Problem-Oriented Guides for Police
Problem-Specific Guide Series
No. 23

Check and Card Fraud, 2nd Edition

Graeme R. Newman and Jessica Herbert

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.

Contents

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 to intermediate level: requires photocopier or personal computer with standard color printer; printing clarity may vary with watermarks, special inks and other security features	Entry level: amateur alterations easily detectable; more advanced card alteration or production requires 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 require ID and may ask for additional security (e.g., fingerprint) measures	Additional ID rarely requested
Signature Checking	Signature rarely checked, unless check-cashing card required	Signature present on card is primary means of verifying card user, not always verified with additional ID
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,	Negotiable: merchant may

	Check	Card
	merchant carries loss and must recoup it from customer; legitimate account owner may be liable, depending on bank policy	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 2009, financial theft researchers reported a 22% increase in financial fraud crimes from the previous year, affecting approximately 9.9 million Americans.[1] Costing consumers an estimated $50 billion annually, the complexities of keeping information secure in a digital world has prevented law enforcement and private businesses from getting a grasp of fraud offenses.[2]

The increase of mobile banking has contributed to this increase of offenses. For check fraud, the increased use of remote deposit capture (RDC) increases vulnerabilities for financial institutions by allowing instantaneous transactions. Financial institutions reported a 400% increase of check fraud through RDC from 2012 to 2014.[3]

For card theft specifically, approximately 40% of victims of financial loss due to fraud reported in 2014 knowing how their personal information or cards were compromised.[4] This is consistent with other fraudulent reporting by researchers and private businesses that approximately 70% of identity theft resulting in financial losses occurs by insiders (e.g., persons with legal access to identifying information).[5] The volume and variety of scams to obtain a person's financial information (e.g., phishing, charity scams) further perpetuates the collections and exploitation of financial accounts.

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.[a] 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.[6]

[a] 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).

- **Identity theft.** There is increasing evidence to suggest that obtaining or accessing credit card or bank accounts are the main motive for identity theft.[b] In 2014, the Bureau of Justice Statistics identified over 15 million persons victimized by identity theft, with a mean loss of $1,090 per event.[7] A majority of these events – 86 percent – were for existing credit or bank cards. Although technology has made the counterfeiting of checks and plastic cards much more difficult over the last decade, the access to tools to recreate these payment mechanism is readily available through online purchasing and in-home printers.
- **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.[c]
- **Pickpocketing.** Pickpockets may be attracted to shopping malls and other crowded 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. Online vendors that offer cash outs for store cards or reloadable cards further assist for cash conversions.
- **Cyber-theft.** Customer databases that include credit card and other personal information are very valuable to cyber hackers. They have therefore become targets for hackers. Cyberattacks for financial information has turned to be a costly crime for financial industries and businesses. The loss of personal and financial information from Target, Home Depot, Aetna and the federal Office of Personnel Management has been estimated over $450 million in loss protections, network defense mitigation and insurances.[8]
- **Extortion.** The permeation of Internet use by individuals has increased victimization through extortion or ransomware techniques. Under the guise that personal information is being kept locked until payment is provided, cyber-thieves willing receive financial information and personal details from victims to "release" information.[9]
- **Organized crime.** Counterfeiting and marketing cards requires little costs, for both production and distribution, and midlevel organization among rings of offenders to execute fraudulent activities. There are two groups that operate here: 1) Organized hacking rings that procure personal and/or financial information and sell this information for profit and 2) Organized theft rings, or carders, who use this information to produce counterfeit cards and fraudulent transactions in either physical or virtual sales in retail stores, or within ATM and bank transactions. These organized rings vary by region of the world[10], although the United States hosts a significant number of carding organized rings.[11] In 2013, eight offenders were charged in New York with stealing $45 million from banks through the use of fraudulent ATM cards.[12] In 2014, a Georgia man was one of six persons indicted for $50 million theft from stolen credit card data.[13]

---

[b] 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%

[c] 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).

- **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.
- **Cons and scams.**[14] 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. Phishing scams and corporate email takeovers are key cyber techniques that solicit personal and financial information from unsuspecting victims. 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).[15] Point of sale fraud accounted for approximately $6 billion in losses from retail stores in 2014.[16]
- **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 has continued to evolve. Issuers now offer both debit and credit services on one card, with all cards having encrypted chip technology, requiring a personal identification number (PIN) for each transaction. Paperless or electronic checks are increasingly used in business-to-business transactions, as well as monthly payments for individual expenses (e.g., rent or mortgage, car payments). 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., debit cards) without actually *acquiring* the cards (e.g., by stealing account numbers).

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.[d]

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

- 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). PINs can also be obtained through placement of cameras near ATMs or other point-of-sale devices to capture images during transactions. This is common in ATM skimming operations.
- 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, either in spoofing or ransomware techniques, that request credit card and other personal information.

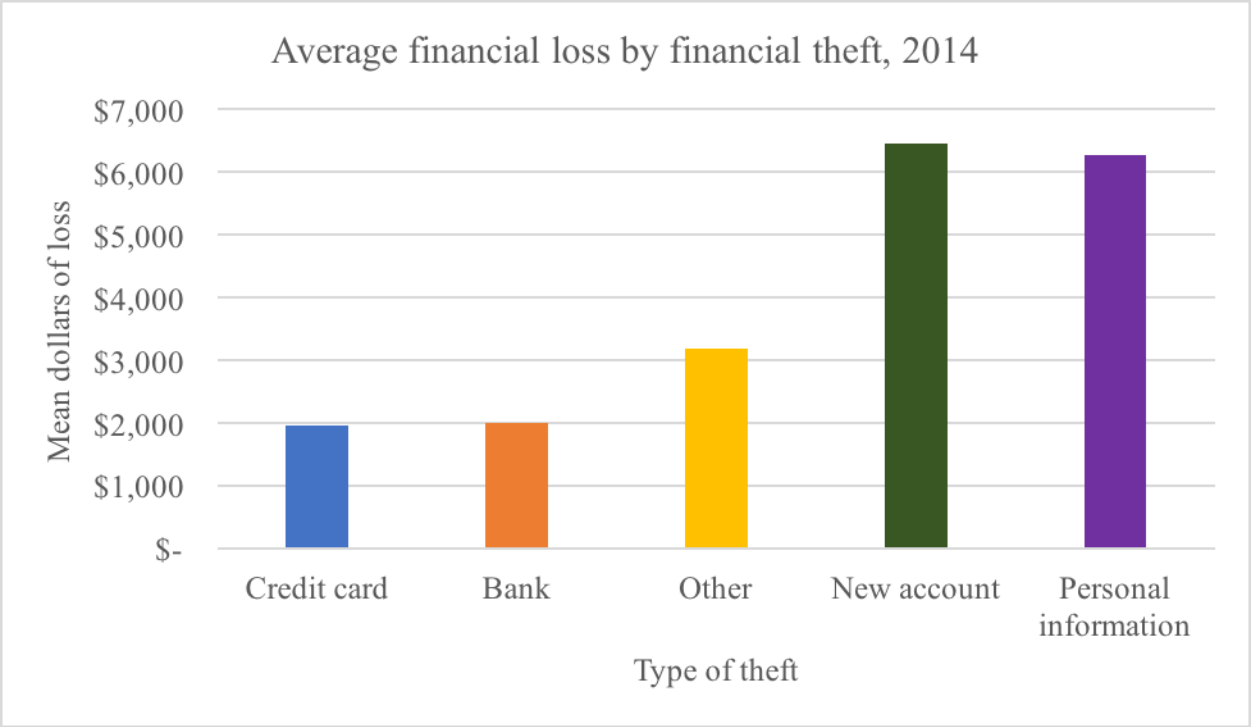
Illegal Use of Checks and Cards

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 businesses, 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.[17]
- 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.[18]
- Targeting ATMs for cash withdrawals. Counterfeit cards can be used for routine cash withdrawals, sometimes moving to several ATMs to maximize amount of withdrawal.[e] More sophisticated theft rings may adapt the information on the magnetic strip, which affects the operating system of the ATM and may allow for unlimited cash to be withdrawn from corresponding accounts.

[e] Although banks have limits on daily cash withdrawals, the use of multiple cards/accounts make ATM cash thefts attractive to many organized rings.

Figure 1. Average financial loss by theft type, 2014[19]



Low Reporting of Check and Card Fraud

Perhaps the biggest problem for police is that people rarely report check and card fraud to them.[f] In one recent study, only one in four incidents of check and card fraud were reported to the police.[20] 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. With the increase of offenses, and the fear of being victimized again by account holders with fraudulent claims, banking institutions commonly request for victims of card fraud to file a report with local police. Some police departments capture these reports as a courtesy report for insurance purposes, rather than criminal events, which may minimize departmental awareness of fraud trends. 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 or reputation.[21] 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.[22]

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

[f] 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).

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.[23] 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.[24]

Banks, some retail stores, and supermarket chains commonly prefer to deal with merchandise loss, employee theft, shoplifting, and check and card fraud internally.[25] 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 a majority of check and card fraud is due to factors beyond police control. Such factors include the following:

- 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).[g]
- Information about counterfeiting, skimming, and hacking is now widely available on the Internet. Thus, it is easier to commit card fraud than ever before.[26]
- 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. These differences are largely related to the structure of financial service markets in the various countries.

[g] 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.

- The amount of card fraud committed internationally has substantially increased in recent years. While the implementation of EMV technologies in Europe around 2004 slowed point-of-sale card fraud, the influx of online shopping and transactions has made consumers vulnerable through computer hacking techniques which obtain financial and personally identifying information. The United States move to EMV technologies for both credit and debit cards may impact point of sale, but the online sales are likely to still be vulnerable.
- 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."[27] 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.
- 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. Some 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.[28] Other groups stem from South America and Russian, primarily due to computer hacking skills aimed at the exfiltration of personal and financial information. The organized groups recruit "droppers", complicit criminals, or unsuspecting persons to assist in the sale of fraudulently purchased goods in order to gain cash.
- 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. This has shifted as the rate of card fraud has increased with technological access to fraudulent purchases. Card issuers have agreed to implement high security at point-of-sale (e.g., EMV technology, PIN requirements) to decrease the amount of loss incurred.

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 the offenses being committed at the same or similar businesses (e.g., small, local businesses, large retailers)? If so, what are the policies of the business that manage transactions? What are the protections the business has in place to verify checks or cards?
- 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?
- Is a specific bank, or ATM, being targeted for thefts? Is a specific retailer the common element in retail fraud purchases?

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.)

- 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?[h]
- What tools do the offenders use or have access to (e.g., skimmers, network scanning at open cafes)?

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 information do they collect on the fraud? 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 information are the corresponding banks collecting on the fraud activity? Do they have a Financial Investigation Unit that can assist local police with addressing the issue? What procedures do they have for detecting or preventing fraud among their customers? Do they have information or notices that can assist with education of consumers and businesses?
- 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?

[h] 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).

- 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)?
- Are there temporal patterns of check and card fraud? These may change due to time of year (e.g., tax return check fraud, increased card fraud at holiday season) and can assist you in focusing efforts to manage potential crime.

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)[29]
- 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.[30] Other studies have found that fraudsters tend not to switch easily *between* different types of credit card fraud[31] though they are resourceful in shifting between different types of check fraud, or at least in inventing new ways to commit check fraud.[32]
- 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, most measures used against check and card fraud have been swiftly met with alternatives, particularly with the pace of technology. For example, ATMs were placed within office lobbies or other enclosed spaces to protect against robberies. However, these physical barriers did not prevent thefts, as fraudsters use skimmers and cameras to capture card information, or manipulate the magnetic strip of the card to increase withdrawal amounts. Regardless, the pace of these changes have rarely been evaluated for effectiveness, although institutions have reported lower rates of check or card fraud after implementation.

The government has funded little research in this field, generally regarding it as the private sector's domain. The private sector has focused on this issue due to the frequency and amount of loss stemming from cyber-attacks and methods.

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.[33]

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.[34] 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.[i] 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)
- Coordinate services by a local security company, or fraud protection company, to offer discounts to local retailers on products that assist in antifraud procedures
- Enlist the support of the local Chamber of Commerce or other business organizations in persuading business owners to improve security
- 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.[j] All parties concerned must be convinced of their responsibility:

- Merchants and bankers: to adopt antifraud procedures
- Card issuers: to adopt marketing techniques that do not offer opportunities to potential fraudsters
- Customers: to take security precautions with their cards (e.g., understanding secure online purchases, awareness of common scams to obtain card information).

[i] 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.

[j] 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.

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. Most financial institutions require consumers to file a police report of the incident for record; however, it is important for the police department to treat this as a crime, not just a courtesy or non-victim offense. Capturing specific details about the offenses (e.g., time(s) of offense, method detected, type of card, financial institution, quantity of loss, location of purchase) can assist in identifying specific preventive efforts for action, rather than merely adding information to police records. You must also consider a strategic communication plan to handle perceptions of merchant reputations and increased reporting of fraud. Unless there is an active and positive program linked to reporting fraud, negative publicity can easily ensue.[35]

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.[36] 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, 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 person offering the check or card is the account holder. Sales clerks typically do this by checking the customer's signature or another form of identification. 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.
- Limit the amount of sale allowed by check. Small businesses can be an attractive target for fraudsters, yet the financial loss (regardless of actual dollar amount) can significantly impact business. Restricting the amount of a sale by a personal check can deter a fraudster and minimize any potential loses.

Researchers have shown that adding simple security procedures can significantly reduce check and card fraud. In one U.S. study in a retail store,[37] 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[38] showed that legislation requiring people to show two forms of ID when cashing checks reduced check fraud by over 80 percent.[k]

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.

The recent implementation of EMV card technology within the United States may also impact the perceptions of merchants and consumers. It should be noted that will the transmission of the financial transaction is encrypted, this does not prevent against fraudulent use of cards. The EMV technology encrypts the transmission of the consumer's information, merchants' information and bank information, which is intended to protect against cyberattacks and data exfiltration attempts by hackers. While the replication of an EMV card is more difficult for fraudsters, the technology has been replicated in fraudulent cards and other alterations to the card technology has been used to allow sales or ATM withdrawals to occur.[39]

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.[l]

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. Both the introduction of PINs and biometric techniques have shown initial impacts to point of sale fraud transactions; however, the endurance of these programs by merchants, or the consistency among checkout staff over time, varies and can allow fraud to occur.[40]

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

[k] 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).

[l] 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.

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.[41]
- 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.
- Encourage collaboration between local businesses, regional financial institutions or banking groups and information security groups to ensure there is a local focus and communication on fraudulent trends and vulnerabilities (e.g., Association of Certified Anti-Money Laundering Specialists (ACAMS), Association of Certified Financial Crime Specialists (ACFCS), information security meetings).

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.[m]

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.[42] 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.)

[m] 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.).

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/

Association of Certified Financial Crime Specialists: https://www.acfcs.org/

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 Cyber Crime information page: https://www.fbi.gov/investigate/cyber or White Collar Crime information page: https://www.fbi.gov/investigate/white-collar-crime

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/

Financial Fraud Enforcement Task Force: https://www.stopfraud.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,[n] but also errant merchant processing. Stores that issue check-cashing cards could also use this service.

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 common for retail and other business, and it is certainly at the operational core of USPS, 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),[43] vehicles (including delivery vehicles),[44] 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.[45] Because of the massive increase in online retailing, many more products are delivered to the home, creating opportunities for theft during shipping. 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.[46]

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

- Fraudsters claiming non-delivery 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 non-delivery 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.[47] 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.[48] 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 cameras 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 "https" in the URL, to include the green padlock emblem on all pages, to ensure your transaction is encrypted and secure
- Never leaving credit or bankcards in a vehicle, whether locked or unlocked (these are among the most common items stolen from cars)[49]
- Never letting anyone (including family members) use your debit or credit card, or know your PIN

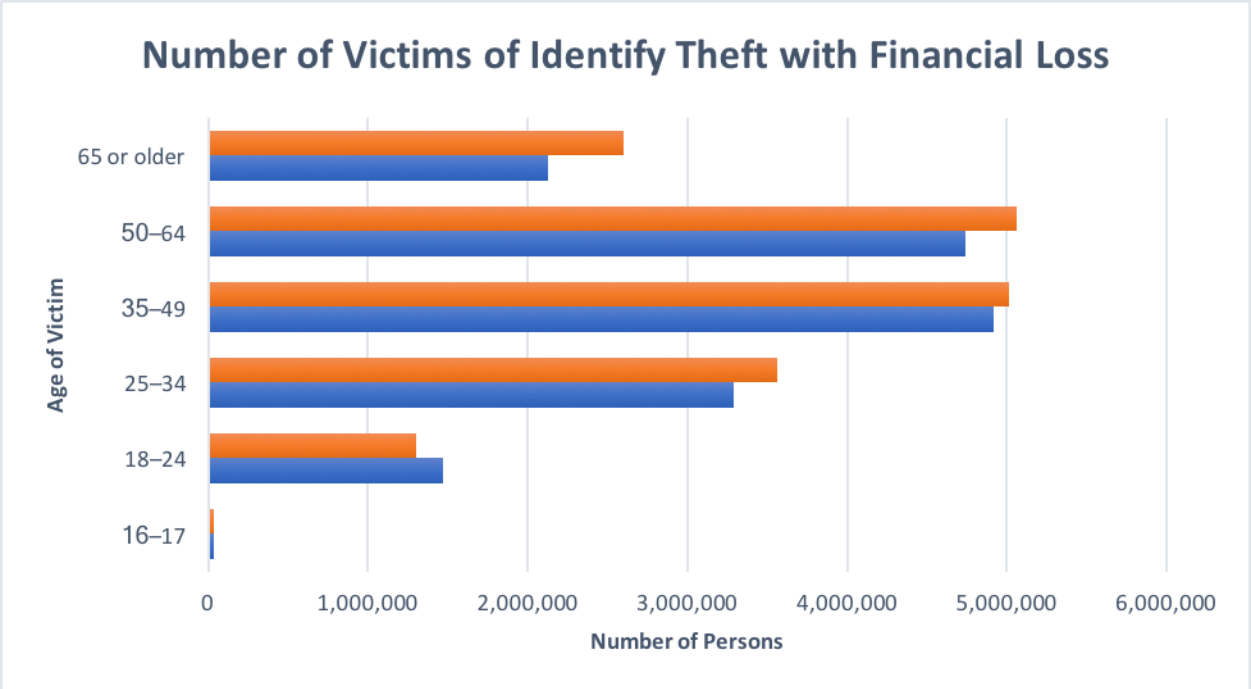
- Watching carefully how sales clerks process your credit card and, if the store still uses mechanical card-processing devices, making sure that copies of receipts are destroyed
- Not using publicly accessible computers (e.g., in libraries or Internet cafes) to make online purchases, because hackers may 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 have taken proactive steps to inform their residents through websites, social media (e.g., Twitter, NextDoor) or newsletters.[50] While past programs have focused on senior citizens, or youth/young adults, the majority of card fraud occurs among people ages 25 to 64 years of age (see Figure 2).[51] Here are some strategies for increasing awareness among groups within your community:

- Set up educational programs to give talks to senior citizen groups and high school students about fraud trends and how they can protect themselves
- Work with local universities to push out fraud awareness campaigns among students (particularly during campus events that solicit students to get credit cards)
- Hold information sessions at local recreation centers or athletic clubs to reach adults that may otherwise not attend other community held events.

Of course, the effectiveness of these programs will be difficult to measure, since it requires a broad approach directed at affecting future behavior.

Figure 2. Victims of at least one identity theft incident with financial loss in 2012 and 2014[52]



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).[53] 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?[54] 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 or social media outlets, which tend to be very interested in reporting on crime victims.[55] 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.[56] 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.[57] 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,[58] 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.[59] 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. Local regulations for pawnshops and their collection of transaction data can assist investigations in identifying organized rings of fraudsters; however, the common use of pawn shop data bases (e.g., LeadsOnline, PawnMaster) in legitimate pawn shops may deter fraudsters. 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,[60] 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.

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 (e.g., 4chan, ICQ), bulletin boards, information posting websites (e.g., Pastebin.com, Backpage.com, Craig's List) and social media forums (e.g., YouTube, Facebook) where people discuss acquiring counterfeit or stolen cards, hacking into databases containing card information, and committing card fraud. 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.

Phishing, corporate account takeover and other email scams are a large entry point for fraudsters. In 2015, an Omaha, Nebraska commodity company lost $17 million as a result of an email scam among employees.[61] In 2016, the FBI reported multiple businesses fell victim to the "CEO Fraud" scam, resulting in a $2.3 billion-dollar loss across several businesses.[62] These scams change often, in order to further collect private information on individuals and businesses. Here are a few websites that track latest scams and inform consumers quickly with techniques and preventative measures:

- Fraudwatch International - https://fraudwatchinternational.com/
- Arstechnica - https://arstechnica.com/
- The Swiss Security Blog - https://www.abuse.ch/
- Dark Reading - http://www.darkreading.com/

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, local bank Financial Intelligence Units, and 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 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.[63] 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, or higher end stores for card fraud, and supermarkets for check fraud). Or they may target particular stores because they are considered "easy." Using crime mapping,[64] 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.[65] 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.[66] 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.[67] Nonprofit groups like the National Cyber-Forensics & Training Alliance (NCFTA) work with the FBI and private businesses to monitor Internet scams and network defenses to detect, deter and disrupt financial hackers and fraudsters. Their Cyber Financial Program focuses specifically on card fraud and methods to inform regional businesses of risks based on current trends (visit https://www.ncfta.net/ for more information or local contacts). The Financial Fraud Enforcement Task Force (www.stopfraud.gov) may also be of assistance in educating your community and reporting types of fraud trends in your region.

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,[o] 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.[68]

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.[69] 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.[70]

[o] 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*.

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		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		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 than an aid to planned preventive procedures
3		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		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

Response No.	Page No.	Response	How It Works	Works Best If…	Considerations
5		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		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
7		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		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		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		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		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		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		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		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		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		Conducting crackdowns	Police conduct very public, intensive campaigns to catch fraudsters		Merchants may fear that crackdowns will drive business away
17		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

Response No.	Page No.	Response	How It Works	Works Best If…	Considerations
18		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		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

References

Bureau of Justice Statistics. (2014). *National Crime Victimization Survey, Identify Theft Supplement.* Washington, DC.

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." *Trends 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.

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

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

Delamaire, L., H. Abdou, and J. Pointon (2009). "Credit Card Fraud and Detection Techniques: A Review." *Banks and Bank Systems,* 4(2), 57-68.

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.

Europol. (2012). "Situation Report: Payment Card Fraud in the European Union Perspective of Law Enforcement." Europol Public Information.

Evansville (Indiana) Police Department (n.d.). "Fraud Awareness." http://www.evansvillepolice.com/fraud_awareness, https://nextdoor.com/agency-post/nc/stallings/stallings-police-department/fraud-awareness-seminar-for-residents-and-citizens-45767428/. Accessed May 24, 2020.

Finklea, M. (2010). *Identify Theft: Trends and Issues*. Washington, D.C.: The Federation of American Scientists.

Gara, T. (2014). "An Expensive Hack Attack: Target's $148 million Breach." *The Wall Street Journal*. http://blogs.wsj.com/corporate-intelligence/2014/08/05/an-expensive-hack-attack-targets-148-million-breach/

Geuss, M. (2016). "An ATM Hack and a PIN-pad Hack Show Chip Cards Aren't Impervious to Fraud." *arsTechnica*. https://arstechnica.com/security/2016/08/an-atm-hack-and-a-pin-pad-hack-show-chip-cards-arent-impervious-to-fraud/

Glenny, M. (2011). *DarkMarket: Cyberthieves, Cybercops and You.* New York: Knopf Publishing.

Guardian Analytics (2016). "Fraud Update: Mobile RDC Trends." http://guardiananalytics.com/wp-content/uploads/2016/06/FraudUpdate_MobileRDCTrends_March2016.pdf

Harrington, E. (2015). "OPM Hack Costing Taxpayers $350 Million." *The Washington Free Beacon*. http://freebeacon.com/issues/opm-hack-costing-taxpayers-350-million/

Hedayati, A. (2012). "An Analysis of Identity Theft: Motives, Related Frauds, Techniques and Prevention." *Journal of Law and Conflict Resolution*, 4(1), 1-12.

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

Isidore, C. (2013). "8 Charged in $45 million Cybertheft Bank Heist." *CNN*. https://money.cnn.com/2013/05/09/technology/security/cyber-bank-heist/index.html

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

Johnston, C. (2015). "Company Loses $17m in Email Scam." *The Guardian*. https://www.theguardian.com/technology/2015/feb/05/company-loses-17m-in-email-scam

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

Krebs, B. (2016). "FBI: $2.3 Billion Lost to CEO Email Scams." Krebs on Security. https://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/

Lacoste, J., and P. Tremblay (2003). "Crime Innovation: A Script Analysis of Patterns in Check Forgery." In M. J. Smith and D. B. Cornish (eds.), *Theory for Practice in Situational Crime Prevention. Crime Prevention Studies*, Vol. 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.

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.

Musil, S. (2016). "Home Depot Offers $19M to Settle Customers' Hacking Lawsuit." *CNET Magazine*. https://www.cnet.com/news/home-depot-offers-19m-to-settle-customers-hacking-lawsuit/

Pegues, J. (2016). "Authorities Bust International Cyber Theft Ring that Helped Hack Computers." *CBS*. http://www.cbsnews.com/news/avalanche-network-international-cyber-theft-ring-busted-by-authorities/

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.

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/

Santora, M. (2013). "In Hours, Thieves Took $45 Million in ATM Scheme." *The New York Times*. http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?mcubz=0

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: http://www.popcenter.org/Library/Goldstein/1995/95-80.pdf.

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. Department of Justice. (2014). "Member of Organized Cybercrime Ring Responsible for $50 Million in Online Identify Theft Sentenced to 115 Months in Prison." Washington, D.C.: U.S. Department of Justice Office of Public Affairs. https://www.justice.gov/opa/pr/member-organized-cybercrime-ring-responsible-50-million-online-identity-theft-sentenced-115

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. http://www.consumer.gov/idtheft/reports/gao-d02363.pdf

Endnotes

[1] Hedayati, A. (2012).
[2] Finklea, M. (2010).
[3] Guardian Analytics (2016).
[4] Bureau of Justice Statistics (2014).
[5] Hedayati (2012).
[6] Levi (1998).
[7] Bureau of Justice Statistics (2014).
[8] Gara (2014); Harrington (2015); Musil (2016).
[9] Newman and Clarke (2003).
[10] Pegues (2016).
[11] Glenny (2011).
[12] Isidore (2013). See also Santora (2013).
[13] U.S. Department of Justice. (2014).
[14] Newman and Clarke (2003).
[15] Levi (2000).
[16] Javelin Strategy & Research (2014).
[17] Levi and Handley (1998a).
[18] Levi and Handley (1998b).
[19] Bureau of Justice Statistics (2014).
[20] Taylor (2002).
[21] Clarke and Newman (2002).
[22] Levi, Bissell, and Richardson (1991).
[23] Levi, Bissell, and Richardson (1991).
[24] Duncan (1995).
[25] Newman and Clarke (2003).
[26] Newman and Clarke (2003).
[27] Ekblom (2000).
[28] Mativat and Tremblay (1997).
[29] Scott (2001).
[30] Levi and Handley (n.d.).
[31] Mativat and Tremblay (1997).
[32] Lacoste and Tremblay (2003)
[33] Levi, Bissell, and Richardson (1991); Levi and Handley (1998a).
[34] Mativat and Tremblay (1997).
[35] Scottsdale Police Department (1995).
[36] Levi and Handley (n.d.).
[37] Masuda (1996).
[38] Knutsson and Kulhorn (1997).
[39] Geuss (2016).
[40] Texas Banking (2001); Delamaire, Abdou & Pointon (2009); Europol (2012); Hedayati (2012).
[41] Pierce (2003); Clarke (2001a); Painter and Tilley (1999).
[42] Levi and Handley (n.d.).
[43] DiLonardo (1996).
[44] McKinnon and Tallam (2002).
[45] Newman and Clarke (2003).
[46] McKinnon and Tallam (2002); Laycock and Tilley (1995).
[47] McKinnon and Tallam (2002).
[48] Clarke (1997); Clarke (2001b).
[49] Clarke (2001a).
[50] Evansville Police Department (n.d.).
[51] Bureau of Justice Statistics (2014).
[52] Bureau of Justice Statistics (2014).

[53] Clarke (1997).
[54] Levi and Handley (n.d.).
[55] Chermak (1995).
[56] CALPIRG (2000).
[57] Newman and Clarke (2003).
[58] Sampson (2002).
[59] Sutton (1995).
[60] Levi (2000); Mativat and Tremblay (1997).
[61] Johnston (2015).
[62] Krebs (2016).
[63] Levi, Bissel, and Richardson (1991).
[64] Eck and Weisburd (1995).
[65] Scottsdale Police Department (1995).
[66] Scottsdale Police Department (1995).
[67] Newton (1994); Mativat and Tremblay (1997).
[68] Charlton and Taylor (2003).
[69] Scottsdale Police Department (1995).
[70] Clarke (2001a).