U.S. Department of Justice
Office of Community Oriented Policing Services

Problem-Oriented Guides for Police
Problem-Specific Guides Series
No. 21

Check and Card Fraud

by
Graeme R. Newman

www.PopCenter.org

Center for Problem-Oriented Policing

Got a Problem? We've got answers!

Log onto the Center for Problem-Oriented Policing website at www.popcenter.org for a wealth of information to help you deal more effectively with crime and disorder in your community, including:

- Web-enhanced versions of all currently available Guides
- Interactive training exercises
- On-line access to research and police practices

Designed for police and those who work with them to address community problems, www.popcenter.org is a great resource in problem-oriented policing.

Supported by the Office of Community Oriented Policing Services, U.S. Department of Justice.

Problem-Oriented Guides for Police
Problem-Specific Guides Series
Guide No. 21

Check and Card Fraud

Graeme R. Newman

This project was supported by cooperative agreement #2002CKWX0003 by the Office of Community Oriented Policing Services, U.S. Department of Justice. The opinions contained herein are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Justice.

www.cops.usdoj.gov

ISBN: 1-932582-27-4

About the Problem-Specific Guides Series

The *Problem-Specific Guides* summarize knowledge about how police can reduce the harm caused by specific crime and disorder problems. They are guides to prevention and to improving the overall response to incidents, not to investigating offenses or handling specific incidents. The guides are written for police–of whatever rank or assignment–who must address the specific problem the guides cover. The guides will be most useful to officers who

- **Understand basic problem-oriented policing principles and methods.** The guides are not primers in problem-oriented policing. They deal only briefly with the initial decision to focus on a particular problem, methods to analyze the problem, and means to assess the results of a problem-oriented policing project. They are designed to help police decide how best to analyze and address a problem they have already identified. (An assessment guide has been produced as a companion to this series and the COPS Office has also published an introductory guide to problem analysis. For those who want to learn more about the principles and methods of problem-oriented policing, the assessment and analysis guides, along with other recommended readings, are listed at the back of this guide.)

- **Can look at a problem in depth.** Depending on the complexity of the problem, you should be prepared to spend perhaps weeks, or even months, analyzing and responding to it. Carefully studying a problem before responding helps you design the right strategy, one that is most likely to work in your community. You should not blindly adopt the responses others have used; you must decide whether they are appropriate to your local situation. What is true in one place may not be true

elsewhere; what works in one place may not work everywhere.

- **Are willing to consider new ways of doing police business.** The guides describe responses that other police departments have used or that researchers have tested. While not all of these responses will be appropriate to your particular problem, they should help give a broader view of the kinds of things you could do. You may think you cannot implement some of these responses in your jurisdiction, but perhaps you can. In many places, when police have discovered a more effective response, they have succeeded in having laws and policies changed, improving the response to the problem.

- **Understand the value and the limits of research knowledge.** For some types of problems, a lot of useful research is available to the police; for other problems, little is available. Accordingly, some guides in this series summarize existing research whereas other guides illustrate the need for more research on that particular problem. Regardless, research has not provided definitive answers to all the questions you might have about the problem. The research may help get you started in designing your own responses, but it cannot tell you exactly what to do. This will depend greatly on the particular nature of your local problem. In the interest of keeping the guides readable, not every piece of relevant research has been cited, nor has every point been attributed to its sources. To have done so would have overwhelmed and distracted the reader. The references listed at the end of each guide are those drawn on most heavily; they are not a complete bibliography of research on the subject.

- **Are willing to work with other community agencies to find effective solutions to the problem.** The police alone cannot implement many of the responses discussed in the guides. They must frequently implement them in partnership with other responsible private and public entities. An effective problem-solver must know how to forge genuine partnerships with others and be prepared to invest considerable effort in making these partnerships work.

These guides have drawn on research findings and police practices in the United States, the United Kingdom, Canada, Australia, New Zealand, the Netherlands, and Scandinavia. Even though laws, customs and police practices vary from country to country, it is apparent that the police everywhere experience common problems. In a world that is becoming increasingly interconnected, it is important that police be aware of research and successful practices beyond the borders of their own countries.

The COPS Office and the authors encourage you to provide feedback on this guide and to report on your own agency's experiences dealing with a similar problem. Your agency may have effectively addressed a problem using responses not considered in these guides and your experiences and knowledge could benefit others. This information will be used to update the guides. If you wish to provide feedback and share your experiences it should be sent via e-mail to **cops_pubs@usdoj.gov**.

For more information about problem-oriented policing, visit the Center for Problem-Oriented Policing online at www.popcenter.org or via the COPS website at www.cops.usdoj.gov. This website offers free online access to:

- the *Problem-Specific Guides* series,
- the companion *Response Guides* and *Problem-Solving Tools* series,
- instructional information about problem-oriented policing and related topics,
- an interactive training exercise, and
- online access to important police research and practices.

Acknowledgments

The *Problem-Oriented Guides for Police* are very much a collaborative effort. While each guide has a primary author, other project team members, COPS Office staff and anonymous peer reviewers contributed to each guide by proposing text, recommending research and offering suggestions on matters of format and style.

The principal project team developing the guide series comprised Herman Goldstein, professor emeritus, University of Wisconsin Law School; Ronald V. Clarke, professor of criminal justice, Rutgers University; John E. Eck, associate professor of criminal justice, University of Cincinnati; Michael S. Scott, assistant clinical professor, University of Wisconsin Law School; Rana Sampson, police consultant, San Diego; and Deborah Lamm Weisel, director of police research, North Carolina State University.

Karin Schmerler, Rita Varano and Nancy Leach oversaw the project for the COPS Office. Suzanne Fregly edited the guides. Research for the guides was conducted at the Criminal Justice Library at Rutgers University under the direction of Phyllis Schultze.

The project team also wishes to acknowledge the members of the San Diego, National City and Savannah police departments who provided feedback on the guides' format and style in the early stages of the project, as well as the line police officers, police executives and researchers who peer reviewed each guide.

Contents

About the Problem-Specific Guides Series i

Acknowledgments v

The Problem of Check and Card Fraud 1
- Illegal Acquisition of Checks and Cards 6
- Illegal Use of Checks and Cards 7
- Low Reporting of Check and Card Fraud 8
- Factors Contributing to Check and Card Fraud 10

Understanding Your Local Problem 13
- Asking the Right Questions 13
  - Incidents 13
  - Offenders 14
  - Victims 15
  - Locations/Times 15
- Measuring Your Effectiveness 16

Responses to the Problem of Check and Card Fraud 19
- General Considerations for an Effective Response Strategy 20
  - Working with Businesses 21
  - Community Partnerships 33
  - Enforcement 36
- Responses with Limited Effectiveness 40

Appendix: Summary of Responses to Check and Card Fraud 43

Endnotes 49

References 51

About the Author 57

Recommended Readings 59

Other Problem-Oriented Guides for Police 63

The Problem of Check and Card Fraud

This guide describes the problem of check and card fraud, and reviews factors that increase the risks of it. It then identifies a series of questions to help you analyze your local problem. Finally, it reviews responses to the problem, and what is known about them from evaluative research and police practice.

The guide covers fraud involving (1) all types of checks and (2) plastic cards, including debit, charge, credit, and "smart" cards. Each can involve a different payment method. While there are some obvious differences between check and card fraud, the limitations and opportunities for fraud and its prevention and control by local police are similar enough to warrant addressing them together. Furthermore, some cards (e.g., debit cards) are used and processed in a similar way to checks, and electronic checks are processed in a similar way to cards, so that the traditional distinction between cards and checks is fast eroding. Table 1 summarizes the essential differences between check and card fraud.

Table 1
Common Differences between Check and Card Fraud

	Check	**Card**
Counterfeiting	Entry level: requires photocopier or personal computer with standard color printer	Entry level: amateur alterations easily detectable; more advanced card alteration or production requires more costly resources
Conversion to Cash	Can be converted to cash at checkout	Cannot be converted to cash at checkout (except for debit and phone cards)
Additional ID	Retail stores typically require additional ID; banks may not ask for ID if account number on check matches bank records	Additional ID rarely requested
Signature Checking	Signature rarely checked, unless check-cashing card required	Signature prime means of verifying card user
Payment Processing	Merchant submits check to bank for payment	(Highly simplified): merchant submits card charge to bank, which submits payment request to card issuer, which verifies payment to merchant's bank, which then pays merchant
Loss Liability	If bank rejects payment, merchant carries loss and must recoup it from customer; legitimate account owner may be liable, depending on bank's policies	Negotiable: merchant may incur loss, or card issuer may agree to do so; legitimate card owner generally protected from loss
Vulnerability Points	Check acquisition; check payment and cashing; check processing; and bank, business, and consumer environments	Card issuance; card acquisition; checkout; card-not-present sales (usually telephone or online sales); and after the sale (product returns)
Organized Crime	Less common with checks, though sophisticated check-counterfeiting rings do exist	Counterfeiting and distribution of credit cards widely adopted by organized crime groups

In 2000, Visa International estimated that the yearly cost of fraud worldwide was about 0.05 cent per every dollar spent. This small amount works out to 300 million pounds in Britain and an estimated $1 billion in the United States. Since 1995, the amount of fraud losses on payment cards has consistently risen in the United Kingdom,[1] and in the United States, the losses from online credit card fraud[2] *alone* are estimated to reach $3.2 billion in 2007. Over 50 percent of Britons surveyed fear they will be victims of credit card fraud.[3]

Apart from the obvious financial loss caused by check and card fraud, it is a serious crime that requires preventive action. It affects multiple victims and significantly contributes to other types of crime. At an elementary level, fraud is easy to commit, and the chances of apprehension and punishment are slight.† Thus check and card fraud is an ideal entry-level crime from which people may graduate to more serious offenses. Other crimes that either feed off check and card fraud or facilitate its commission include the following:

- Drug trafficking. Addicts forge checks or fraudulently use credit cards (often bought cheaply as "second string" cards–that is, stolen or counterfeit cards that have already been used). So the fraud fuels the drug trade.[4]
- Identity theft. There is increasing evidence to suggest that obtaining or accessing credit card accounts is the main motive for identity theft,†† a crime that causes victims very serious economic harm (ranging from $5,000 to $20,000 per victim)[5] and psychological harm.††† Sophisticated technology has made the counterfeiting of checks and plastic cards much more difficult over the last decade. Although there is no

† In a Montreal study, the success rate with a totally counterfeit card was 87 percent, and with an altered card, 77 percent. At checkout, the average success rate was 45 percent, although in most of the cases where the sales clerk rejected the card, the offender simply walked away, without being accosted (Mativat and Tremblay 1997).

†† In 2002, the Federal Trade Commission reported that the main motives for identity theft were as follows: To obtain/take over a credit card account - 53%; To acquire telecommunications services - 27%; To obtain/take over a checking account - 17%; Other - 3%.

††† A 2000 survey of identity theft victims found that less than half felt their problems had been fully resolved; all but one had gone to the police as a last resort and had received little satisfaction from doing so (CALPIRG 2000).

definitive research available, it is likely that, as counterfeiting has become increasingly difficult, offenders have turned to the next best thing: stealing cardholders' identity, and using legitimate cards. Thus identity theft has become a serious crime; the U.S. Congress has passed a special bill to deal with it.[6]

- Mail fraud. Offenders intercept checks, credit cards, or bankcards in the mail, or do not forward mail that card issuers or banks send to a customer's old address.
- Burglaries, robberies, and thefts from cars. Offenders may commit these crimes specifically to get plastic cards, or they may get them as a by-product of the crime.†
- Pickpocketing. Pickpocketers may be attracted to shopping malls and other crowded shopping venues where people use checks and cards.
- Fencing. In areas where offenders commit check and card fraud to buy high-priced goods, a fencing operation may arise to facilitate conversion of the goods into cash.
- Extortion. Customer databases that include credit card and other personal information are very valuable to businesses. They have therefore become targets in their own right, and hackers sometimes steal them and hold them for ransom.[7]
- Organized crime. Counterfeiting and marketing cards requires considerable organization, for both production and distribution. International organized crime rings working out of East Asia tend to be involved in such operations.
- Local gang-related crime. Small gangs may feed the needs of addicts and the poor by using second-string cards to buy food and other items at supermarkets. The locals may protect these gangs, because they provide a "service" to the community.

† Thefts from cars may increase as a way to get credit card and personal information if other opportunities to get such information are blocked by improved security measures in the manufacture and processing of plastic cards and checks (Levi 1998). However, in other studies, this "displacement" does not always occur, even within card fraud itself–for example, from using stolen credit cards to counterfeiting cards (Mativat and Tremblay 1997).

- Cons and scams.[8] The Internet now carries a wide range of cons and scams offenders use to get credit card and other personal information from unknowing victims. People can easily create false websites and storefronts, as little skill is required to do so. Furthermore, many websites offer information on setting up such websites and on running scams.
- Financial crimes against the elderly. The elderly are prime targets of cons and scams, including check and credit card fraud. (For more information, see the *Problem-Specific Guide* on *Financial Crimes Against the Elderly*.)
- Shoplifting. Committing check and card fraud is simply another way of "lifting" products from retailers. Using a credit card fraudulently at checkout is much less risky (because the authentication methods are so cursory).[9] This type of theft from retail stores is probably much greater than regular shoplifting, or it may be used in concert with shoplifting.
- Car theft. Car rental companies are prime targets for credit card fraud. Offenders may sell fraudulently rented cars in the stolen vehicles market.

Plastic-card technology is developing rapidly. Issuers are now offering both debit and credit services on one card, are requiring a personal identification number (PIN) for credit cards (introduced in France a decade ago, and in England in 2001), and are replacing magnetic strips with computer chips. Paperless or electronic checks are increasingly used in business-to-business transactions. Criminal use of these different products involves a wide range of skills, activities, and financial investment. The type of fraud will depend on the points of vulnerability targeted in the delivery of services, as outlined in Table 1.

In general, check and card fraud may be divided into two activities: the illegal *acquisition* of checks and cards, and the illegal *use* of checks and cards. This distinction is not absolute, since offenders may gain *access* to some cards (e.g., phone cards) without actually *acquiring* the cards (e.g., by stealing account numbers).

† Levi (1998) has noted that one in five street robbers in London obtain credit or debit cards from their victims.

Illegal Acquisition of Checks and Cards

The following are some of the ways offenders illegally acquire checks and cards:

- Altering checks and cards. Offenders can do so with the simplest equipment. However, altered checks and cards are sometimes easy to detect.
- Counterfeiting checks and cards. Reasonably priced machines for embossing, encoding, and applying holograms to cards are available on the Internet.
- Committing application fraud. Offenders get a checking or credit card account by using another person's identity or a fictitious one.
- Stealing checks and cards through muggings, pickpocketing, theft from cars, and burglaries.†
- Intercepting checks and cards in the mail. Intercepted cards are particularly desirable because they are unsigned. Offenders may also intercept boxes of blank checks.
- Getting another person's PIN through trickery, for example, by "shimming" (watching as the person punches in a PIN).
- Manufacturing and marketing counterfeit cards via internationally organized crime rings.
- Renting or selling stolen or counterfeit cards to a group of "steady customers" via locally organized crime rings.

- Hacking into a retailer's customer database to get credit card numbers.
- Setting up bogus websites that request credit card and other personal information.

Illegal Use of Checks and Cards

The following are some of the ways offenders illegally use checks and cards:

- Presenting a bogus check or card at checkout. The sales clerk is supposed to verify that (a) the check or card represents an actual account (usually done by checking a computer database), and (b) the person presenting the check or card is the account holder. If the offender gets away with using the check or card, he or she may then dispose of the goods by (a) selling them through a known fencing operation or informally in local bars, or (b) returning the goods to the same store (or a different branch of the store) for cash.
- Making a "card-not-present" purchase (by telephone or on the Internet). Offenders avoid the scrutiny of sales clerks or security cameras and need only the card information, not the card itself. Card-not-present fraud is a major contributor to overall card fraud (see Figure 1). Between 1999 and 2001, it increased some 130 percent in the United Kingdom, with similar increases internationally.[10]
- Denying ordering and/or receiving an item. Customers who order an item online using a legitimate credit card may deny doing so, claim they never received the item, and stop payment on the card. Or they may claim that an item they *did* order was never delivered, and demand a refund.

- Targeting a particular store or set of stores. Small bands of career fraudsters may work together to "hit" a particular store or set of stores with stolen or counterfeit cards. These bands usually do not target stores in or near their own neighborhoods; rather, they will travel some 50 miles to other shopping areas to commit fraud.[11]

† Over 90 percent of people report their lost or stolen card to the card issuer within one day. They rarely, however, report their loss to the police, unless it results from a crime such as pickpocketing, burglary, or mugging (Levi and Handley 1998a).

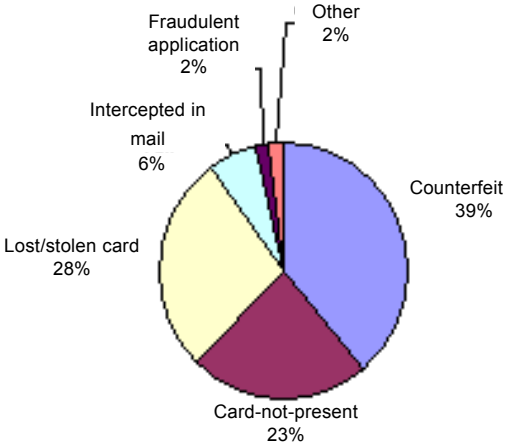

Fig. 1. U.K. card fraud loss by type of fraud, 2001
Source: Adapted from Association of Payment Clearing Services (2002): www.epaynews.com/statistics/fraud.html.

Low Reporting of Check and Card Fraud

Perhaps the biggest problem for police is that people rarely report check and card fraud to them.† In one recent study, only one in four incidents of check and card fraud were reported to the police.[12] It is very likely that you have a check or card fraud problem in your area, but do not know about it. Many credit card issuers promise zero loss to the user if the card is lost or stolen and illegal are charges made. Thus, if cardholders do not suffer

financially, they may have less motivation to report the offense to the police. Merchants are also reluctant to report fraud, or even to use fraud prevention techniques at checkout, for fear that it will slow down the purchasing process and negatively affect sales.[13] Thus, fraudsters think their chances of getting caught are very slim. One study reported that some 80 percent of respondents thought it was easy or very easy to carry out credit card fraud.[14]

The situation with check fraud is slightly different. Some banks hold the account holder liable for loss. The merchant who accepts the check may also be held responsible, since the bank simply refuses to honor the check if it detects a forgery. (Thus, retailers–especially North American supermarkets, where check cashing is a common service–are often more willing to cooperate with police or develop their own security procedures concerning check fraud.) It is not uncommon for some conflict to arise between merchants and banks as to who should bear the loss.[15] This is a serious problem because, as we will see, cooperation among competing merchants and between merchants and banks is central to preventing and reducing check and card fraud.[16]

Banks, large retail stores, and supermarket chains commonly prefer to deal with merchandise loss, employee theft, shoplifting, and check and card fraud internally.[17] There are three significant reasons for this preference:

- They do not think police have the specific skills, knowledge, and experience needed to deal with security issues in the banking and retail environment.

- They hold a widespread view that losses due to theft and fraud are simply a cost of doing business, and that those losses are more than offset by the profits made from using tempting product displays or only quickly checking customer identities at checkout.
- They fear that calling in the police might negatively affect business, because the crime problems become public.

The check and card fraud that businesses *do* report to the police is usually committed by repeat or "professional" fraudsters. Or, for whatever reasons, the in-house security wants to transfer responsibility to the criminal justice system.

Factors Contributing to Check and Card Fraud

Understanding the factors that contribute to your problem will help you frame your own local analysis questions, determine good effectiveness measures, recognize key intervention points, and select appropriate responses. You should be aware that most check and card fraud is due to factors beyond police control. Such factors include the following:

- There are security flaws in check and card design and production.
- Police typically do not have access to the vulnerability points in the complex transactions that make up check and card processing.
- It is inherently difficult to verify a check or card user's identity.
- The Internet has greatly increased the opportunities for fraud, perhaps having its greatest impact through fraudulent card-not-present sales (see Figure 1).†

† A traditional credit card purchase goes something like this: At checkout, the customer gives the card to the sales clerk, who runs it through the computer to check whether the account is legitimate. The clerk then checks whether the customer is the person named on the card (usually by comparing signatures, which are not an especially reliable form of identification, by the way). In a face-to-face situation, the clerk can try to verify the customer's identity. However, with telephone and online purchases, there is no direct way to do so.

- Information about counterfeiting, skimming, and hacking is now widely available on the Internet. Thus, it is easier to commit card fraud than ever before.[18]
- To some extent, the sheer volume of card use accounts for the increased amount of card fraud. In the United Kingdom, the United States, and Australia, debit and credit card use has increased tremendously over the last 20 years, although in the U.S., checks remain the primary form of payment (besides cash). In Japan, credit cards have been very slow to catch on, but debit cards have gained wider acceptance.[19] These differences are largely related to the structure of financial service markets in the various countries.
- The amount of card fraud committed internationally has substantially increased in recent years. For example, the proportion of fraud committed abroad on U.K. cards has doubled in the past decade.[20]
- Although the rate of check fraud has decreased considerably in the past decade, the financial loss due to check fraud continues to increase, simply because of the increase in the volume of sales.
- There is a technological "arms race."[21] Each technological advance makes it harder and harder to counterfeit checks and cards. Microdot printing on checks, hidden markings on checks and cards that show up on color photocopiers, holograms, magnetic strips, and now embedded chips–all these and many more advances have raised the level of skill and equipment needed for fraudsters to counterfeit checks and cards. Unfortunately, dedicated fraudsters quickly acquire the skills and equipment, so are soon able to produce checks and cards that are extremely difficult to identify as counterfeit. In fact, as Figure 1 shows, counterfeiting is the major type of card fraud, and it is increasing rapidly.[22]

- International organized crime groups that specialize in counterfeit credit cards generally lie beyond the reach of local police, although their markets certainly lie within local neighborhoods. These groups became very active in Southeast Asia toward the end of the 1990s, and in a short time, have managed to overcome every new security feature introduced into plastic-card manufacture. Their distribution system employs Asians in large North American and European cities.[23]
- Many card issuers are eager to get customers. In recent years, the competition has become very intense. The mail and Internet are loaded with tempting offers, and it is now very easy to get a credit card.
- Many card issuers do not hold cardholders responsible for any loss incurred through fraudulent use by another. Thus, cardholders have no real motivation to take security precautions. In fact, they may even collude with others. Retailers may bear the loss in card-not-present sales, and card issuers in standard credit-card sales.

Although police face these and other obstacles when addressing check and card fraud, there is much that can be done.

Understanding Your Local Problem

The information provided above is only a generalized description of check and card fraud. You must combine the basic facts with a more specific understanding of your local problem. Analyzing the local problem carefully will help you design a more effective response strategy later on.

Asking the Right Questions

The following are some critical questions you should ask in analyzing your particular problem of check and card fraud. (Depending on the local circumstances, you may need to focus on one specific type of fraud. In general, it is best to focus on one small aspect of the problem at a time, such as a single merchant or bank.) Your answers to these questions will help you choose the most appropriate set of responses later on.

Incidents

- Have checks or cards been targeted in other crimes such as burglaries of homes and offices, pickpocketing in shopping malls, muggings, and thefts from cars?
- When you receive reports of check or card fraud, what kinds of offenses do they usually entail: check alteration, card counterfeiting, assaults at ATMs, Internet fraud, etc.?
- Who typically reports these crimes: checking or card account holders, retailers, banks, or card issuers?
- Is online fraud (from card-not-present sales) a problem in your area? Online fraud may become apparent when fraudsters order online but arrange to pick up merchandise at the store. Do merchants report any such instances?

- Are there any cases of parcels stolen or "lost" during delivery of items ordered online?
- Are there known fencing operations in or near your area? If so, what kinds of items are most commonly fenced, and are they traceable to any local stores? Do new items frequently appear in pawnshops?
- What national, regional, or local databases do public or private agencies maintain concerning check and card fraud?

Offenders

- Do fraudsters work alone, or in groups? How many work alone? How many work with others? How and where do they get together? How do they offend together? Why do they offend together? (Arrested offenders are a good information source, but remember that they may differ from active fraudsters in important ways. In addition, they may be reluctant to share information if they are concerned about three-strikes laws.)
- What are fraudsters' demographic characteristics, such as age and gender? What is their ethnicity, as this may relate to the source of counterfeit or stolen cards, or the targeting of victims?
- Where do fraudsters live, work, or hang out?
- Do they know their victims?
- How active are fraudsters? Do particular offenders account for a few frauds, or many? Do they specialize in one particular type of check or card fraud?
- What, specifically, motivates fraudsters? Do they need quick cash to party or to support a family? Are they addicted to drugs, and if so, to what? Are they recently jobless, or are they long-term offenders?

- Do they show evidence of planning their crimes, or do they take advantage of easy opportunities?
- What special skills and techniques do they use to commit their crimes?†

† In one study, fraudsters had worked out over 100 different ways of committing credit card fraud (Jackson 1994). In another, offenders displayed considerable innovation in switching from one technique of check forgery to another (Lacoste and Tremblay 2003).

Victims

- How do individuals respond to their victimization? (It is likely that you will rarely speak with cardholders, because they usually report stolen cards to the card issuers, rather than to the police.)
- Are particular individuals repeatedly victimized? If so, why?
- How do businesses respond to their victimization? Do they routinely report check and card fraud to the police? (Some may be unwilling to do so for fear that police attention will drive business away, or, in the case of card fraud, because they do not have to bear the loss.) What kinds of stores report fraud: small family stores, large retail chains, supermarkets, local or regional banks, etc.? Why do they report it?
- What are merchant attitudes regarding police involvement in dealing with fraud?
- What procedures do they have for detecting or preventing fraud?
- Are particular businesses repeatedly victimized? If so, why?

Locations/Times

- Does check and card fraud occur in a specific area, on a particular day, and/or at a particular time?
- Are specific types of places targeted, such as supermarkets, electronics stores, retail chains, restaurants, or online stores?

- Do muggings or thefts from cars that entail theft of credit cards occur in neighborhoods where drug dealing is common?
- Does fraud occur at checkout in local stores?
- How do fraudsters travel to and from the scene?
- If fraudsters make "card-not-present" purchases, do they use the telephone or the Internet? Do they call stores from home or from public phones? Do they access online stores from home computers or those available in public places (e.g., college campuses, public libraries, Internet cafés)?

Measuring Your Effectiveness

Measurement allows you to determine to what degree your efforts have succeeded, and suggests how you might modify your responses if they are not producing the intended results. You should take measures of your problem *before* you implement responses, to determine how serious the problem is, and *after* you implement them, to determine whether they have been effective. (For more detailed guidance on measuring effectiveness, see the companion guide to this series, *Assessing Responses to Problems: An Introductory Guide for Police Problem-Solvers.*) It should be emphasized that some measures will depend on merchants' providing information and establishing systematic procedures for collecting the data you need. You will need to convince merchants that the loss-prevention benefits will offset the data-collection costs, and that data collection is necessary for a cost/benefit analysis.

The following are potentially useful measures of the effectiveness of responses to check and card fraud:

- Fewer repeat offenders.
- Increased reporting of check and card fraud.
- Decreases in retail losses attributed to check and card fraud. Retailers may use the number of transactions, or the total amount of sales, as the base against which they compute losses.
- Differences in reported frauds between stores or banks where you focus your activities and those where you do not (keeping in mind that changes may be due to other factors, and that reported crime does not always reflect actual crime).
- Reductions in related crimes such as burglaries, thefts from cars, or robberies at ATMs where credit or bankcards may be a prime target (keeping in mind that changes may be due to other factors related to those crimes).[24]
- Increases in some related crimes when fraudsters' efforts are thwarted and they shift to easier targets (displacement). One study has suggested that acquisitive crime may increase as credit card fraud decreases.[25] Other studies have found that fraudsters tend not to switch easily *between* different types of credit card fraud[26] though they are resourceful in shifting between different types of check fraud, or at least in inventing new ways to commit check fraud.[27]
- Reductions in the amount of new products fenced or available in pawnshops.
- Fewer reports of lost or stolen goods purchased for home delivery.

Responses to the Problem of Check and Card Fraud

Your analysis of your local problem should give you a better understanding of the factors contributing to it. Once you have analyzed your local problem and established a baseline for measuring effectiveness, you should consider possible responses to address the problem.

This section reviews what is known about the effectiveness of various practices in dealing with check and card fraud. Unfortunately, the information is severely limited because few of the common preventive practices have been evaluated. Card issuers, retailers, and bankers have been reluctant to conduct the necessary studies, or to share the results of those they do conduct. The government has funded little research in this field, generally regarding it as the private sector's domain.

The following response strategies provide a foundation of ideas for addressing your particular problem. It is critical that you tailor responses to local circumstances, and that you can justify each response based on reliable analysis. In most cases, an effective strategy will involve implementing several different responses. Do not limit yourself to considering what police can do: give careful consideration to others in your community who may share responsibility for the problem. It will be essential to work closely with local businesses and community groups. The most effective program to reduce check and card fraud reported to date involved banks, retailers, business associations, database administrators, and local, regional, and national police.[28]

† Most large retail stores now have standard antishoplifting technology, such as item tagging, tracking, etc. However, such technology cannot prevent card fraud at checkout. People commonly do not notice their credit cards are missing until a day or more after their loss. Unlike shoplifters, card fraudsters are in no immediate risk of being detected or of setting off alarms. Thus it may be expected that, as technology makes shoplifting more and more difficult, thieves may turn more to card fraud.

General Considerations for an Effective Response Strategy

As noted, local police can do little on their own to prevent check and card fraud. In many cases, you will have to persuade local bankers and merchants to act. You may have to explain why police can achieve little using traditional responses such as surveillance and arrest, and why heavier court sentences are of limited value. You may want to explain to merchants that the way they process check and card payments may be contributing to the problem. You may have to convince retailers and bankers that they cannot ignore the problem, because the costs to the community are too great and, in the long run, the stores and banks themselves suffer. Finally, you will need to advise them on preventive measures they can take to reduce the problem.

It is important that responses be selective and based on a thorough understanding of the particular circumstances. For example, fraudsters often target high-priced electronic gadgets and appliances because they promise more cash.[29] Or, it might be better to concentrate on preventing check and card fraud by casual offenders, who are easier to deter, than to focus on the much smaller number of "professionals," who are harder to defeat. Again, such choices depend on your local circumstances. In framing advice, you must think carefully about the nature of the risk, which varies greatly depending on the kind of store and goods offered; the types of cards accepted; the store's check-cashing policies; and the store's or bank's marketing practices. These factors determine the nature of the remedies. Department stores with huge turnovers of expensive goods can afford to spend much more on security than small retailers can, and their corporate headquarters often dictate security procedures.† In all

cases, you must appreciate stores' need to make a profit. *It cannot be emphasized enough that the success of your efforts will depend heavily on how well you can convince local retailers that improved security procedures can and do increase the bottom line.* In making your case, you may need to:

- calculate the likely cost of measures such as installing a computerized customer database and issuing customers ID cards for check cashing;
- convince retailers that they can recoup the cost of increased security through reduced losses from fraud (e.g., item replacement, profit, and lawsuit losses);
- enlist the support of the local Chamber of Commerce or other business organizations in persuading business owners to improve security; and
- brief (with care) the local media on the problem and the proposed solutions.

Working with Businesses

1. **Raising responsibility awareness.** As noted, many card issuers and banks do not hold cardholders liable for losses if their card is lost or stolen. Nor, in many cases, do they hold the merchant who accepts the card liable. Similarly, although merchants and banks incur losses from bad checks, they are reluctant to implement the security procedures necessary to prevent these losses, because they believe customers (especially regular customers) are "turned off" by being asked for ID. Yet research has shown that simply requiring two forms of ID for check cashing can significantly reduce the rate of fraudulent checking (see response #3). You must convince card issuers, banks, and merchants that any monetary losses due to fraud are serious losses both to them and to customers

(who, of course, eventually bear the ultimate loss through higher prices and higher card interest rates). Perhaps worse, though, is the harm done to the community when identity theft is part of the fraud, because of the loss of trust it causes.† All parties concerned must be convinced of their responsibility:

† The 2000 British Crime Survey (Home Office 2000) found that 50 percent of respondents reported being fairly worried or very worried about credit/bankcard fraud–more than for mugging/robbery or physical attack.

- merchants and bankers: to adopt antifraud procedures;
- card issuers: to adopt marketing techniques that do not offer opportunities to potential fraudsters: and
- customers: to take security precautions with their cards (for example, not leaving their purses or wallets in a locked car).

2. **Increasing the reporting of fraud.** You should try to persuade local retailers and bankers to report fraud so that you can get some estimate of both the extent and the pattern of the problem. This will help you to raise awareness of the problem and to pinpoint businesses experiencing a higher rate of fraud. However, you must take care to ensure that any reporting of incidents be linked to a planned preventive program, not done merely "to add information to police records." That is to say, data collection must have a specific preventive purpose. You must also take care that police action resulting from increased reporting of fraud does not receive publicity that may negatively affect merchant activity, or be perceived to do so. Unless there is an active and positive program linked to reporting fraud, negative publicity can easily ensue.

3. **Verifying checks, cards, and users**. Check and card manufacturers have introduced an impressive array of technological features that make counterfeiting or alteration very difficult. However, two significant facts work against them:

- Committed counterfeiters can easily match technological developments because all the equipment they need is relatively cheap and widely available on the Internet.
- Counterfeit checks and cards do not need to be all that good. They just need to get by what is usually only a cursory or inadequate checkout inspection.[31] Even amateurs who simply need a small amount of cash quickly to buy food or drugs can often avoid detection at checkout.

Thus, while local police may not be able to get at the source of many counterfeit cards (Asia), they can do something about where counterfeit cards and checks are used (checkout), if they work with the merchants concerned.

You can do much to inform merchants about modern verification procedures, particularly small businesses that, unlike large retail chains, may not have ready access to account and cardholder databases. Many police department websites offer lists of specific actions merchants can take to detect check and card fraud at checkout. In general, sales clerks must do the following:

- Verify that the check or card is legitimate and represents a legitimate account. In the case of cards, this is usually done electronically by transmitting the card information to a central card-issuer database.

- Verify that the person offering the check or card is the account holder. Sales clerks typically do this by checking the customer's signature. Unfortunately, it is widely known that a signature alone is a very poor verification of customer identity. So there is a very high probability (over 60 percent) that someone using, say, a stolen check or credit card will get away with it at checkout.

† Since the late 1990s, U.S. retailers have increasingly required a customer thumbprint (using special invisible ink) to accept checks. Some police departments provide the ink for free to local retailers. However, unless police work closely with retailers, retailers may fear this requirement will have a negative effect on customers, who may consider it an invasion of their privacy (even though the print is used only if the check turns out to be fraudulent).

Researchers have shown that adding simple security procedures can significantly reduce check and card fraud. In one U.S. study in a retail store,[32] a system that used picture IDs of customers who paid with credit cards reduced fraud by over 80 percent. Furthermore, retail stores (especially supermarkets) have found that customer databases that issue customers ID cards can also be used as an effective marketing tool to advertise special sales and promotions. A study in Norway[33] showed that legislation requiring people to show two forms of ID when cashing checks reduced check fraud by over 80 percent.†

A sales clerk checks a customer's thumbprint.

While these simple measures seem obvious and commonsense, if you visit any retail store and observe the security procedures for verifying checks or cards, you will see that sales clerks rarely or only casually use the ones described here. As noted, merchants often do not implement such procedures because they fear the negative effect they may have on sales. There is, however, no research to justify this view–although there is research that suggests that checkout delays do reduce sales. Therefore, you must take these concerns into account if you try to get local merchants to change their security procedures. Simply informing them about security possibilities is not enough. To avoid the negative effects of checkout delays, a carefully planned system has to be developed. This may require the input not only of the merchants, but also of security experts. Finally, *an evaluation of the program's effectiveness must be built in to show that the savings from frauds prevented more than offset the cost of implementing the program*. Without this assurance, retailers are unlikely to adopt security procedures.†

† A simple, inexpensive, and quick procedure that can be done without checkout delays is to use black light to check for counterfeit cards. All major cards (MasterCard, Visa, American Express, and Discover) contain images that are visible under black light. The Troy (N.Y.) Police Department has successfully implemented this procedure.

4. **Training checkout staff.** As noted in the previous response, introducing new technology and procedures to identify illegal credit card use or fraudulent check cashing will be of little help if the staff who are required to check IDs are not trained to do so effectively. Ideally, a combination of technology (e.g., biometric techniques) and procedures that make identity verification independent of sales clerks' judgment would be the solution. The introduction of PINs for credit cards (as with debit cards) has been shown to substantially reduce credit card fraud in Europe, but widespread introduction will take several years. Using thumbprint, black light, and other biometric techniques to validate checks also shows promise.[34]

In the meantime, there are three important ways you can help businesses train staff:

- Work with business associations or specific businesses to play a role in their training of new and continuing staff. In training sessions, you should work to raise staff's responsibility awareness (see response #1), for you can be assured that if the general business attitude is that card fraud is simply a cost of doing business, that attitude will show in the everyday practices of checkout staff.
- You should also inform staff of the known methods of check-cashing fraud and illegal card use that involve collusion with sales clerks, and inform them of the dangers of participating in such offenses. Keep in mind that, by various estimates, some 50 percent of "shrinkage" (loss of stock in a retail store due to any cause) is attributed to employee theft. For this reason, if a business has an especially serious fraud or theft problem, it may be advisable to install closed-circuit television (CCTV) cameras at checkouts. This step should, however, be a last resort, because CCTV requires carefully planned and defined implementation, usually requiring the services of an experienced security professional for installation and, especially, evaluation.[35]
- You should encourage the merchant to conduct–and, where legally appropriate, you should assist with–background checks on new employees. The U.S. Chamber of Commerce estimates that some 30 percent of all business failures result from employee theft. If businesses hire honest employees, then the risk of collusion with customers at checkout is obviously less.

As with other responses in this section, you will need to gain a considerable amount of trust from businesses–and,

where appropriate, security professionals–to participate in staff training. You must make your role and goals very clear to businesses, so they know you are not out to find something amiss in their business practices.†

† Unfortunately, there are merchants who set up bogus companies to collude with co-offenders to process fraudulent purchases made with credit cards, or to defraud honest cardholders. Merchant-alert databases have been successfully used in the United Kingdom to identify fraudulent merchants and warn honest cardholders of possibly risky locations and businesses (Levi and Handley n.d.).

5. **Reducing card application fraud.** By far the biggest contributor to application fraud is the huge volume of invitations to apply for cards sent out in the mail every day, and available on the Internet. Fraudulent applications are very easy to complete using false personal information.[36] In general, local police cannot do much about this–it is a problem of national and international proportions. However, there are three types of local card application fraud:

- Getting new cards using a stolen identity.
- Intercepting card renewal mail or other mail that contains a person's identifying information (some postal employees have done this).
- Surveilling mail delivered to vacant houses, such as those for sale, or obtaining credit card applications by not forwarding mail to a previous resident. (In this case, you can work with real estate agencies and the post office to ensure that card renewal letters reach their proper destination. Since vacant residences may be located in several different mail-delivery areas, coordination with the post office may be very difficult.)

6. **Using information to fight online card fraud.** Offenders make online or telephone card-not-present purchases from retail stores that are most likely out of state or even abroad, beyond local police jurisdiction. A significant amount of card application fraud also occurs when people apply for cards either online or by telephone. As distant as such frauds may seem to local police, the fact

remains that they are committed by people who live in particular jurisdictions, and at the other end, fraud victims, whether merchants or individual cardholders, also live in particular jurisdictions. Depending on your department's resources (some large departments have specialized fraud and electronic-crime squads), you can take some practical steps (limited though they might be) to counteract at least the effects of fraud, and perhaps prevent some of it from occurring. You can do this by using the most powerful tool available in the 21st century–information:

- In 2002, the FBI set up a computer crime squad that has considerable technical and prosecution capabilities. The U.S. Justice Department also issues updates on current frauds and scams, and on where they are occurring in the United States.
- Check with the major online websites that specialize in collecting information about frauds and scams in general, credit card frauds, and other fraud-related crime that occurs on the Internet. Many sites provide useful information on how to identify various frauds and how to protect against victimization (see list in box).

Useful Internet Sources

Association of Payment Clearing Services: www.cardwatch.org.uk/

Better Business Bureau: www.bbb.org/

CERT/CC. Carnegie Mellon University repository of reported hacking incidents: www.cert.org/stats/cert_stats.html

Credit Federal: www.creditfederal.com/credit-card-fraud-prevention.htm

Crime Prevention Service: http://crimeprevention.rutgers.edu/

FBI National Computer Crime Squad, through the Washington Field Office: email nccs@fbi.gov, or call 202.324.9164

FBI Washington Field Office: www.nipc.gov/sites/ipcis/ipcis.htm

Federal Citizen Information Center: www.pueblo.gsa.gov/scamsresources.htm

Federal Communications Commission, Consumer and Governmental Affairs Bureau: www.fcc.gov/cgb/information_directory.html

Federal Trade Commission: www.ftc.gov/

International Web Police: www.scamwatch.com/

Netcheck.com: www.netcheck.com/

US Department of Justice: www.usdoj.gov/criminal/fraud.html

Most states have websites for their attorney general's office, many of which provide updates and advice on current and past scams:

New Jersey Office of the Attorney General: www.state.nj.us/lps/oag/index.html

Office of New York State Attorney General: www.oag.state.ny.us/

- Because of the risks involved in maintaining massive online databases of individual cardholder information, businesses should (and increasingly do) develop and clearly publicize a privacy policy to ensure their customers that their personal information is safe, and will not be used for any other purposes except purchases. Small local businesses can increasingly accept credit card payments online as web-purchasing software becomes cheaper and easier to install on small websites. You can help local businesses by providing any available information on privacy policies and procedures. This may involve simply providing website addresses as part of maintaining a productive working relationship with local businesses. You should not assume that businesses, especially small ones, are well acquainted with such information, since many hire website developers to design their websites and may have limited knowledge of the risks involved in web retailing.
- As an information provider, you may be able to help small businesses get connected to services that maintain databases of card-use patterns. Currently, the major card issuers (e.g., Visa, MasterCard, and American Express) provide this service, which analyzes card use and detects any abnormal patterns. This service has significantly reduced card fraud by not only flagging unusual card use,† but also errant merchant processing. Stores that issue check-cashing cards could also use this service.

† Visa claimed card fraud reductions of up to 20 percent after it introduced software that detected unusual spending patterns (Maremont 1995).

The obvious difficulty with this response is that it does not focus as much on a specific crime as is usual in problem-oriented policing, but instead entails a more general approach of enhancing police-business relations. Thus, although it may help in implementing some of the

other responses described in this section, it may be difficult to evaluate its specific effects on online credit card fraud.

7. **Tracking products.** Legitimate cardholders sometimes use the following techniques to commit online card fraud:

- They deny having made a purchase and insist the item was not delivered.
- They say they made a purchase (it was charged to their account), the item was not delivered, and they want a refund.

In the first case, local police can do very little. But in the second, they might work with delivery companies to locally track items bought online. Tracking technology is revolutionizing retailing and many other business areas, and it is certainly at the operational core of UPS, Federal Express, and other delivery companies. Small transmitters are rapidly replacing bar coding, the most pervasive tracking technology of the late 20th century. These transmitters can be placed on retail items (they have proved particularly effective in reducing shoplifting),[37] vehicles (including delivery vehicles),[38] pets, livestock, and even people. They can be programmed to hold substantial information and to transmit location. Such devices make the recovery of stolen items much easier and can precisely track the delivery of products. Indeed, some companies already provide this service for stolen cars and trucks.[39] Because of the massive increase in online retailing, many more products are delivered to the home, creating opportunities for theft en route. The following are ways you can help businesses verify product delivery and detect possible card fraud:

- Work with Neighborhood Watch and local delivery companies to ensure that deliveries to residences where no one is home are left in safe places. Using focused Neighborhood Watch programs is one of many ways to ensure safe deliveries.[40]
- Fraudsters claiming nondelivery may give a bogus address (perhaps that of a vacant house) to get the item. Working with real estate agencies (see response #5) to track vacant local residences may help reduce such opportunities.
- Work with local retail chains from which customers can purchase products online. Credit card fraudsters commonly return items to the store for a refund. Patterns of product return and cases of excessive returns should be monitored.

The amount of card fraud committed through nondelivery claims is probably quite low, though there are no data to support this assumption. There may be high rates of product theft from delivery vehicles in some densely populated urban areas.[41] You may have to balance your delivery-monitoring efforts against competing demands on police time. But bear in mind that your responses to delivery theft may also work in reducing other crimes, such as selling stolen goods, returning stolen goods for refunds, and shoplifting.

8. **Raising perceptions of wrongdoing and risk.** Reminding would-be shoplifters that shoplifting is a crime and warning them that they will be prosecuted can help reduce shoplifting.[42] Stores commonly post signs to that effect. As noted above, making purchases via check or card fraud is a form of shoplifting, but with much less risk. A simple sign such as "WE REQUIRE ID FOR CHECKS AND CARDS" indicates that the business takes

IDs seriously. Sign placement may depend on a store's particular patterns of theft, procedures for processing check and card payments, and ways of dealing with customers. Putting up a sign costs very little, and monitoring its effectiveness is relatively straightforward. Of course, this presumes that stores keep records of check or card fraud incidents.

Community Partnerships

9. **Educating cardholders.** Although cardholders are not liable for losses if their credit cards are lost or stolen, they may be liable for many other card-related thefts. And if their entire identities are stolen, they may suffer considerable financial loss. Customer education concerning practical precautions to avoid identity theft, including credit card and bank account access, may contribute substantially to preventing fraud. These precautions may include:

- carrying only a minimum of cards in high-risk neighborhoods;
- covering the keypad when punching in a PIN at an ATM, or a card number and PIN on a telephone, to prevent a passerby or someone using binoculars from seeing your number;
- never giving out personal information (e.g., Social Security, credit card, or bank account numbers) over the phone to telemarketers or anyone claiming to be collecting money for charity;
- never responding to online requests for personal or card information unless they are on a trusted website;
- never buying from an online retailer unless the website has a clear statement about the security measures it takes with its personal information databases, and about its online privacy policy;

† See the POP Guide on *Financial Crimes Against the Elderly*.

- never leaving credit or bankcards in a vehicle, whether locked or unlocked (these are among the most common items stolen from cars);[43]
- never letting anyone (including family members) use your debit or credit card, or know your PIN;
- watching carefully how sales clerks process your credit card and, if the store still uses mechanical card-processing devices, making sure that copies of receipts are destroyed; and
- not using publicly accessible computers (e.g., in libraries or Internet cafes) to make online purchases, because hackers may later retrieve your personal data.

Who should tell cardholders about these precautions? Local police do not have the ready access to customers that merchants and card issuers do: it is much easier for merchants and card issuers to provide crime prevention information along with customer bills and statements, or on ATM welcome screens. However, police do have access to two groups of customers (or potential customers): those who are typically targets of scams–senior citizens–and those who know little about banking or using credit cards–children. With the cooperation of local businesses and community groups, police could set up educational programs to give talks to senior citizen groups, and to visit schools to talk to students about responsibly managing personal information, bank accounts, and payment cards.† While it would be sensible to target high school students, as some either already use credit and debit cards, or soon will, there may be good reason to target younger students as well, as they increasingly use the Internet. Of course, the effectiveness of such a program will be difficult to measure, since it requires a broad approach directed at affecting future behavior.

10. **Publicizing the costs of fraud.** Perhaps the biggest challenge in dealing with fraud is changing attitudes toward it. Offenders typically view merchants and banks as rich and able to afford losses from fraud (one of their "excuses" for breaking the law).[44] Card issuers view fraud as a cost of doing business. Police must allocate scarce resources where they are most cost-effective. It seems reasonable, then, given merchants' reluctance to report credit card fraud and banks' reluctance to report check and debit card fraud, for police to give such crime a low priority. Yet don't merchants–who pay taxes–have at least some right to expect the police to "do something" about fraud when it directly affects their businesses?[45] The problem here is one of perception: who does fraud harm, how much harm does it do, and who is responsible for preventing it?

One response is to publicize what is known about fraud–emphasizing its financial and human costs, and spelling out the steps people can take to avoid becoming victims. Response #2 entailed working with businesses to increase the reporting of fraud, and response #1 suggested ways of raising responsibility awareness among merchants, card issuers, and customers. The most direct and–probably–effective way to reach all those affected by fraud is through the local media, which tend to be very interested in reporting on crime victims.[46] Police could write a piece outlining the costs to both victims and police: for example, it can take victims up to three months to straighten out credit problems caused by stolen identity, and may cost police up to $20,000 to investigate a case of identity theft.[47] As usual, you must take care to ensure that any publicity is linked to a planned prevention program agreed to by local business associations and merchants.

11. **Collaborating with colleges.** College students using campus computers have committed some of the major hacking offenses.[48] Offenders have committed other crimes, such as stalking and pornography-related offenses, using Internet cafes and public libraries. As part of your overall strategy, you might work with college computer departments, to make sure that they have established a clear and publicized policy on campus computer use, outlining users' rights and responsibilities, and that they can track computer use if a hacking incident is traced to the campus. In addition, colleges are increasingly adopting "smart" cards that students use to charge meals and buy items from campus stores. You should work with colleges to make sure they have taken precautions to prevent fraudulent use of such cards and, if possible, work with campus security to educate students about fraud prevention. There is some indication that a fraud prevention program may work best if combined with programs to prevent other common campus crimes,[49] such as shoplifting and mobile phone theft. Bear in mind, though, that different colleges have different traditions and policies regarding local police participation in crime prevention. They also carefully guard information about crimes occurring on or near campus, for fear that publicity may adversely affect college applications. You should be sensitive to this issue and be aware that collecting the necessary information or data to measure the effectiveness of crime prevention programs may be difficult.

Enforcement

12. **Monitoring fencing outlets, pawnshops, and online auctions.** A major problem for check and card fraudsters is converting goods into cash. At the local level, you can be sure that the existence of fencing outlets may substantially contribute to fraud and to retail theft, in

general.[50] Thus you should monitor any known outlets, as well as monitor the flow of new items into pawnshops and the sale of goods through online auctions. The majority of auction websites now list the sellers' locations–though these tend to be broad regions. However, since research has shown that card fraudsters tend to operate some distance from home,[51] the broad regional information is probably accurate enough. To make monitoring the sale of stolen goods of use in preventing fraud, you will need to have a close working relationship with retailers, so that you can track the items. Today's tracking technology will help in doing so.

13. **Monitoring chat rooms, bulletin boards, and bogus websites.** Response #12 included monitoring online auctions for sales of stolen goods. You may also monitor chat rooms and bulletin boards where people discuss acquiring counterfeit or stolen cards, hacking into databases containing card information, and committing card fraud. Have a look at alt.phreaking (http://members.tripod.com/~SeusslyOne/FAQ.html) or the various alt.hacker newsgroups (http://newsgroup.netwings.ch/alt.hacker.html). It is not difficult to join these chat rooms and bulletin boards, and given the anonymity the Internet allows, it is relatively easy to conduct "undercover" surveillance of them. Unfortunately, finding out users' location is difficult without the help of Internet service providers (ISPs) or computer crime specialists.

You should be on the lookout for bogus websites, as well. (Again, not much skill is needed to set up a website. Nor does it cost much, if anything, to do so.) Fraudsters have tricked many unsuspecting web users into sending credit card and other personal information to bogus companies.

There are websites that constantly monitor the Internet for such scams, so you should routinely visit these to check on the latest incidents. Again, unless you have help from an ISP or a computer crime expert, you may have difficulty determining the location of the people operating the scams. As suggested in response #6, you should keep in close contact with nearby police departments that have specialized computer crime departments, and with the relevant state and federal agencies that monitor Internet fraud. You can also check with the Better Business Bureau or other local consumer-reporting agencies, as well as pay attention to news reports, to find out if there have been scams in your area.

14. **Targeting high-risk merchants.** Rates of check and card fraud vary enormously, both between different chains and between stores in the same chain. One study reported that recoveries per fraudulent check ranged from approximately one in 268 for one large chain, to one in 24 for another in a similar line of business.[52] You must develop a systematic way of collecting fraud information, so that you can identify high-risk merchants in your area. If collecting incident data is initially impossible (and it probably will be), you should try other avenues such as working with business associations to get a rough idea of which businesses are victimized most. It is likely that offenders target particular types of stores (such as large electronics stores for card fraud, and supermarkets for check fraud). Or they may target particular stores because they are considered "easy." Using crime mapping,[53] perhaps with assistance from specialized task forces in the region or from larger police departments nearby (see next response), may also help in identifying high-risk merchants. Once you have identified them, you should try to build a working relationship with management to implement fraud-prevention measures.

15. **Getting help from experts.** If your police department is in or near a big city, you probably have access to a variety of experts who can help you. These may fall into several categories:

- **Professional security consultants.** These experts specialize in areas such as product scanning and tracking, checkout fraud, CCTV, card authentication, employee screening and training, and check verification. You can find them through a simple web search.
- **Specialist police units or individuals.** Some police departments have specialist units or individuals who conduct fraud investigations. However, the extent to which they address fraud proactively (with prevention in mind) rather than reactively (from an investigative viewpoint) is not known. Unless these units or individuals adopt carefully planned preventive programs, they may find themselves inundated with incident reports from merchants who see the police as the solution to their problems.[54] For example, a 1995 Scottsdale (Ariz.) Police Department program successfully addressed a serious case-backlog problem in the check fraud bureau by adopting a team approach to working with local merchants.[55] Many police departments in the United States and elsewhere have special antifraud programs, though they vary considerably in sophistication. A web search will reveal hundreds of such programs, though few with a problem-oriented approach.
- **Regional or national squads.** Some check and card fraud is of a regional, national, or international scope. For example, credit card counterfeiting and distribution operations reach from Southeast Asia to North America and Europe, requiring highly focused and specialized squads to track down the perpetrators and

identify their manufacturing and marketing systems.[56] There is a good chance that these organized crime networks reach into your area; hence the importance of working with regional and national squads. However, bear in mind that, with a few notable exceptions, such squads primarily (perhaps necessarily) focus on investigating and prosecuting individual cases, and do not use a problem-oriented approach.

† If crackdowns are to work–and they do in some cases, for some crimes–they should be carefully tailored to work with the other responses described in this guide. See the POP Guide on *The Benefits and Consequences of Police Crackdowns*.

Responses with Limited Effectiveness

16. **Conducting crackdowns.** There are some difficulties with crackdowns. If, by "crackdowns," we mean intensive campaigns to publicly catch and arrest perpetrators of check and card fraud,† then we face a serious problem in police-business relations. This is because retailers, and even bankers, have a longstanding belief that a strong police presence on or near their premises, especially when arrests are likely, contributes considerably to negative customer attitudes that translate into decreased business. The reluctance of merchants to use thumbprints to verify ID, even when strongly pressured to do so by police, illustrates this problem.

17. **Implementing business watch.** The popularity of Neighborhood Watch has spawned some attempts to use that approach for businesses. However, unless business watch is clearly oriented toward solving a specific problem (e.g., the reduction or prevention of check fraud at supermarkets), in contrast to reducing business crimes in general, it is likely to fail for want of focus, enthusiasm, and participation. Business owners must have specific crime-prevention goals if they are to devote the time and effort needed to make the program work.[57]

18. **Handling offenders through means other than the criminal justice system.** Check and card fraud offenders who are reported to the criminal justice system tend to receive a low priority in processing, resulting in extensive case backlogs.[58] Rather than formally report people who commit crimes against businesses (e.g., shoplifting, drug- and alcohol-related misdemeanors, vandalism), many jurisdictions opt for informal procedures, issuing warnings to offenders, requiring that they compensate their victims, and/or requiring that they get counseling. These alternatives to the regular criminal justice system are usually reserved for juveniles and depend heavily on community–and, in the case of shoplifting, business and shopping mall security–involvement. No research exists on whether these alternatives would work for check and card fraud, nor has research established the extent to which juveniles are involved in such fraud. What data are available suggest that check and card fraud offenders tend to be adults, with an occasional preponderance of drug users and college students. However, without research that examines the entire range of behaviors that make up check and card fraud, it is difficult to predict whether any criminal justice or quasi-criminal justice procedures that effectively address shoplifting could also be applied to fraud.

19. **Conducting publicity campaigns.** We have recommended establishing educational programs to help people avoid being fraud victims (response #9), and publicizing the economic and human costs of fraud (response #10). These responses must be part of a broader business and community initiative, not solely a police initiative (as with "lock your car" campaigns). In fact, a study of a Stockholm, Sweden campaign failed to demonstrate any measurable effect on the rate of theft from cars. The campaign looked more promising, however, when combined with security measures such as environmental changes to enhance natural surveillance.[59]

Appendix: Summary of Responses to Check and Card Fraud

The table below summarizes the responses to check and card fraud, the mechanism by which they are intended to work, the conditions under which they ought to work best, and some factors you should consider before implementing a particular response. It is critical that you tailor responses to local circumstances, and that you can justify each response based on reliable analysis. In most cases, an effective strategy will involve implementing several different responses. Law enforcement responses alone are seldom effective in reducing or solving the problem.

Response No.	Page No.	Response	How It Works	Works Best If…	Considerations
Working With Businesses					
1.	21	Raising responsibility awareness	Local businesses and card issuers are encouraged to take more responsibility for preventing fraud	…police emphasize the community costs of fraud to merchants	Many security, card-issuing, and verification policies are dictated by national and international card issuers, bankers, and retail chains, making it difficult to change local practices
2.	22	Increasing the reporting of fraud	Data collection allows police to determine the extent of the problem in their area	…it is combined with a preventive program (see response #3)	The media may portray increased reporting of incidents as a "crime wave" demanding a police crackdown, rather then an aid to planned preventive procedures

Response No.	Page No.	Response	How It Works	Works Best If…	Considerations
3.	23	Verifying checks, cards, and users	Retailers with high check or card fraud losses are targeted, and verification procedures are established	…verification procedures are integrated into the established checkout practices, and an evaluation demonstrates cost-effectiveness	Merchants may resist spending money on verification, especially if it requires investing in new technology and changing checkout procedures
4.	25	Training checkout staff	Regular staff training raises awareness about fraud prevention	…police establish a close, trusting relationship with businesses and clearly communicate goals	Merchants may distrust police attempts to participate in staff training sessions
5.	27	Reducing card application fraud	Vacant residences and newly occupied residences where credit card information may be sent are identified	…police work closely with postal employees and real estate agencies to ensure that mail is not delivered to unoccupied residences, and is forwarded to the appropriate people	Vacant residences may be in several different mail-delivery areas, requiring extensive coordination with the post office
6.	27	Using information to fight online card fraud	Specified websites alert users to online fraud	…police provide prevention and enforcement information to small local businesses	It is difficult to evaluate this response's effect on online fraud, since it is primarily directed at enhancing police-business relations; generally, preventing online fraud is beyond the means of local police

Response No.	Page No.	Response	How It Works	Works Best If…	Considerations
7.	31	Tracking products	Police work with delivery companies, local retailers, and Neighborhood Watch to monitor product delivery and product returns	…manufacturers, retailers, and delivery companies use new tracking technology	Cost-effectiveness may be difficult to determine; tracking may work in reducing related crimes such as shoplifting and theft of items in transit
8.	32	Raising perceptions of wrongdoing and risk	Retailers post warning signs at checkouts	…retailers keep records of check and card fraud both before and after posting signs, to measure their effectiveness	Merchants may resist this response, inexpensive though it is, for fear that it will have a negative effect on law-abiding customers
Community Partnerships					
9.	33	Educating cardholders	Educational programs teach people to avoid victimization by taking simple precautions	…it is combined with crime prevention education about a variety of crimes for which they may be targeted	This response requires considerable cooperation from community groups and schools
10.	35	Publicizing costs of fraud	The media are used to publicize the financial and human costs of fraud	…police work with businesses and the media to craft stories that emphasize crime prevention	Stories of victimization may affect businesses negatively; media treatment of stories and information may be unpredictable; effectiveness is probably not measurable

Response No.	Page No.	Response	How It Works	Works Best If…	Considerations
11.	36	Collaborating with colleges	Police encourage colleges to establish responsible-use policies for computing facilities, to minimize hacking	…it is combined with crime prevention education about a variety of crimes for which they may be targeted	Effectiveness is difficult to measure, and depends on colleges' willingness to invite local police to their campuses to help solve crime problems
Enforcement					
12.	36	Monitoring fencing outlets, pawnshops, and online auctions	Police work with businesses to develop strategies to track goods that may be stolen	…police acquire extensive local and regional knowledge of known fencing and pawnshop operations	Local businesses must cooperate in identifying and tracking goods
13.	37	Monitoring chat rooms, bulletin boards, and bogus websites	Police conduct surveillance of crime-facilitating Internet venues	…police get help from ISPs and computer crime experts	It is difficult to determine whether online fraudsters live in your area
14.	38	Targeting high-risk merchants	Police determine what stores have high rates of fraud and focus their efforts on them	…police work with business associations to collect information if incident data are not available	Information-sharing requires a long-term, trusting relationship between police and businesses
15.	39	Getting help from experts	Experts on fraud provide information and skills that may help with local problems	…police network with professional security consultants and fraud squads at the local, regional, and national level	Fraud squads may be investigation-rather than problem-oriented
Responses With Limited Effectiveness					
16.	40	Conducting crackdowns	Police conduct very public, intensive campaigns to catch fraudsters		Merchants may fear that crackdowns will drive business away

Response No.	Page No.	Response	How It Works	Works Best If…	Considerations
17.	40	Implementing business watch	Businesses set up programs similar to Neighborhood Watch	…programs are focused on specific crimes, rather than crime in general	Businesses must have clear crime-prevention goals
18.	41	Handling offenders through means other than the criminal justice system	Police and/or businesses issue offenders warnings, require victim compensation, and/or require counseling rather than make formal criminal reports		This response has usually been used with juveniles who have committed other offenses; it has not been evaluated for check and card fraud
19.	42	Conducting publicity campaigns	Police alone publicize fraud risks	…it is combined with the implementation of practical security measures	Research has not shown this response, alone, to be effective

Endnotes

[1] Levi and Handley (1998a); Association of Payment Clearing Services (2002); www.epaynews.com/statistics/fraud.html
[2] Association of Payment Clearing Services (2002); www.epaynews.com/statistics/fraud.html
[3] Levi and Handley (1998a).
[4] Levi (1998).
[5] U.S. General Accounting Office (2002).
[6] U.S. House (1998).
[7] Newman and Clarke (2003).
[8] Newman and Clarke (2003).
[9] Levi (2000).
[10] Levi and Handley (1998a); Association of Payment Clearing Services (2002); www.epaynews.com/statistics/fraud.html
[11] Levi and Handley (1998b).
[12] Taylor (2002).
[13] Clarke and Newman (2002).
[14] Levi, Bissell, and Richardson (1991).
[15] Levi, Bissell, and Richardson (1991).
[16] Duncan (1995).
[17] Newman and Clarke (2003).
[18] Newman and Clarke (2003).
[19] Mann (2002).
[20] Levi (2000).
[21] Ekblom (2000).
[22] Levi (2000); Levi and Handley (1998a, 1998b).
[23] Mativat and Tremblay (1998).
[24] Scott (2001).
[25] Levi and Handley (n.d.).
[26] Mativat and Tremblay (1997).
[27] Lacoste and Tremblay (2003).
[28] Levi, Bissell, and Richardson (1991); Levi and Handley (1998a).
[29] Mativat and Tremblay (1997).
[30] Scottsdale Police Department (1995).

[31] Levi and Handley (n.d.).
[32] Masuda (1996).
[33] Knutsson and Kulhorn (1997).
[34] Texas Banking (2001).
[35] Pierce (2003); Clarke (2001a); Painter and Tilley (1999).
[36] Levi and Handley (n.d.).
[37] DiLonardo (1996).
[38] McKinnon and Tallam (2002).
[39] Newman and Clarke (2003).
[40] McKinnon and Tallam (2002); Laycock and Tilley (1995).
[41] McKinnon and Tallam (2002).
[42] Clarke (1997); Clarke (2001b).
[43] Clarke (2001a).
[44] Clarke (1997).
[45] Levi and Handley (n.d.).
[46] Chermak (1995).
[47] CALPIRG (2000).
[48] Newman and Clarke (2003).
[49] Sampson (2002).
[50] Sutton (1995).
[51] Levi (2000); Mativat and Tremblay (1997).
[52] Levi, Bissel, and Richardson (1991).
[53] Eck and Weisburd (1995).
[54] Scottsdale Police Department (1995).
[55] Scottsdale Police Department (1995).
[56] Newton (1994); Mativat and Tremblay (1997).
[57] Charlton and Taylor (2003).
[58] Scottsdale Police Department (1995).
[59] Clarke (2001a).

References

British Crime Survey (2000). Home Office: www.homeoffice.gov.uk/rds/bcs1.html.

CALPIRG (2000). *Nowhere to Turn: Victims Speak out on Identity Theft. A CALPIRG/PRC Report–May*. Sacramento, Calif.: Privacy Rights Clearinghouse.

Charlton, K., and N. Taylor (2003). "Implementing Business Watch: Problems and Solutions." T*rends and Issues in Criminal Justice*, No. 244. Canberra, Australia: Australian Institute of Criminology.

Chermak, S. (1995). *Victims in the News: Crime and the American News Media*. Boulder, Colo.: Westview Press.

Clarke, R. (2001a). *Thefts of and From Cars in Parking Facilities, Problem-Specific Guide No. 10*. Problem-Oriented Guides for Police Series. Washington, D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice.

——— (2001b). *Shoplifting, Problem-Specific Guide No. 11*. Problem-Oriented Guides for Police Series. Washington, D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice.

——— (1999). *Hot Products: Understanding, Anticipating, and Reducing the Demand for Stolen Goods*. Police Research Series, Paper 98. London: Home Office.

——— (1997). *Situational Crime Prevention: Successful Case Studies*. 2nd ed. N.Y.: Harrow and Heston.

Clarke, R., and G. Newman (2002). *Modifying Hot Products*. London: Home Office.

DiLonardo, R. (1996). "Defining and Measuring the Economic Benefits of Electronic Article Surveillance." *Security Journal* 7:3–9.

Duncan, M. (1995). "Partners in Crime Prevention." *Canadian Banker* 102(6):25.

Eck, J., and D. Weisburd (eds.) (1995). *Crime and Place, Crime Prevention Studies*, Vol. 4. Monsey, N.Y.: Criminal Justice Press.

Ekblom, P. (2000). "Future Crime Prevention–A Mindset–A Way of Thinking Systematically About Causes of Crime and Solutions to Crime Problems." In Foresight (2000) *Turning the Corner*. London: Department of Trade and Industry, Crime Prevention Panel, DTI/Pub/ 5185/5k/12/00/NP/URN00/136 CD Annex.

Jackson, J. (1994). "Fraud Masters: Professional Credit Card Offenders and Crime." *Criminal Justice Review* 19(1):24–55.

Knutsson, J., and E. Kulhorn (1997). "Macromeasures Against Crime: The Example of Check Forgeries." In R.V. Clarke (ed.), S*ituational Crime Prevention: Successful Case Studies*. 2nd ed. N.Y.: Harrow and Heston.

Lacoste, Julie and Pierre Tremblay (2003). Crime innovation: A script analysis of patterns in check forgery. *Crime Prevention Studies* 16: 171–198.

Laycock, G., and N. Tilley (1995). *Policing and Neighborhood Watch: Strategic Issues*. Policy Research Series, Paper 60. London: Home Office.

Levi, M. (2000). "The Prevention of Plastic and Check Fraud: A Briefing Paper." London: Home Office Research, Development, and Statistics Directorate.

——— (1998). "Organising Plastic Fraud: Enterprise Criminals and the Sidestepping of Fraud Prevention." *The Howard Journal* 37(4):423–438.

Levi, M., P. Bissell, and T. Richardson (1991). *The Prevention of Check and Credit Card Fraud*. Crime Prevention Unit, Paper 26. London: Home Office.

Levi, M., and J. Handley (n.d.). *Criminal Justice and the Future of Payment Card Fraud*. London: IPPR Criminal Justice Forum.

——— (1998a). *The Prevention of Plastic and Check Fraud Revisited*. Research Study 182. London: Home Office Research, Development, and Statistics Directorate.

——— (1998b). *Prevention of Plastic Card Fraud*. Crime Prevention Unit, Paper 71. London: Home Office.

Mann, R. (2002). "Credit Cards and Debit Cards in the United States and Japan." *Vanderbilt Law Review* 55(4):1055–1108.

Maremont, M. (1995). "A Magnetic Mug Shot on Your Credit Card?" *Business Week*, April 24, p. 58.

Masuda, B. (1996). "An Alternative Approach to the Credit Card Fraud Problem." *Security Journal* 7(1):15–21.

Mativat, F., and P. Tremblay (1997). "Counterfeiting Credit Cards: Displacement Effects, Suitable Offenders, and Crime Wave Patterns." *British Journal of Criminology* 37(2):165–183.

McKinnon, A., and D. Tallam (2002). *New Crime Threats from Ecommerce: Theft in the Home Delivery Channel.* Foresight Panel Crime Prevention Programme. London: Home Office: www.foresight.gov.uk/index.html.

Newman, G., and R. Clarke (2003). *Superhighway Robbery: Preventing Ecommerce Crime.* London: Willan.

Newton, J. (1994). *Police Research Award Scheme: Organized "Plastic" Counterfeiting.* London: Home Office Police Department.

Painter, K., and N. Tilley (eds.) (1999). *Surveillance of Public Space: CCTV, Street Lighting, and Crime Prevention. Crime Prevention Studies,* Vol. 10. Monsey, N.Y.: Criminal Justice Press.

Pierce, C. (2003). *The Professional's Guide to CCTF Manual.*: www.ltctrainingcntr.com/.

Sampson, R. (2002). *Acquaintance Rape of College Students, Problem-Specific Guide No. 17.* Problem-Oriented Guides for Police Series. Washington, D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice.

Scott, M. (2001). *Robbery at Automated Teller Machines, Problem-Specific Guide No. 8*. Problem-Oriented Guides for Police Series. Washington, D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice.

Scottsdale Police Department (1995). "A Team Approach to Saving the Check Fraud Bureau From Fiscal Elimination." Submission for the Herman Goldstein Award for Excellence in Problem-Oriented Policing. Center for Problem-oriented Policing: www.popcenter.org/Library/Goldstein/1995/95-80.pdf.

Smith, R. (1997). "Plastic Card Fraud." *Trends and Issues in Crime and Criminal Justice*, No. 71. Canberra, Australia: Australian Institute of Criminology.

Sutton, M. (1995). "Supply by Theft: Does the Market for Stolen Goods Play a Role in Keeping Crime Figures High?" *British Journal of Criminology* 35(3):400–416.

Taylor, N. (2002). "Reporting of Crime Against Small Retail Businesses." *Trends and Issues in Crime and Criminal Justice*, No. 242. Canberra, Australia: Australian Institute of Criminology.

Texas Banking (2001). "Thumbprint Signature Program Fights Check Fraud." *Texas Banking* 40(1):9.

U.S. Comptroller of the Currency (1999). *Check Fraud: A Guide to Avoiding Losses*. Washington, D.C.: U.S. Comptroller of the Currency: www.occ.treas.gov/pubs1.htm.

U.S. General Accounting Office (2002). *Identity Theft: Prevalence and Cost Appear to Be Growing.* GAO-02-363 March. Washington, D.C.: U.S. General Accounting Office: www.consumer.gov/idtheft/reports/gao-d02363.pdf.

U.S. House (1998). *Identity Theft and Assumption Deterrence Act of 1998*. 105th Cong., 2nd sess., H.R. 4151.

——— (1997). Committee on Banking and Financial Services. Subcommittee on Domestic and International Monetary Policy. *Computer-Generated Check Fraud.* Washington, D.C.: U.S. Government Printing Office.

Webb, B. (1996). "Preventing Plastic Card Fraud in the UK." *Security Journal* 7(1):23.

About the Author

Graeme R. Newman

Graeme R. Newman is a distinguished teaching professor at the School of Criminal Justice, University at Albany, State University of New York. He has published works in the fields of the history and philosophy of punishment, comparative criminal justice, private security, situational crime prevention, and ecommerce crime, and has written commercial software. He was the CEO of a publishing company for 15 years and, in 1990, established the United Nations Crime and Justice Information Network. Among the books he has written or edited are *Superhighway Robbery: Preventing Ecommerce Crime* (with Ronald V. Clarke), and *Rational Choice and Situational Crime Prevention* (with Ronald V. Clarke and Shlomo Shoham).

Recommended Readings

- ***A Police Guide to Surveying Citizens and Their Environments***, Bureau of Justice Assistance, 1993. This guide offers a practical introduction for police practitioners to two types of surveys that police find useful: surveying public opinion and surveying the physical environment. It provides guidance on whether and how to conduct cost-effective surveys.

- ***Assessing Responses to Problems: An Introductory Guide for Police Problem-Solvers***, by John E. Eck (U.S. Department of Justice, Office of Community Oriented Policing Services, 2001). This guide is a companion to the *Problem-Oriented Guides for Police* series. It provides basic guidance to measuring and assessing problem-oriented policing efforts.

- ***Conducting Community Surveys***, by Deborah Weisel (Bureau of Justice Statistics and Office of Community Oriented Policing Services, 1999). This guide, along with accompanying computer software, provides practical, basic pointers for police in conducting community surveys. The document is also available at www.ojp.usdoj.gov/bjs.

- ***Crime Prevention Studies***, edited by Ronald V. Clarke (Criminal Justice Press, 1993, et seq.). This is a series of volumes of applied and theoretical research on reducing opportunities for crime. Many chapters are evaluations of initiatives to reduce specific crime and disorder problems.

- ***Excellence in Problem-Oriented Policing: The 1999 Herman Goldstein Award Winners.*** This document produced by the National Institute of Justice in collaboration with the Office of Community Oriented Policing Services and the Police Executive Research Forum provides detailed reports of the best submissions to the annual award program that recognizes exemplary problem-oriented responses to various community problems. A similar publication is available for the award winners from subsequent years. The documents are also available at www.ojp.usdoj.gov/nij.

- ***Not Rocket Science? Problem-Solving and Crime Reduction***, by Tim Read and Nick Tilley (Home Office Crime Reduction Research Series, 2000). Identifies and describes the factors that make problem-solving effective or ineffective as it is being practiced in police forces in England and Wales.

- ***Opportunity Makes the Thief: Practical Theory for Crime Prevention***, by Marcus Felson and Ronald V. Clarke (Home Office Police Research Series, Paper No. 98, 1998). Explains how crime theories such as routine activity theory, rational choice theory and crime pattern theory have practical implications for the police in their efforts to prevent crime.

- ***Problem Analysis in Policing***, by Rachel Boba (Police Foundation, 2003). Introduces and defines problem analysis and provides guidance on how problem analysis can be integrated and institutionalized into modern policing practices.

- ***Problem-Oriented Policing***, by Herman Goldstein (McGraw-Hill, 1990, and Temple University Press, 1990). Explains the principles and methods of problem-oriented policing, provides examples of it in practice, and discusses how a police agency can implement the concept.

- ***Problem-Oriented Policing and Crime Prevention***, by Anthony A. Braga (Criminal Justice Press, 2003). Provides a through review of significant policing research about problem places, high-activity offenders, and repeat victims, with a focus on the applicability of those findings to problem-oriented policing. Explains how police departments can facilitate problem-oriented policing by improving crime analysis, measuring performance, and securing productive partnerships.

- ***Problem-Oriented Policing: Reflections on the First 20 Years***, by Michael S. Scott (U.S. Department of Justice, Office of Community Oriented Policing Services, 2000). Describes how the most critical elements of Herman Goldstein's problem-oriented policing model have developed in practice over its 20-year history, and proposes future directions for problem-oriented policing. The report is also available at www.cops.usdoj.gov.

- ***Problem-Solving: Problem-Oriented Policing in Newport News,*** by John E. Eck and William Spelman (Police Executive Research Forum, 1987). Explains the rationale behind problem-oriented policing and the problem-solving process, and provides examples of effective problem-solving in one agency.

- ***Problem-Solving Tips: A Guide to Reducing Crime and Disorder Through Problem-Solving Partnerships*** by Karin Schmerler, Matt Perkins, Scott Phillips, Tammy Rinehart and Meg Townsend. (U.S. Department of Justice, Office of Community Oriented Policing Services, 1998) (also available at www.cops.usdoj.gov). Provides a brief introduction to problem-solving, basic information on the SARA model and detailed suggestions about the problem-solving process.

- ***Situational Crime Prevention: Successful Case Studies***, Second Edition, edited by Ronald V. Clarke (Harrow and Heston, 1997). Explains the principles and methods of situational crime prevention, and presents over 20 case studies of effective crime prevention initiatives.

- ***Tackling Crime and Other Public-Safety Problems: Case Studies in Problem-Solving***, by Rana Sampson and Michael S. Scott (U.S. Department of Justice, Office of Community Oriented Policing Services, 2000) (also available at www.cops.usdoj.gov). Presents case studies of effective police problem-solving on 18 types of crime and disorder problems.

- ***Using Analysis for Problem-Solving: A Guidebook for Law Enforcement***, by Timothy S. Bynum (U.S. Department of Justice, Office of Community Oriented Policing Services, 2001). Provides an introduction for police to analyzing problems within the context of problem-oriented policing.

- ***Using Research: A Primer for Law Enforcement Managers***, Second Edition, by John E. Eck and Nancy G. LaVigne (Police Executive Research Forum, 1994). Explains many of the basics of research as it applies to police management and problem-solving.

Other Problem-Oriented Guides for Police

Problem-Specific Guides series:

1. **Assaults in and Around Bars.** Michael S. Scott. 2001. ISBN: 1-932582-00-2
2. **Street Prostitution.** Michael S. Scott. 2001. ISBN: 1-932582-01-0
3. **Speeding in Residential Areas.** Michael S. Scott. 2001. ISBN: 1-932582-02-9
4. **Drug Dealing in Privately Owned Apartment Complexes**. Rana Sampson. 2001. ISBN: 1-932582-03-7
5. **False Burglar Alarms.** Rana Sampson. 2001. ISBN: 1-932582-04-5
6. **Disorderly Youth in Public Places.** Michael S. Scott. 2001. ISBN: 1-932582-05-3
7. **Loud Car Stereos.** Michael S. Scott. 2001. ISBN: 1-932582-06-1
8. **Robbery at Automated Teller Machines.** Michael S. Scott. 2001. ISBN: 1-932582-07-X
9. **Graffiti.** Deborah Lamm Weisel. 2002. ISBN: 1-932582-08-8
10. **Thefts of and From Cars in Parking Facilities.** Ronald V. Clarke. 2002. ISBN: 1-932582-09-6
11. **Shoplifting.** Ronald V. Clarke. 2002. ISBN: 1-932582-10-X
12. **Bullying in Schools.** Rana Sampson. 2002. ISBN: 1-932582-11-8
13. **Panhandling.** Michael S. Scott. 2002. ISBN: 1-932582-12-6
14. **Rave Parties.** Michael S. Scott. 2002. ISBN: 1-932582-13-4
15. **Burglary of Retail Establishments.** Ronald V. Clarke. 2002. ISBN: 1-932582-14-2
16. **Clandestine Drug Labs.** Michael S. Scott. 2002. ISBN: 1-932582-15-0
17. **Acquaintance Rape of College Students.** Rana Sampson. 2002. ISBN: 1-932582-16-9
18. **Burglary of Single-Family Houses.** Deborah Lamm Weisel. 2002. ISBN: 1-932582-17-7
19. **Misuse and Abuse of 911.** Rana Sampson. 2002. ISBN: 1-932582-18-5
20. **Financial Crimes Against the Elderly.** Kelly Dedel Johnson. 2003. ISBN: 1-932582-22-3
21. **Check and Card Fraud.** Graeme R. Newman. 2003. ISBN: 1-932582-27-4

Response Guides series:

- **The Benefits and Consequences of Police Crackdowns.** Michael S. Scott. 2003. ISBN: 1-932582-24-X

Problem-Solving Tools series:

- **Assessing Responses to Problems: An Introductory Guide for Police Problem-Solvers.** John E. Eck. 2002. ISBN: 1-932582-19-3

Upcoming Problem-Oriented Guides for Police (2003)

Problem-Specific Guides
Crimes Against Tourists
Disorder at Budget Motels
Domestic Violence
Gun Violence Among Serious Young Offenders
Mentally Ill Persons
Prescription Fraud
Robbery of Taxi Drivers
Stalking
Student Party Disturbances on College Campuses

Problem-Solving Tools
Repeat Victimization
Using Offender Interviews to Inform Police Problem-Solving

Response Guides
Closing Streets and Alleys to Reduce Crime

Future Guide Topics (2004)

Identity Theft
School Break-Ins
Street Racing
Bomb Threats
Problem Drinking Among Young People
Open-air Drug Markets
Sexual Activity in Public Places
Drunk Driving
Cruising
Bank Robbery

Other Related COPS Office Publications

- **Using Analysis for Problem-Solving: A Guidebook for Law Enforcement.** Timothy S. Bynum.
- **Problem-Oriented Policing: Reflections on the First 20 Years.** Michael S. Scott. 2001.
- **Tackling Crime and Other Public-Safety Problems: Case Studies in Problem-Solving.** Rana Sampson and Michael S. Scott. 2000.
- **Community Policing, Community Justice, and Restorative Justice: Exploring the Links for the Delivery of a Balanced Approach to Public Safety.** Caroline G. Nicholl. 1999.
- **Toolbox for Implementing Restorative Justice and Advancing Community Policing.** Caroline G. Nicholl. 2000.
- **Problem-Solving Tips: A Guide to Reducing Crime and Disorder Through Problem-Solving Partnerships.** Karin Schmerler, Matt Perkins, Scott Phillips, Tammy Rinehart and Meg Townsend. 1998.

- **Bringing Victims into Community Policing.** The National Center for Victims of Crime and the Police Foundation. 2002.
- **Call Management and Community Policing.** Tom McEwen, Deborah Spence, Russell Wolff, Julie Wartell and Barbara Webster. 2003.
- **Crime Analysis in America.** Timothy C. O'Shea and Keith Nicholls. 2003.
- **Problem Analysis in Policing.** Rachel Boba. 2003.
- **Reducing Theft at Construction Sites: Lessons From a Problem-Oriented Project.** Ronald V. Clarke and Herman Goldstein. 2003.
- **The COPS Collaboration Toolkit: How to Build, Fix, and Sustain Productive Partnerships.** Gwen O. Briscoe, Anna T. Laszlo and Tammy A. Rinehart. 2001.
- **The Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!).** Kelly J. Harris and William H. Romesburg. 2002.
- **Theft From Cars in Center City Parking Facilities - A Case Study.** Ronald V. Clarke and Herman Goldstein. 2003.

For more information about the *Problem-Oriented Guides for Police* series and other COPS Office publications, please call the Department of Justice Response Center at 800.421.6770 or visit COPS Online at www.cops.usdoj.gov.

For More Information:

U.S. Department of Justice
Office of Community Oriented Policing Services
1100 Vermont Avenue, N.W.
Washington, D.C. 20530

To obtain details on COPS programs, call the
U.S. Department of Justice Response Center at 800.421.6770

Visit COPS Online at the address listed below.

e09032049 Updated Date: September 30, 2003
ISBN: 1-932582-27-4

www.cops.usdoj.gov