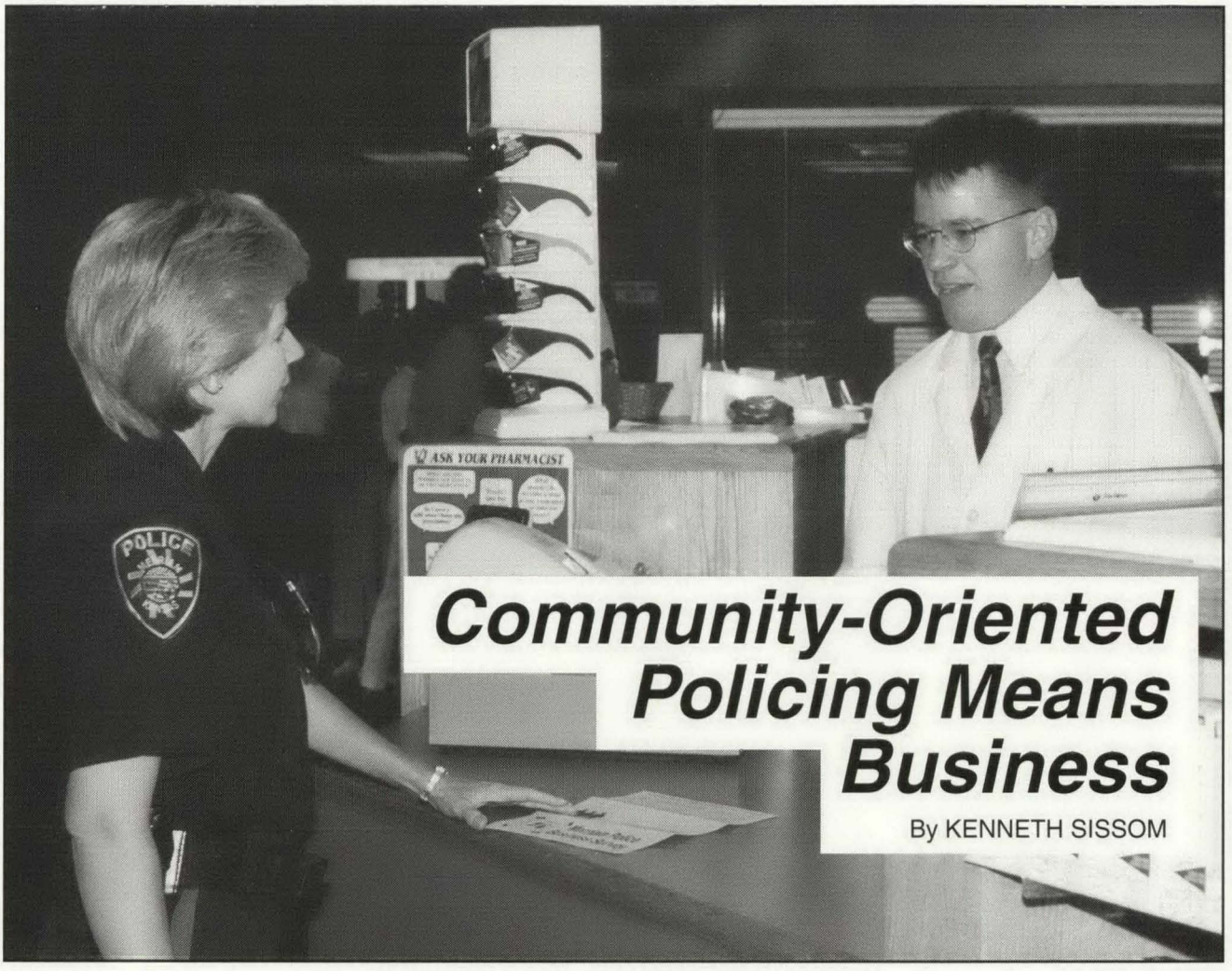
The text goes on to provide a broad examination of the various areas of policing, including patrol, criminal investigations, organization and management, police and the law, police discretion, police personalities, personnel issues, and police-community relations. Throughout the discussion of these issues, the author underscores the relationship of the police to other sectors of the criminal justice system.

In the final chapter, the author discusses issues that affect policing today and explores influences that likely will impact it in the future. The discussion encourages readers to ask critical questions about the future role of policing in society. The chapter concludes with a brief essay on the criteria the author considers necessary to enhance the professional status of policing.

Throughout the text, the author provides an overview of the police research relevant to the topics under discussion. Each chapter concludes with a list of additional resources to which readers can refer to enhance their knowledge of particular topics.

Understanding Today's Police provides a rich learning experience for students and newly sworn law enforcement officers. In addition, the book offers valuable insights for veteran officers wishing to update their knowledge and understanding of the profession. This well-written book provides a comprehensive review of policing today and examines critical issues that will impact it in the future.

Reviewed by
Sgt. Michael L. Birzer, M.A.
Sedgwick County Sheriff's Department
Wichita, Kansas



Community-Oriented Policing Means Business

By KENNETH SISSOM

Police departments across the country profess the value of community-oriented policing. Implementing this popular philosophy requires establishing a closer relationship with citizens. Still, the success and effectiveness of any police department's community policing efforts also depend on maintaining a good working relationship with members of the business community.

Traditionally, police officers make two types of routine contacts with businesses: summoned police responses and visits to popular establishments. Summoned police responses represent the most common type. For example, thieves break into a local business, causing the owner to summon the police. Responding officers take a report, investigate the scene, and leave. Although this typically marks the end of the association, in certain retail businesses, a stronger, more established relationship develops. This occurs when the frequency of contacts escalates due to increased robberies, shoplifting, or disturbances.

The second most common police-business contacts are more personal than professional in nature. Every city has its share of businesses that patrol officers visit regularly, such as convenience stores, restaurants, and—the target of tasteless jokes about the police—doughnut shops. While these visits may improve relations between the department and the business community, these businesses represent only a small portion of the total number of establishments in any city.

What about the other businesses in the city? What type of relationship exists between the department

and those businesses that have very little contact with the police? With its Business Survey Project, the Merriam, Kansas, Police Department set out to answer these questions.

THE BUSINESS SURVEY PROJECT

The police department in Merriam, a suburban city of 12,000 in the Kansas City metropolitan area, implemented community-oriented policing in 1992. Department managers decided to concentrate first on the business community, after meetings with the city administrator and the mayor revealed that several of Merriam's nearly 600 business owners had voiced a desire for more positive contact with the police.

In the months that followed, the department developed a method that would compel line officers to make planned, official contacts with all city businesses. In doing so, officers would provide shopkeepers with information about the department, as well as solicit feedback in an effort to determine how they viewed the department and how the police could serve them better.

Phase One: Identification of All City Businesses

To ensure that the project included all local businesses, the department retrieved a computerized listing of licensed businesses from the city clerk's office. Using computer-generated labels, the chief placed the name and address of each business on the back of a 3-by-5 index card. Then, officers used these cards to record their contacts with business owners or managers.

Phase Two: The Survey Tool

During this phase, the chief developed a mail-in survey form using a standard desktop publishing program and a personal computer. The department printed its address on the tri-fold form to facilitate responses. This design allowed business owners to complete the form, then fold it, seal it, and mail it.

The survey form first gave brief information about the police department, including its address, phone numbers, and contact persons. It described, in lay person's terms, the department's community-oriented policing philosophy and its relevance to the business community.

Then, a series of questions followed. The department designed questions that would be easy for business owners to answer. The first asked respondents to provide an overall rating (excellent, above average, average, below average, or poor) for the service that they had received from the department.

The second asked respondents to identify their biggest concern with regard to crime. Merriam's experience has been that business owners' perceptions of crime-related problems often differ from those of the police. For example, while the police may believe that business owners worry most about burglary or robbery, in reality, they may list abandoned cars or loitering juveniles as their primary concerns. Clearly, knowing business owners' true concerns results in a more accurate and appropriate police response.

The third question requested suggestions for ways to improve the department's level of service. The next, a four-part question, focused on any direct contact the businesses had with the police in the previous 12 months.

> ***"...officers believed that they were making a greater difference in the business community, rather than merely responding to calls for service."***

Chief Sissom heads the Merriam, Kansas, Police Department.

After inquiring about the reason for any contacts, the survey asked if the responding officers had been courteous and helpful and what the officers could have done to improve their performance. Finally, the survey acquainted businesses with the crime prevention analysis services the department provides and asked if they would like the department's crime prevention officer to conduct an analysis of their business.

Phase Three: Education and Implementation

This phase of the project focused mainly on training first-line supervisors, although all officers received instruction on the department's community-oriented policing philosophy and the workings of the survey. As with most new projects, the support of shift supervisors would help ensure the success of this program. Furthermore, the chief made it clear that first-line supervisors would share in the successes of the officers on their shifts. At the onset of the survey, supervisors received a written, detailed explanation of the project, including how it related to community-oriented policing.

The department placed more emphasis on the day shift, because more business owners and managers were available during this time, and because the day shift could accommodate the additional work more readily. As a result, day shift officers were tasked with contacting three businesses per shift, every workday. The day shift supervisor's goal was one business per shift.

Officers on the evening shift needed to make one or two contacts, depending on police activity. Their supervisors did not have a set goal, but were encouraged to check a business when time permitted. Officers on the midnight shift, although omitted from the project, were required to make frequent routine contacts with those businesses open during their shift.

Supervisors reduced the goals of individual officers once the majority of community businesses had been contacted. At the end of the year, the department recognized the officer with the greatest number of contacts.

> "...first-line supervisors would share in the successes of the officers on their shifts."

In sum, each regular district officer, working Monday through Friday on the day and evening shifts, chose businesses to contact during their shift, retrieving the businesses' index cards from a file box in the squad room. The officers made contact with the business owners or managers and introduced themselves. They explained the department's philosophy of community-oriented policing and the nature of the project. This served a two-fold purpose. It required that the officers gain a reasonable understanding of community-oriented policing, and it educated the public about the benefits of this philosophy.

During the contacts, officers inquired about the business owners' problems or concerns. At the end of the meeting, the officer left a business card and a survey, asking the owner to complete the survey and mail it back to the department.[1]

Officers also completed the front of the index card with their name, shift, the date of the contact, the contact person, the business' fax number, and the business type. At shift's end, officers returned the index cards—whether completed or not—to the file box. This system gave officers credit for their contacts, while preventing duplication of visits.

Phase Four: Public Relations Considerations

Before implementing any program that might impact public relations either positively or negatively, police leaders should seek political support. From the start, the chief realized that business owners might contact city officials immediately, so he met with the mayor and the city administrator to gain their support. Both officials expressed gratitude for being informed in advance so that they could prepare a response to questions or comments that local business leaders might have.

In Merriam, an active chamber of commerce has long been an excellent forum for police personnel to meet with leaders of the business community. The police chief regularly attends the chamber's monthly meetings. After meeting with the chief to discuss the survey project, the director of the chamber of commerce featured the program in an article in its monthly newsletter. Later that year, the chief gave a

short presentation about the project at a chamber meeting.

Finally, the media can make or break a police program. In this case, the media provided positive public relations for the project. During the first month, the local newspapers ran features about the project. A local television station sent a reporter and camera person to follow a department officer while contacting local businesses.

Phase Five: Project Followup

When initiating a new program, department managers must incorporate steps to ensure its proper implementation. By conducting followup measures, department administrators communicate a strong message to line officers that their actions during this important project will be monitored.

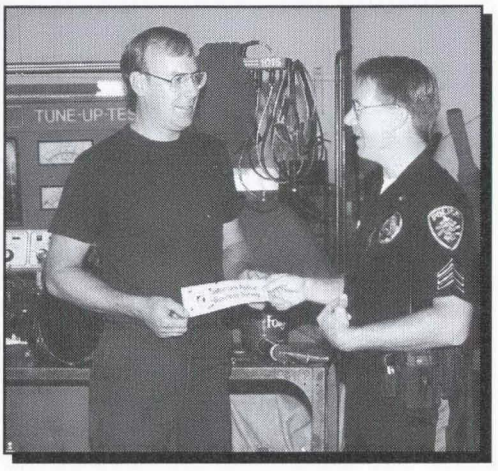
Each month, Merriam department managers audited the business contact file in the squad room. As officers completed cards on the businesses they had contacted, it became clear which officers did not make regular contacts. Supervisors met with these officers to encourage them to get more involved. After a few monthly audits, most problems disappeared.

Phase Six: Compiling and Processing Returned Surveys

From January to December of 1993, officers of the Merriam Police Department contacted 534 businesses. Thirty-three percent of these businesses completed a survey.

The chief personally reviewed every completed survey. If a business owner rated the department below average or reported a past negative experience with the police, the chief immediately contacted the owner to resolve the problem.

On the survey, business owners listed their biggest crime concerns as robbery, burglary, theft, vandalism, and loitering. Shift supervisors received this information and responded with changes in routine patrol techniques. For example, although some businesses listed robbery as a primary concern, department records indicated that only a few actually had fallen victim to robbers.



This finding identified the real problem as one of perception and fear, not one based on the business' history of robbery. After this discovery, officers targeted these businesses for frequent walk-in checks; soon, business owners reported feeling more confident in the police, and as a result, less fearful.

Some businesses voiced concern over traffic problems. Traffic officers handled any obvious problem. In cases where business owners only perceived a problem, department officers studied the situation and reported the results to the owners. This approach changed their perception.

Each business that took the time to complete and mail in a survey received a personal thank you letter from the chief. The crime prevention officer contacted each business that requested a crime prevention analysis, 81 in all. This officer also compiled survey responses, which administrative personnel studied in January 1994.

Results

The survey results revealed that, overall, the Merriam business community had a very favorable opinion of its police department. Forty-eight percent of respondents rated the department excellent; 37 percent, above average; 7 percent, average; and 2 percent, below average. Six percent of the businesses did not provide a rating.

Although respondents' answers most likely were influenced by the positive publicity the survey generated, the department still achieved its goal: to improve basic relations between the police and the business community by opening a line of communication. The survey became a tool to do just that. This enhanced relationship fostered an environment of cooperation that built upon the community-oriented policing philosophy.

As an added bonus, the officers involved in the project also discovered its value. Faced with the survey results, they changed their initial perception that business owners considered the police a hindrance instead of a help. In addition, officers

believed that they were making a greater difference in the business community, rather than merely responding to calls for service. Indeed, their efficiency at routine patrol had increased with the new flow of information about criminal or suspicious activity now coming from their new business contacts.

FUTURE PLANS

The Merriam Police Department currently is conducting its second Business Survey Project. Results so far show not only a greater rate of return for the surveys but also higher ratings for the department. In the future, the department will conduct biennial business surveys, focusing on neighborhood programs in intervening years.

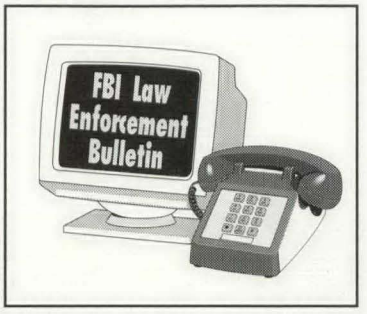
CONCLUSION

While this project was completed in a small suburban city, the concept can work in any community, large or small. As police departments institute community policing in their jurisdictions, many focus almost exclusively on programs aimed at residents. But, just as increased contact with citizens enhances the ability of a department to fulfill its mission, so too does a positive relationship with business owners. With its Business Survey Project, the Merriam Police Department proved that community policing also means business. ✦

Endnote

Some departments may want to pay for postage to save the business the expense and to encourage a greater return. Due to budget constraints, the Merriam Police Department chose to let each business pay for postage.

Law Enforcement's Internet Address



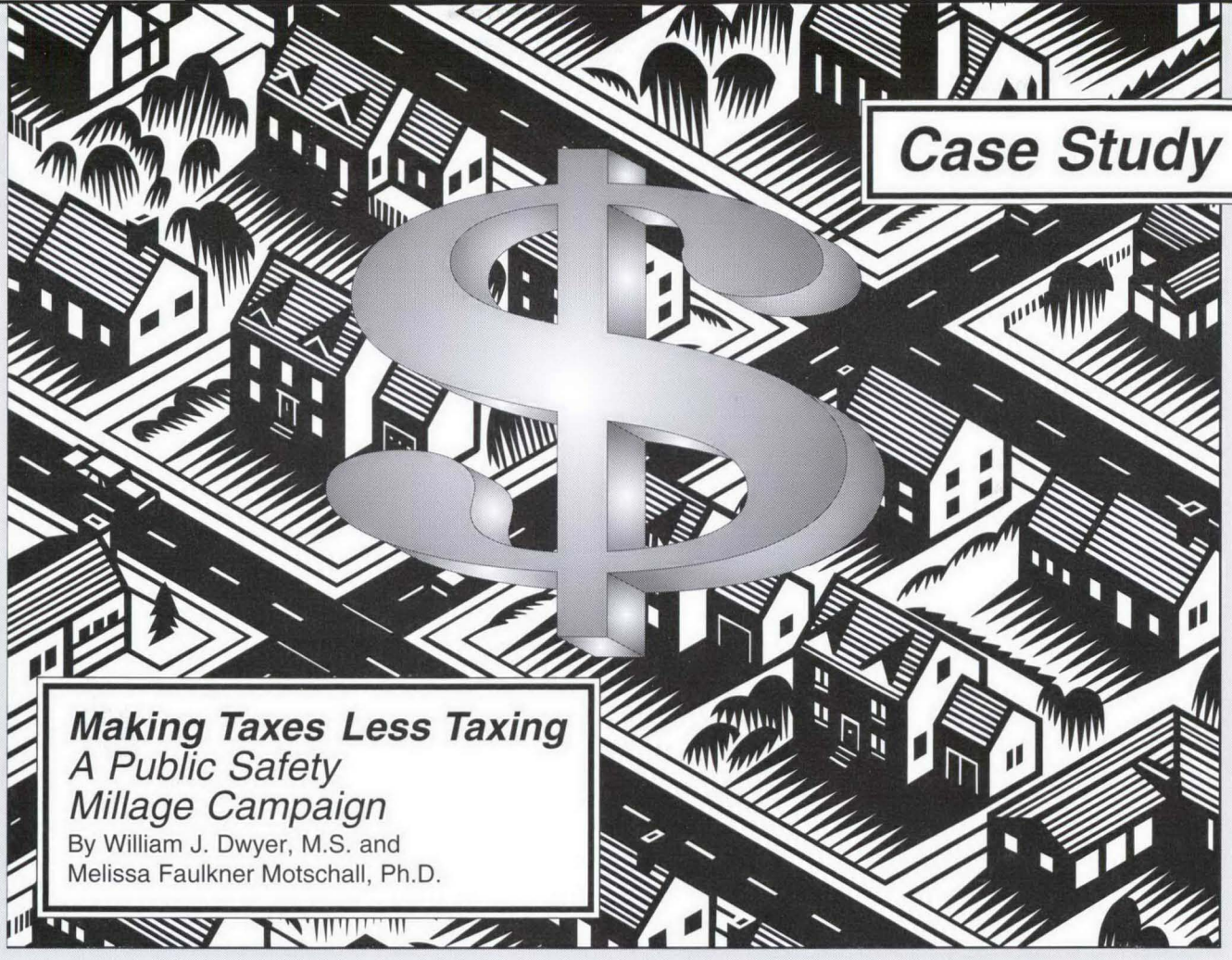
The *FBI Law Enforcement Bulletin* staff invites you to communicate with us via e-mail. Our Internet address is:

leb@fbi.gov

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

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

http://www.fbi.gov



Case Study

Making Taxes Less Taxing
A Public Safety Millage Campaign

By William J. Dwyer, M.S. and
Melissa Faulkner Motschall, Ph.D.

No new taxes. American taxpayers have heard this political battle cry before. Yet, in an era of shrinking budgets, no new taxes may mean not only no new services but also a decrease in the ones already in place.

Police and fire officials in Farmington Hills, Michigan, faced this situation and came out ahead. Together, they waged a successful campaign that secured badly needed resources, while strengthening community support for public safety. They directed their efforts to increase the tax rate, or millage,[1] applied to the assessed value of property.

BACKGROUND

Farmington Hills, a suburban community 25 miles northwest of Detroit, has a population of about 81,000. This figure represents an increase of more than 10 percent since 1990. The rapid growth in the city's population and that of surrounding communities resulted in a greater demand for public safety services. Yet, due to a lack of funding, the level of staffing, technology, and support programs for the police and fire departments remained unchanged. Police and fire officials appealed to Farmington Hills residents for additional resources to meet the increasing demands for service.

The success of the millage campaign can be attributed largely to good planning and organization. Police and fire representatives and community supporters developed a campaign strategy that included documenting the need for the initiative, placing the issue on the ballot, securing campaign funds, disseminating a consistent and credible message, and targeting and mobilizing key audiences.

DOCUMENTING THE NEED

Police and fire officials relied on a number of key documents to help pave the way for a tax increase. First, following a 1995 audit, a management consulting firm predicted that without additional resources, both the police and fire departments would be unable to serve the community effectively in the future.[2]

Worse, the consultants recommended that police and fire services be reduced if more funds were not made available.

In addition, both the police department's and the fire department's 5-year plans, which were submitted to the city council in May 1995, established the need for the millage campaign.[3] These plans reiterated the necessity for such resources as additional personnel, a computer system, and a fifth fire station to accommodate the community's substantial growth.

The reports contained charts and graphs that illustrated past, present, and projected increases in calls for service. In addition, the 5-year plans emphasized that the departments' staffing levels have remained lower than less-populated neighboring communities. Based on these statistics, officials made a strong case for additional public safety services.

> "Police and fire officials...waged a successful campaign that secured badly needed resources, while strengthening community support for public safety."

Moreover, the stated police and fire needs coincided with goals set forth in a strategic plan the city had developed in 1989. The product of a communitywide effort, the plan identified two public safety goals—adequate staffing and advanced technology—to keep pace with population growth and increases in crime.[4] Through these key documents, Farmington Hills public safety officials confirmed the need for the millage and achieved early support from public officials.

PLACING THE INITIATIVE ON THE BALLOT

The first step in undertaking any millage campaign is putting the tax measure on the ballot. To do this, police and fire officials made a presentation before the city council at a meeting in late July 1995.

City officials strongly advocated the millage increase. The mayor and city council members were well aware of the city's public safety needs, for members had reviewed the management consulting report and the 5-year plans, and many had been involved in the citywide strategic planning process. The mayor and council members approved the ballot issue; this gave campaign organizers 3 months to implement a communitywide campaign.

SECURING CAMPAIGN FUNDS

After the ballot initiative was approved, police and fire officials spearheaded the development of a special task force to develop strategy and secure funding for the campaign. Members of the Public Safety Task Force were selected from lists submitted by police and fire officials, the city and deputy city managers, and the Crime Prevention Advisory Board.

Police and fire officials estimated that they would need between $12,000 and $14,000 to cover campaign costs, such as printing presentation materials, signs, and other items. The funds could come only from private donations and in-kind contributions, such as donated printed items.

The Public Safety Task Force secured contributions from such sources as local businesses, the chamber of commerce, residents, and police and fire unions. Their successful fundraising efforts generated a $2,000 surplus, which city officials donated to local charitable organizations after the campaign.

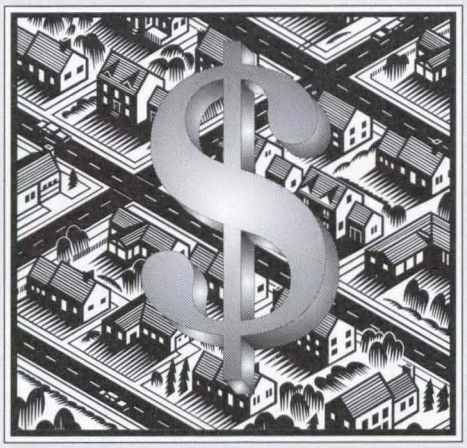
DEVELOPING STRATEGIC COMMUNICATIONS

The success of the millage campaign was due in part to the positive image of public safety services in Farmington Hills. The organizations had well-established community relations programs in the city. Relying on this network, officials developed a comprehensive communication plan for disseminating their campaign message, which emphasized the crime- and fire-fighting records of both departments.

Police and fire officials adapted their campaign message to various community groups and delivered it through a variety of communication media. Officials made approximately 10 presentations per week before such diverse groups as business owners, service

agency employees, senior citizens, resident association members, and church congregations.

Because government employees are prohibited from publicly supporting a yes-or-no vote on an issue, officials needed to present the facts as clearly and as effectively as possible. They hoped that by stating facts, showing comparisons to other cities, and projecting future needs, they could help voters draw their own conclusions without telling them how to vote.



To accomplish this, officials used several methods. A four-page fact sheet emphasized that staffing levels and equipment resources had not kept pace with the city's increases in population and subsequent rises in demands for emergency response. An accompanying slide presentation featured simple, but effective, color charts, graphs, and other visuals. Because child abuse and domestic violence concerns hit close to home for many people, officials included pie charts that depicted the time required to investigate these cases and emphasized the importance of having sufficient resources to do so.

The local city newsletter, "Focus," published a front-page article 1 month before the election that contained the same information as the fact sheet and presentation materials. The companion photograph featured a smiling police officer exchanging a high-five with a toddler.

In addition to printed materials, police and fire officials used the broadcast medium to disseminate their campaign message. They produced three different videos that ran on local cable television shows, such as "Police Journal," which airs 2 days a week.

The videos included dramatic footage of police and fire department personnel answering calls for service. Dispatchers, patrol officers, and investigators made heartfelt requests for much-needed funds. One video contained statements from city officials—including the police and fire chiefs in full uniform—and the chairperson of the Public Safety Task Force. One month before the election, officials stepped up the campaign video broadcast times to every night until Election Day.

TARGETING KEY AUDIENCES

Another important aspect of the millage campaign was the interaction with key audiences—before and during the campaign. The ongoing relationships that police and fire officials had developed with various constituents before the campaign proved instrumental in securing support for the millage. These individuals included public employees and members of the media and community groups.

Police and Fire Employees

In addition to targeting external groups, officials marshalled the support of their employees. Because state laws prohibit public employees from campaigning on ballot issues during work hours, these dedicated men and women volunteered their own time to work on the campaign. The police and fire unions also endorsed and made financial contributions to the millage campaign.

Media

Police and fire officials met with editorial staff members of the local newspaper to inform them of the departments' plans to undertake the campaign. After the meeting, a newspaper editorial proclaimed, "Simply put: It's necessary."[5] This endorsement came a full 6 weeks before Election Day.

Community Groups

Police and fire officials knew that they would need the support of groups that represented key sectors in the community. Accordingly, officials made presentations to educators, residents, and business people to secure their endorsements for the millage.

The Citizen's Crime Prevention Advisory Board—composed of business, educational, religious, and neighborhood organizations—also was consulted early in the campaign. Police, in particular, have a positive

working relationship with the group. The activities of the advisory board include meeting regularly with public officials to discuss concerns and to recommend crime prevention programs. As a result, members already were aware of the need for increased public safety services, and they were committed to assisting with the campaign.

After securing the support of key advocacy groups, police and fire officials began to target audiences who they knew would not readily support the millage. The most difficult of these groups was senior citizens. Officials knew that seniors, most of whom live on a fixed income, would be especially hard to convince of the benefits of a tax increase. Fortunately, police representatives had developed positive relationships with seniors through such programs as Police and Seniors Together,[6] in which police employees provide companionship to lonely seniors.

> "...officials and campaign spokespersons skillfully organized a network of community supporters who endorsed the tax increase."

In addition, during the campaign, officials met personally with several senior citizen groups and emphasized two points. First, the additional tax would be levied once a year for only 10 years. Second, the increased police and fire services would reduce response times. This was a particularly convincing argument for seniors, who are among the most frequent users of emergency medical services.

TALLYING THE VOTES

On Election Day, Farmington Hills police and fire representatives achieved their goal. Nearly 66 percent of the voters passed the one mill tax increase to upgrade the city's police and fire services. The city will use the money to hire additional police and fire employees, upgrade its 911 communication system, increase crime analysis and institute appropriate crime prevention programs, and build a centrally located fire station to be staffed around the clock.

CONCLUSION

The groundswell of support Farmington Hills officials garnered for the millage increase was the culmination of a strategy that began long before the issue came to a vote. Building on a foundation of close relationships with community groups, officials and campaign spokespersons skillfully organized a network of community supporters who endorsed the tax increase. Communication tools, such as fact sheets and videos, effectively conveyed the need for and the benefits of the tax increase to seniors, business owners, and other key voters.

By Election Day, the question on voters' minds was not whether they would support a millage increase; rather, they wondered why officials had not asked for more. In communities nationwide, citizens often clamor for improved services but vote against tax increases to pay for them. Police and fire officials in Farmington Hills, however, have shown that the millage campaign can serve as a viable funding alternative and a tool for building even stronger community relations. ✦

Endnotes

[1] A one mill increase generates an additional dollar of revenue for each thousand dollars of taxable property. In Farmington Hills, the tax applied to both commercial and residential real estate.

[2] Bennett Associates, "City of Farmington Hills, Michigan, Management Audit," January 1995, 34.

[3] "Farmington Hills Police Department Five-Year Plan: 1995-1999," Farmington Hills Police Department, Farmington Hills, Michigan; "Farmington Hills Fire Department Five Year Plan: 1995-1999," Farmington Hills Fire Department, Farmington Hills, Michigan.

[4] "Traditions, Progress, and the Year 2000 Forecast," City of Farmington Hills, Michigan, 1989.

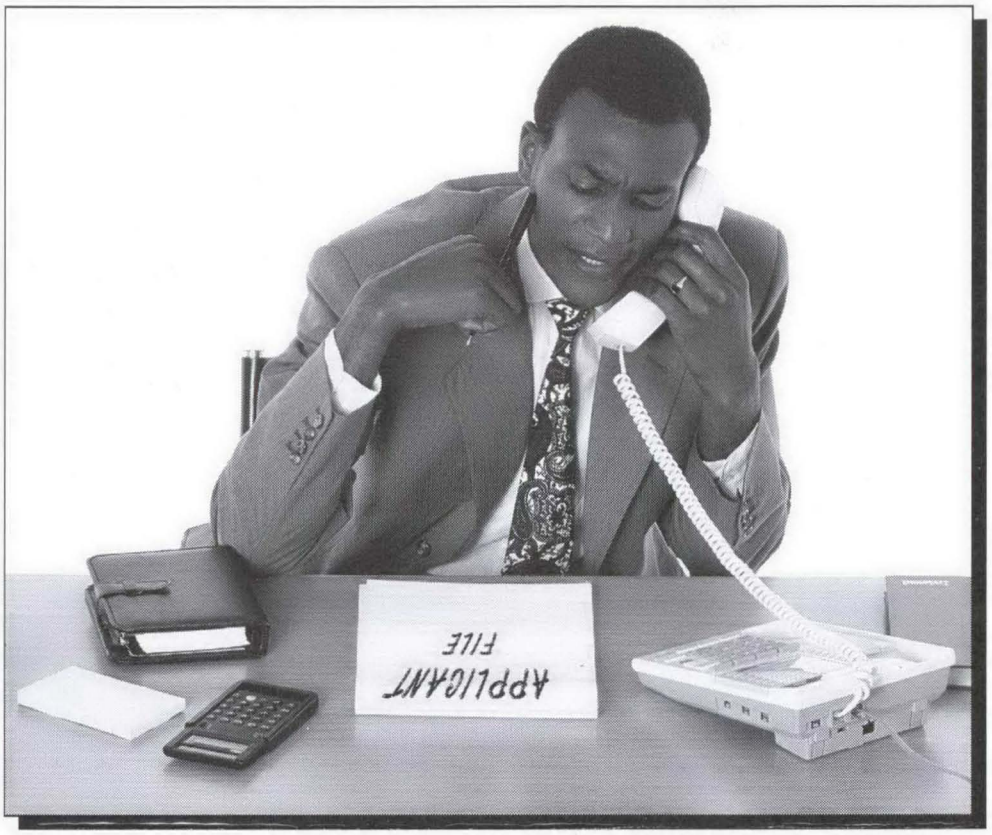
[5] "For Safety's Sake: Hills Tax Increase Is Justified," *Farmington Observer*, September 21, 1995, 10A.

[6] *See* William J. Dwyer, "Building Bridges: Police and Seniors Together," *FBI Law Enforcement Bulletin*, May 1993, 6-8.

Chief Dwyer heads the City of Farmington Hills, Michigan, Police Department. Dr. Motschall is currently an assistant professor of public relations at Eastern Michigan University in Ypsilanti, Michigan, and has served as an instructor for the Northwestern Traffic Institute School of Police Staff and Command in Evanston, Illinois.

Employment Information Release Agreements

By DANIEL J. SCHOFIELD, S.J.D.



Law enforcement organizations need to hire employees who possess the highest degree of integrity, character, and professional competence. The public expects this to be true of all law enforcement hirings, and rightfully so. However, when former employers refuse to disclose information regarding an applicant's prior employment history, it becomes more difficult for a law enforcement organization to evaluate whether an applicant meets these high standards.

Because some employers presumably base restrictive disclosure policies on an inaccurate assessment of their potential liability, this article discusses the extent to which public and private sector employers can be held liable for the disclosure of employment information. Specifically, this article examines whether an applicant's authorization to release personnel information affords immunity from defamation liability for former employers who disclose such information to a law enforcement organization.

The article begins with a brief discussion of the general principles concerning consent and immunity from defamation liability. Next, it examines two court decisions involving the use of release agreements to determine the scope of protection such agreements afford former employers who disclose

personnel information to a law enforcement organization. Finally, the article offers several recommendations regarding the contents and structure of release agreements to achieve maximum protection. A sample release agreement is provided at the end of the article.

Consent Affords Absolute Privilege from Defamation

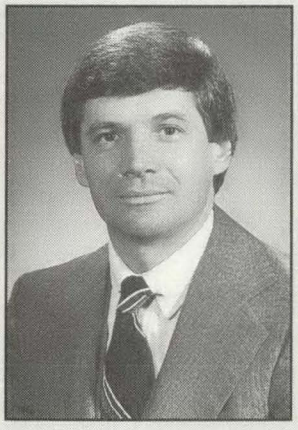
What is the legal significance of requiring an applicant for employment to sign an authorization for the release of personnel information? Does a release agreement afford former employers an absolute immunity from defamation liability for information disclosed pursuant to that agreement?

Courts generally afford employers an absolute privilege from defamation liability for disclosing employment information within the scope of a release agreement because a job applicant "...can consent to a defamation, and that consent creates an absolute bar to a defamation suit."[1] Courts and legal scholars recognize the efficacy of consent agreements and conclude that such agreements are not against public policy, even if they require job applicants to consent to an intentional tort, such as defamation.[2]

Consent creates an absolute privilege that is unaffected by a finding that a disclosure was made with malice, because an absolute privilege is intended to "...elevate the good to be accomplished by the free and open exchange of information over the harm which may result from a falsehood."[3] Moreover, an absolute privilege prevents an inquiry into a prior employer's motive or purpose in disclosing personnel information pursuant to a job applicant's consent "...since this could result in subjecting the honest person to harassing litigation and claims."[4]

For example, the U.S. Court of Appeals for the Ninth Circuit in *Cox* v. *Nasche*[5] ruled that a release form signed by an applicant for government employment afforded an absolute privilege against a defamation action, even if statements of the former employer were made maliciously.[6] Courts display a greater willingness to afford former employers absolute immunity where a person is applying for a law enforcement position for which the free flow of information may be especially important to ensure integrity and fitness for duty.

In that regard, the Supreme Court of New Mexico said a compelling reason for holding that consent creates an absolute privilege for information provided to the police is the need to ensure that only appropriate individuals with integrity and high moral character are employed in law enforcement positions.[7] Because it is essential that law enforcement organizations acquire information about the background of applicants, the court said that granting absolute immunity to employers who supply such information "...makes possible the free flow of information vital to a law enforcement organization's ability to make responsible decisions regarding the fitness of its applicants."[8]



Special Agent Schofield is chief of the Legal Instruction Unit at the FBI Academy.

"...courts afford absolute immunity to employers for disclosures pursuant to an applicant's consent...."

Courts Uphold Law Enforcement Release Agreements

The two court decisions discussed here involve defamation actions against employers for disclosing information about a former employee to a law enforcement organization. Both cases uphold the legal effectiveness of authorizations for the release of personnel information when disclosure is within the scope of a job applicant's consent.

In a case from New Mexico, a state police department recruit sued

his former employer, alleging he was dismissed from recruit training as a result of his former employer's defamatory statements. As part of the application process, the recruit signed an agreement that allowed the state police to investigate his background and released from liability those who provided information to the state police under a guarantee of confidentiality.

The alleged defamatory statements made by the former employer included: 1) statements made to the state police characterizing the recruit as unfit for law enforcement because of emotional instability, dishonesty, drinking on the job, and resistance to authority; and 2) statements made to the offices of the Governor and the Attorney General characterizing the recruit as a security risk, a danger to certain individuals, and a person who has serious alcohol and drug problems and who exhibits extreme anger. The Supreme Court of New Mexico in *Baker* v. *Bhajan*[9] ruled the statements made to the state police were absolutely privileged but found the disclosures to the Governor's and Attorney General's offices to be outside the scope of the applicant's consent.

In a case from Texas, a police department trainee in the Big Springs Police Department successfully completed police academy training but was terminated during field training because of poor evaluations from training officers. Several months later, the former officer applied for a job with the U.S. Marshals Service (USMS) and completed, as part of the application process, a form authorizing persons contacted to give out information about job applicants. The form purported to "...release any individual... from any and all liability for damages of whatever kind or nature which may at any time result to me on account of compliance, or any attempts to comply, with this authorization."[10]

> ***"...the scope of the consent depends on the terms of the authorization-to-release agreement."***

A USMS investigator presented a copy of this authorization to the Big Springs chief of police, who then told the investigator about his dealings with the former officer. The former officer sued the chief for defamation after receiving a letter from the USMS stating that she was being rejected for employment because the chief had characterized her as having engaged in "irresponsible behavior." The Court of Appeals of Texas in *Smith* v. *Holley* ruled the consent agreement absolutely barred the defamation suit and was broad enough to immunize the chief from liability for the personnel information he disclosed to the USMS investigator.[11]

Terms of Agreement Determine Scope of Disclosure Privilege

Both *Baker* and *Smith* illustrate the generally accepted principle that a job applicant's consent to the release of personnel information creates an absolute bar to defamation liability when former employers disclose information within the scope of the consent. In essence, the scope of the consent depends on the terms of the authorization-to-release agreement.

Consent as embodied in an authorization to release does not necessarily give former employers license to tell everything about a former employee to everyone. The disclosure of personnel information pursuant to a release authorization must "...not exceed what is reasonable in light of the language or circumstances that created it."[12] For example, a job applicant's consent for the release of personnel information to a law enforcement organization would not afford the former employer a privilege to disclose that information to a newspaper for publication.

Unsolicited Disclosures

The *Smith* court ruled that the disclosures by the Big Springs chief did not exceed the applicant's consent because he spoke only about the former officer's job performance and capabilities and only disclosed information to the USMS investigator. The court found that the broad and all-encompassing terms in the applicant's release agreement, in effect, said to the USMS: "You may find out what other people say about me, and I will not litigate if the responses are unfavorable."[13]

Conversely, the *Baker* court found the former employer's disclosures to the offices of the Governor and Attorney General exceeded the terms of the consent because the applicant only agreed to the release of information solicited by the

state police under a guarantee of confidentiality.[14] Thus, the former employer faces potential liability for these two unsolicited disclosures if they were made maliciously or for an improper purpose.[15]

Unanticipated Disclosures

Courts and legal scholars agree that a job applicant's consent does not immunize defamatory disclosures by former employers that the applicant had no reason to anticipate.[16] However, it is not necessary that the defamed applicant know that the personnel information of which he consents is defamatory in character. Instead, it is enough that the applicant knows the contents of the personnel file or has reason to know that it may be defamatory.[17]

A job applicant who signs a release authorization thereby invites the disclosure of personnel information by former employers "...knowing that its contents may damage his reputation cannot complain when his fears come true."[18] Accordingly, the *Smith* court ruled the disclosures by the Big Springs chief were not unanticipated because the former officer knew that the chief and others at the department held unfavorable opinions about her performance at the department.[19]

Good managerial practices will help ensure that disclosures of personnel information are not unanticipated by former employees. These practices include: 1) limiting written disclosures to information contained in official personnel files; 2) limiting oral comments to information that is essentially coextensive with the information contained in official personnel files;[20] 3) affording employees regular and documented feedback on their performance; and 4) affording all employees procedural due process (i.e., notice, reasons, and opportunity to respond) prior to all adverse personnel actions.

> ***"Consent, whether expressed or implied, gives rise to an absolute privilege to disclose."***

Another legal benefit of affording due process prior to adverse personnel actions was set forth in a June 1992 article in the *FBI Law Enforcement Bulletin*, which examined an employer's potential liability for disclosing information that infringes a former employee's constitutionally protected liberty interest.[21] In essence, a liberty interest violation occurs only when the government disseminates stigmatizing and false information concurrent with an employee's termination. Accordingly, affording due process prior to final adverse personnel actions permits government employers to disclose all relevant personnel information to prospective law enforcement employers without fear of violating a former employee's liberty interest.

Disclosures by Persons Not Named in the Consent Agreement

Consent, whether expressed or implied, gives rise to an absolute privilege to disclose. Consent is implied where circumstances show that a former employer's disclosures are relevant to the purpose for which a release agreement is used and is limited to the appropriate prospective employer.[22]

In that regard, the former officer in *Smith* argued that the Authorization for Release of Information she executed did not specifically name the Big Springs chief and, therefore, did not authorize his disclosures. The court rejected that argument by concluding that while a *release for past tortious conduct* might only be effective for specifically named persons, a *consent to future conduct* can be effective against unnamed persons.[23]

Requiring specific names would render consent agreements less effective because there is no way that a general release concerning future disclosures could name all the unknown persons that a prospective law enforcement organization might want to interview. Moreover, the *Smith* court said that implying consent for the future disclosure of personnel information by unnamed persons promotes "...the candid exchange of information that is essential to our job market."[24]

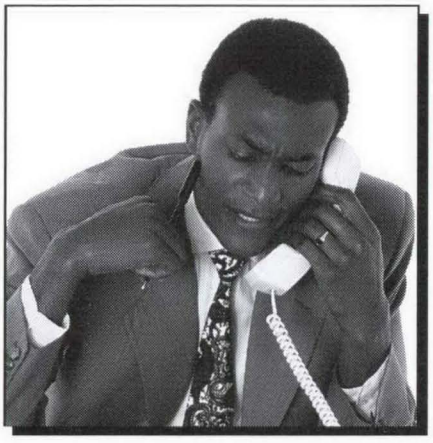
Prior Agreements Not to Disclose

Employers sometimes enter into contractual agreements with employees whereby they promise not to disclose certain personnel information in exchange for an employee's voluntary resignation. These agreements are used as an incentive to get problem employees to resign, thereby saving the employer from time-consuming and costly termination procedures and related litigation.

For example, after the former officer in *Smith* v. *Holley* appealed her termination from the police department, the Big Springs city manager entered into an agreement with her. This agreement stipulated: 1) that the Big Springs Police Department would reinstate her and then allow her to resign citing personal reasons; and 2) that the city would purge from its personnel records all references to the involuntary termination and would mark each page of her personnel file with a notice prohibiting the release to anyone by anybody of any information in her file except the date she was hired as a police officer trainee and the date she resigned for personal reasons.[25]

The *Smith* court concluded that this agreement by the city to keep secret the real reasons for the officer's departure from the police force did not preclude the disclosures made by the Big Springs chief pursuant to the authorization-to-release agreement. First, the court noted the chief was not a party to the city manager's agreement with the former officer and, therefore, was not personally bound by it.[26] Second, the court suggested that a broadly worded agreement like the one signed by the former officer authorizing personal contact with individuals and the release of information would likely be sufficient to relieve former employers of an earlier contractual agreement not to disclose such information.[27]

To ensure that authorizations to release information are not limited by prior contractual agreements, law enforcement organizations should include specific language in release agreements making clear that the applicant consents to the release of that information. For example, the authorization for release of information upheld by the federal court of appeals in *Cox* v. *Nasche* contained a specific provision stating: "I Direct You to Release such information upon request of the duly accredited representative of any authorized agency *regardless of any agreement I may have made with you previously to the contrary.*"[28]



Conclusion

The fear of potential litigation and liability is apparently sufficient to make many employers uncooperative when a law enforcement organization requests they disclose employment information. Courts recognize a compelling public interest for employers to fully disclose all relevant information to a law enforcement organization conducting a background investigation on an applicant for employment.

Accordingly, courts afford absolute immunity to employers for disclosures pursuant to an applicant's consent, as embodied in an authorization-to-release agreement. Therefore, all applicants for sensitive law enforcement positions should be required to sign a release agreement that authorizes full disclosure of all relevant information and that provides maximum protection to those who disclose pursuant to the agreement, a sample of which can be found on the next page.✦

Endnotes

[1] See authorities cited in *Smith* v. *Holley*, 827 S.W.2d 433, 436 (Tex.App.1992).
[2] *Id.*
[3] *Id.* at 439.
[4] *Id.*
[5] 70 F.3d 1030 (9th Cir.1995).
[6] The significance of an absolute, as opposed to a qualified, privilege is that an absolute privilege bars a defamation action, even for maliciously made statements. *Id.* at 1031, n.1.
[7] *Baker* v. *Bhajan*, 871 P.2d 374, 378 (Sup.Ct.N.Mex. 1994).
[8] *Id.*
[9] *Id.*
[10] *Smith v. Holley*, 827 S.W.2d 433,435 (Tex.App.1992).
[11] *Id.* at 436.
[12] *Id.* at 439.
[13] *Id.* at 440.
[14] 871 P.2d at 378.
[15] *Id.* at 379.
[16] 827 S.W.2d at 440.
[17] *Id.*
[18] *Bagwell* v. *Peninsula Regional Medical*, 665 A.2d 297, 316 (Md.App.1995)
[19] 827 S.W.2d at 440.
[20] 665 A.2d at 316.
[21] *See* Jeffrey Higginbotham, "Disclosure of Personnel Information—Constitutional Limitations," *FBI Law Enforcement Bulletin*, June 1992, pp. 26-32.
[22] 871 P.2d at 377.
[23] 827 S.W.2d at 441.
[24] *Id.*
[25] *Id.* at 435.
[26] *Id.* at 440.
[27] *Id.*
[28] 70 F.3d at 1031.

Law enforcement officers of other than federal jurisdiction who are interested in this article should consult their legal advisors. Some police procedures ruled permissible under federal constitutional law are of questionable legality under state law or are not permitted at all.

Sample Authorization for Release of Information Agreement

Law enforcement organizations can use this sample to develop their authorization-to-release information agreement. Any agreement should include space for the applicant's name, current address and telephone number, date of birth, and Social Security Number. All agreements should be signed and dated by the applicant and properly notarized.

TO WHOM IT MAY CONCERN: I am an applicant for a position with the _____Department. The department needs to thoroughly investigate my employment background and personal history to evaluate my qualifications to hold the position for which I applied. It is in the public's interest that all relevant information concerning my personal and employment history be disclosed to the above department.

I hereby authorize any representative of the _____ Department bearing this release to obtain any information in your files pertaining to my employment records and I hereby direct you to release such information upon request of the bearer. I do hereby authorize a review of and full disclosure of all records, or any part thereof, concerning myself, by and to any duly authorized agent of the _____Department, whether said records are of public, private, or confidential nature. The intent of this authorization is to give my consent for full and complete disclosure. I reiterate and emphasize that the intent of this authorization is to provide full and free access to the background and history of my personal life, for the specific purpose of pursuing a background investigation that may provide pertinent data for the _____Department to consider in determining my suitability for employment in that department. It is my specific intent to provide access to personnel information, however personal or confidential it may appear to be.

I consent to your release of any and all public and private information that you may have concerning me, my work record, my background and reputation, my military service records, educational records, my financial status, my criminal history record, including any arrest records, any information contained in investigatory files, efficiency ratings, complaints or grievances filed by or against me, the records or recollections of attorneys at law, or other counsel, whether representing me or another person in any case, either criminal or civil, in which I presently have, or have had an interest, attendance records, polygraph examinations, and any internal affairs investigations and discipline, including any files which are deemed to be confidential, and/or sealed.

I hereby release you, your organization, and all others from liability or damages that may result from furnishing the information requested, including any liability or damage pursuant to any state or federal laws. I hereby release you, as the custodian of such records of _____organization, including its officers, employees, or related personnel, both individually and collectively, from any and all liability for damages of whatever kind, which may at any time result to me, my heirs, family, or associates because of compliance with this authorization and request to release information, or any attempt to comply with it. I direct you to release such information upon request of the duly accredited representative of the _____Department regardless of any agreement I may have made with you previously to the contrary. The law enforcement organization requesting the information pursuant to this release will discontinue processing my application if you refuse to disclose the information requested.

For and in consideration of the _____Department's acceptance and processing of my application for employment, I agree to hold the _____, its agents and employees harmless from any and all claims and liability associated with my application for employment or in any way connected with the decision whether or not to employee me with the _____ Department. I understand that should information of a serious criminal nature surface as a result of this investigation, such information may be turned over to the proper authorities.

I understand my rights under Title 5, United States Code, Section 552a, the Privacy Act of 1974, with regard to access and to disclosure of records, and I waive those rights with the understanding that information furnished will be used by the _____department in conjunction with employment procedures.

A photocopy or FAX copy of this release form will be valid as an original thereof, even though the said photocopy or FAX copy does not contain an original writing of my signature.

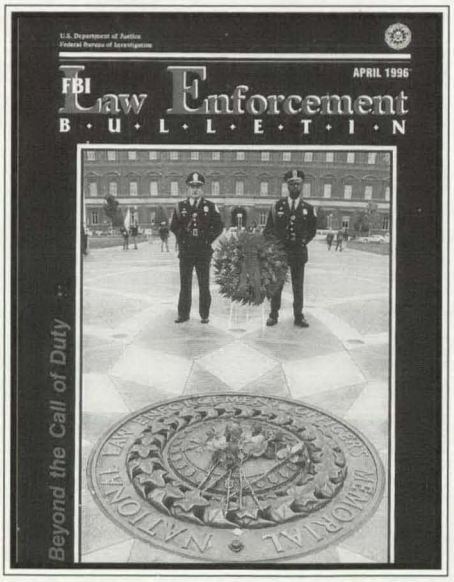
This waiver is valid for a period of _____ from the date of my signature.

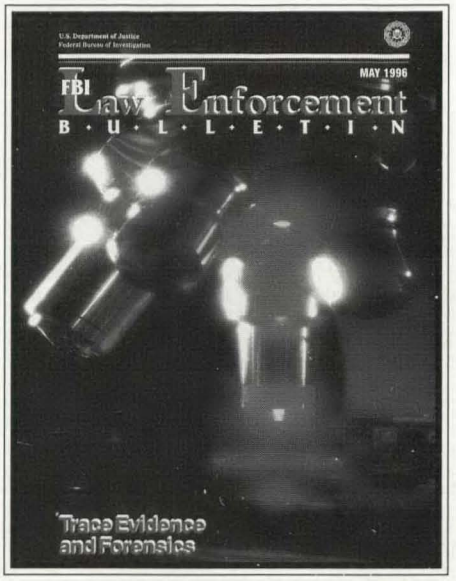
Should there be any questions as to the validity of this release, you may contact me at the address listed on this form.

I agree to pay any and all charges or fees concerning this request and can be billed for such charges at the address listed on this form.

I agree to indemnify and hold harmless the person to whom this request is presented and his agents and employees, from and against all claims, damages, losses and expenses, including reasonable attorney's fees, arising out of or by reason of complying with this request.

1996 Subject Index





PERSONNEL

"College Internship Program: Prospective Recruits Get Hands-on Experience," (police practice), Kevin W. Dale, September, p. 21.

"Critical Incident Stress in Law Enforcement," Arthur W. Kureczka, February/March, p. 10.

"Police Cynicism: Causes and Cures," Wallace Graves, June, p. 16.

"Police-Defendants: Surviving a Civil Suit," Dave Chambers, February/March, p. 34.

"The Police Supervisor and Stress," (focus), Steven R. Standfest, May, p. 7.

"Preventing Police Suicide," Thomas E. Baker and Jane P. Baker, October, p. 24.

"Retirement: A New Chapter, Not the End of the Story," Bill Rehm, September, p. 6.

POLICE-COMMUNITY RELATIONS

"Bank Robbery: A Target for Community Policing," Phillip W. Lissenden, September, p. 16.

"Community-Oriented Policing Means Business," Kenneth Sissom, December, p. 10

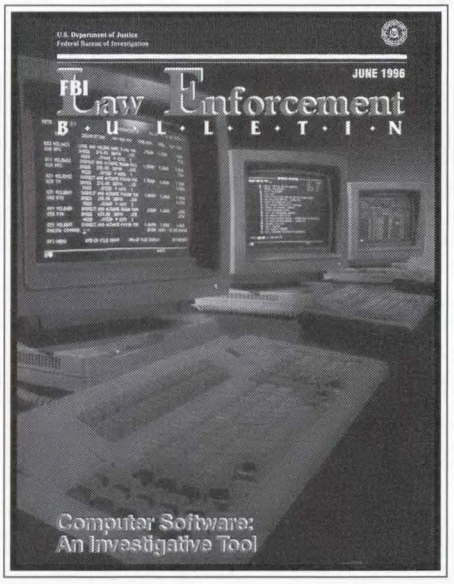
"Implementing Change: Community-oriented Policing and Problem Solving," Ronald W. Glensor and Ken Peak, July, p. 14.

"Neighborhood Service Team," Robert R. Barber, January, p. 17.

POLICE PROBLEMS

"Canaries in Cages: Responding to Chemical/Biological Incidents," Larry A. Mefford, August, p. 20.

"The Lethal Triad: Understanding the Nature of Isolated Extremist Groups," Kevin M. Gilmartin, September, p. 1.



"Social Protests in the 1990s: Planning a Response," Gary A. Allgeyer, January, p. 1.

"Suspect Restraint and Sudden Death," Donald T. Reay, May, p. 22.

RESEARCH

"Above and Beyond the Call of Duty: Preventing Off-duty Officer Deaths," Edward F. Davis and Anthony J. Pinizzotto, April, p. 1.

"The Project on Human Development in Chicago Neighborhoods," (research forum), Kimberly J. Waggoner, February/March, p. 28.

TECHNOLOGY

"Laptop Computers: New Technology for Law Enforcement," Keith J. Cutri, February/March, p. 1.

"The New Horizon: Transferring Defense Technology to Law Enforcement," Rome Laboratory Law Enforcement Technology Team, April, p. 10.

"Online Services for Law Enforcement," Timothy M. Dees, October, p. 1.

TRAINING

"Ethics Training: Using Officers' Dilemmas," Joycelyn M. Pollock and Ronald F. Becker, November, p. 20.

"Integrated Use-of-Force Training System," Brian R. Arnspiger and Gordon A. Bowers, November, p. 1.

"Interagency Drug Training," (focus), William M. Toms and Stephen G. McAllister, November, p. 8.

"Pursuing Publication," Julie R. Linkins, May, p. 26.

VIOLENT CRIMES

VICAP Alert: Thomas Edward Luther, January, p. 22.

1996 Author Index

A

Adams, Susan H., Special Agent, FBI Academy, Quantico, VA, "Statement Analysis: What Do Suspects' Words Really Reveal?" October, p. 12.

Allgeyer, Gary A., Captain, Melbourne, FL, Police Department, "Social Protests in the 1990s: Planning a Response," January, p. 1.

Arnspiger, Brian R., Detective, Burbank, CA, Police Department, "Integrated Use-of-Force Training System," November, p. 1.

B

Baker, Jane P., Assistant Director, Student Development Services, Marywood College Counseling Center, Scranton, PA, "Preventing Police Suicide," October, p. 24.

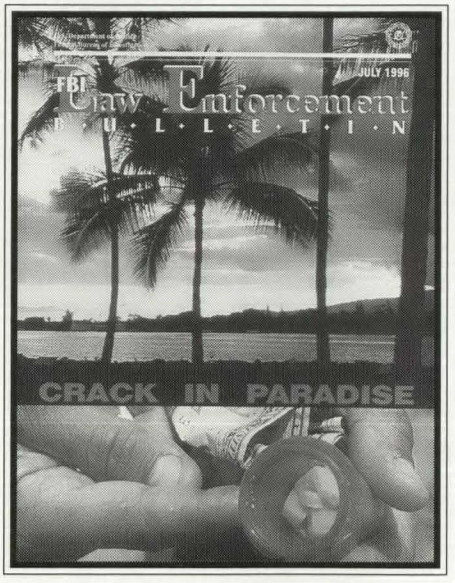
Baker, Thomas E., Assistant Professor, University of Scranton, Scranton, PA, "Preventing Police Suicide," October, p. 24.

Barber, Robert R., Commander, Garland, TX, Police Department, "Neighborhood Service Team," January, p. 17.

Becker, Ronald F., Professor, Southwest Texas State University, San Marcos, TX, "Ethics Training: Using Officers' Dilemmas," November, p. 20.

Birzer, Michael L., Sergeant, Sedgwick County Sheriff's Department, Wichita, KS, "Police Supervision in the 21st Century," (point of view), June, p. 6.

Blackledge, Robert D., Senior Chemist, Regional Forensic Laboratory, Naval Criminal Investigative Service, San Diego, CA, "Condom Trace Evidence: A New Factor in Sexual Assault Investigations," May, p. 12.



Bliss, Lynne, Police Officer (reserve), Colorado Springs, CO, Police Department, "Assisting Senior Victims," (police practice), February/March, p. 6.

Bowers, Gordon A., Captain, Burbank, CA, Police Department, "Integrated Use-of-Force Training System," November, p. 1.

Bowker, Arthur L., Investigator, Office of Labor Management Standards, U.S. Department of Labor, Cleveland, OH, "Downloading: Using Computer Software as an Investigative Tool," June, p. 1.

Branon, William D., Special Agent in Charge (retired FBI), Chicago, IL, "Operation REACT: Targeting Violence in Chicago," July, p. 22.

C

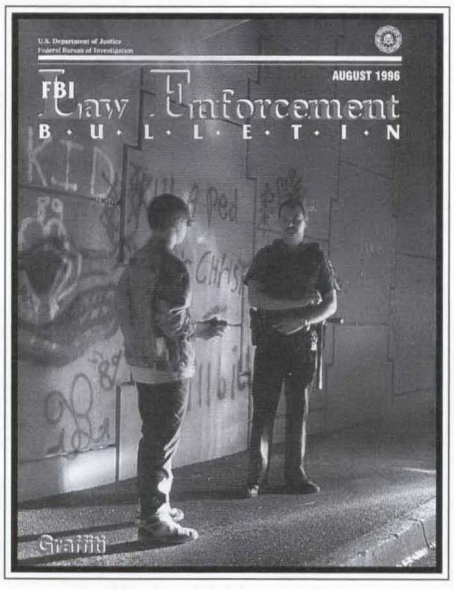
Carter, David L., Professor, Michigan State University, East Lansing, MI, "Computer Crime: An Emerging Challenge for Law Enforcement," December, p. 1.

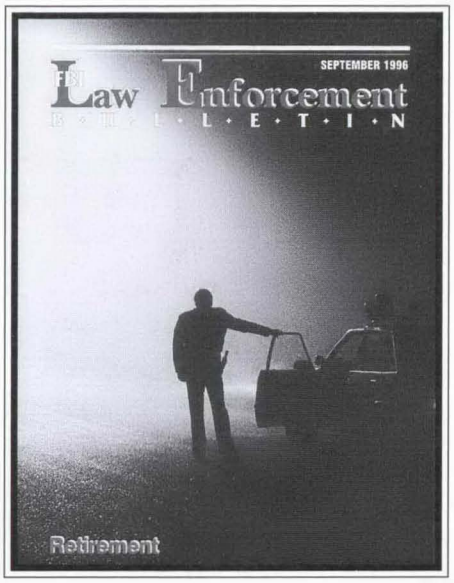
Chambers, Dave, Consultant, Pacific Palisades, CA, "Police-Defendants: Surviving a Civil Suit," February/March, p. 34.

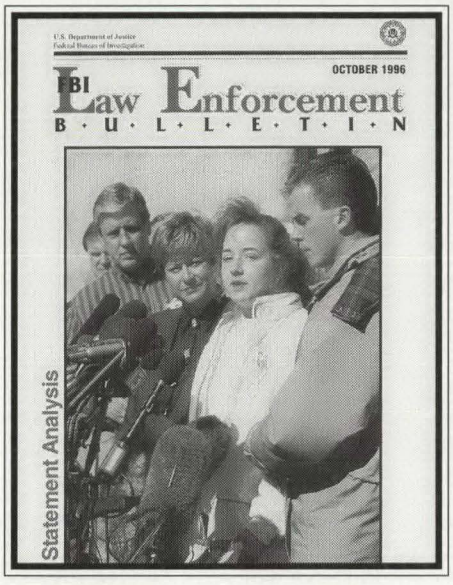
Colletti, Joseph L., Chief, Emeryville, CA, Police Department, "Why Not Hire Civilian Commanders?" (point of view), October, p. 8.

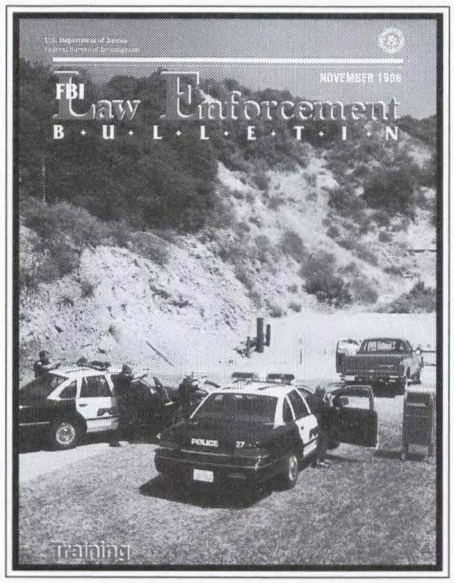
Courtney, Kevin M., Director, Big Rapids, MI, Department of Public Safety, "Internal Affairs in the Small Agency," (focus), September, p. 12.

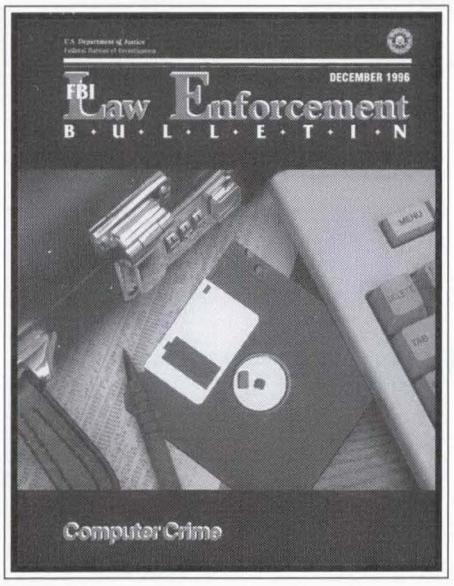
Crawford, Kimberly A., Special Agent, FBI Academy, Quantico, VA, "Consent Searches: Guidelines for Officers," August, p. 27.





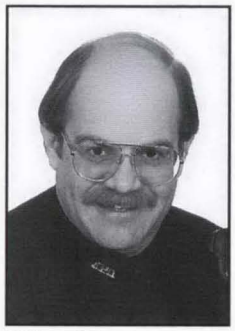




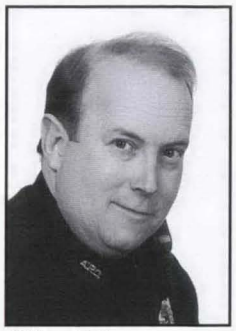


The Bulletin Notes

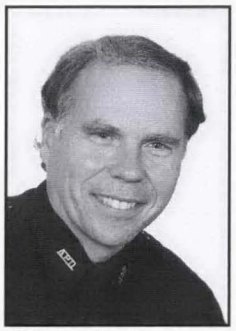
Law enforcement officers are challenged daily in the performance of their duties; they face each challenge freely and unselfishly while answering the call to duty. In certain instances, their actions warrant special attention from their respective departments. *Law Enforcement* also wants to recognize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



Officer Bair



Officer Dalos



Officer Gilbertson

On a quiet Sunday morning, a man carrying a loaded semi-automatic rifle walked into the main terminal of the Minneapolis/St. Paul International Airport. When an unarmed security guard approached him, the gunman fired wildly, missing the guard, but sending passengers throughout the terminal seeking cover. The gunman then continued walking through the terminal, randomly firing his weapon. Airport police department officers Ronald E. Bair, John A. Dalos, and Brian C. Gilbertson observed the gunman exit the terminal and walk onto an airport runway. When they instructed the man to drop his weapon, he ignored their commands and fired nearly 30 rounds at the officers, who had taken positions behind concrete pillars. From a distance of 50 yards, the officers returned fire and struck the subject three times. They then took the man into custody and rendered first aid until he could be transported to a local hospital. Fortunately, none of the 43 rounds fired by the gunman struck anyone. The former mental patient later pled guilty to violating a new provision of the U.S. Code, which makes it a federal crime to commit an act of violence at an international airport.

Officer McCollum

Chris McCollum, when chief of the Pickensville, Alabama, Police Department, drove into a neighboring jurisdiction to assist in the late-night search for a vehicle that had reportedly struck a utility pole. Seeing no sign of the wreck, Chief McCollum started to return to Pickensville. As he drove behind a pickup truck and a local patrol car, he saw an oncoming vehicle lose control, strike the patrol car, and skid into the truck before bursting into flames. Chief McCollum immediately stopped to render assistance and, with the help of the driver of the pickup truck, was able to save two of the four occupants of the vehicle by pulling them out of the burning wreckage. Chief McCollum then went to the aid of the Aliceville, Alabama, police officer, who had been ejected from his vehicle and was laying face down in a ditch of water. Chief McCollum carried the officer out of the ditch, possibly saving him from drowning. Former Chief McCollum since has become an officer with the Aliceville Police Department.

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

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

Official Business
Penalty for Private Use $300

Patch Call

The patch of the Kitsap County, Washington, Sheriff's Department depicts the clear blue skies of the Pacific Northwest over evergreen trees, Puget Sound and the Olympic mountain range. The county also is the home base for a Trident submarine, a likeness of which is shown on the patch below a sheriff's badge.

The Huachuca City, Arizona, Police Department patch features a bald eagle, indigenous to the area, flying over the three local mountain ranges known as the Whetstones, Huachucas, and the Dragoons. Huachuca City is nicknamed "The Sunset City" because of the beautiful colors that are cast over the mountains at sunset.