



**Defending America  
Against Identity Crime**

**Identity Crime Toolkit  
for Police Executives**



In partnership with:  
**Bank of America** 

### International Association of Chiefs of Police

Founded in 1893, the International Association of Chiefs of Police is the world's oldest and largest association of law enforcement executives with more than 19,000 members in 93 countries. For more information, visit [www.theiacp.org](http://www.theiacp.org).

### Bank of America

Bank of America is one of the world's largest financial institutions, serving individual consumers, small and middle market businesses and large corporations with a full range of banking, investing, asset management and other financial and risk-management products and services. The company provides unmatched convenience in the United States, serving more than 54 million consumer and small business relationships with more than 5,700 retail banking offices, nearly 17,000 ATMs and award-winning online banking with more than 19.8 million active users. Bank of America is the No. 1 overall Small Business Administration (SBA) lender in the United States and the No. 1 SBA lender to minority-owned small businesses. The company serves clients in 175 countries and has relationships with 98 percent of the U.S. Fortune 500 companies and 79 percent of the Global Fortune 500. Bank of America Corporation stock (NYSE: BAC) is listed on the New York Stock Exchange. For more information, visit [www.bankofamerica.com](http://www.bankofamerica.com).

Identity crimes are among the fastest growing and most serious crimes affecting our citizens today. This toolkit will help law enforcement agencies make systemic changes, and ultimately, reduce victimizations by identity crimes.

## Table of Contents

I.	Introduction .....	2
II.	Executive Briefing .....	2
III.	Leadership and Management .....	4
	A. Assessment of Current Status .....	4
	B. Tools for Improving Effectiveness .....	6
	C. Further Information .....	7
IV.	Officer Training .....	8
	A. Assessment of Current Status .....	9
	B. Tools for Improving Effectiveness .....	10
	C. Further Information .....	11
V.	Agency Partnerships.....	12
	A. Assessment of Current Status .....	12
	B. Tools for Improving Effectiveness .....	13
	C. Further Information .....	14
VI.	Community Outreach .....	15
	A. Assessment of Current Status .....	15
	B. Tools for Improving Effectiveness .....	16
	C. Further Information .....	18
VII.	Attachments.....	19
	A. Sample Job Description for an Identity Crime Specialist .....	19
	B. Guidelines for Taking a Police Report on Identity Crime.....	20
	C. Guidelines for Helping Residents Affected by Identity Crimes .....	22
	D. Guidelines for Investigating Identity Crimes.....	23
	E. Checklist for Investigating Identity Crimes .....	24
	F. Typical Fraud Schemes .....	26
	G. Community Outreach Flyer.....	28



## I. Introduction

On October 17, 2006, the International Association of Chiefs of Police (IACP) and Bank of America (BAC) announced a three-year partnership to create a national strategy aimed at helping consumers and law enforcement understand and respond to identity crime.

Through joint efforts, the partnership hopes to raise citizen awareness of identity crimes, including guidance to prevent being victimized and steps to take when suspecting or experiencing identity crime. The strategy will also bolster law enforcement's expertise in responding to identity crime and conducting investigations.

The primary goal of the partnership is to educate both the public and law enforcement officials in the U.S. and abroad on ways to prevent and respond to identity crime.

As the first joint project, the partnership launched a Web site, [www.idsafety.org](http://www.idsafety.org), aimed at educating both consumers and law enforcement about identity crime. It marks the first time that the banking industry and law enforcement have come together to create a Web site to help consumers and law enforcement officials understand and respond to identity crime.

Recognizing the special challenges this type of crime poses for local law enforcement, the IACP has created this toolkit for police executives. This resource can be used in conjunction with those available on [www.idsafety.org](http://www.idsafety.org) to ensure that police leadership is able to meet these challenges head on.

## II. Executive Briefing

It is not news that the digital age has brought great change to every aspect of our lives. As always, change brings new forms of public safety risks and challenges. For many police departments, identity crimes are among those new, emerging types of crimes that are just beginning to show their impact on communities.

For police, these crimes are complex. Often the perpetrators live in another jurisdiction, and are not going to be arrested by the local law enforcement agency. But the victims are local. The victim's avenue to restoring his/her life to pre-crime status begins at his/her local police department, with the simple act of filing a police report.<sup>1</sup>

The fact that victims need to file a local police report to trigger the steps necessary to restore their names and credit requires that police departments across the country actively work to create a change in law enforcement attitudes about these kinds of crimes. Today, many police officers believe that they have no role in identity crime, or that victims should start their restoration with banks or credit companies. This is simply not possible.

**Police must be partners in preventing these crimes, and must be ready to take the report and help the victim in responding to them.** Police investigators also play a key role in identifying perpetrators, and police outreach can reduce overall victimization. But all of these important outcomes rely on police

<sup>1</sup> The Fair and Accurate Credit Transaction Act of 2003 (FACTA) added new sections to the federal Fair Credit Reporting Act (FCRA, 15 U.S.C. 1681 et seq.), intended primarily to help consumers fight identity crime. Accuracy, privacy, limits on information sharing, and new consumer rights to disclosure are included in FACTA. (Pub. L. 108-159, 111 Stat. 1952). FACTA requires victims of identity crime to have a police report to prove they are truly victims.

leadership to demonstrate to line officers that these crimes really do matter at the local level, and warrant the attention of the local law enforcement agency. This toolkit is intended to help you, as the chief executive of your agency, to lead that change in perceptions among officers.

In fact, identity crimes are among the fastest growing, and most serious, crimes affecting our citizens today. The impact of these crimes can be devastating, and the perpetrators may victimize many people in many places before they are even noticed, let alone apprehended. Making systemic changes that will improve identification, apprehension, and successful prosecution of identity criminals is essential to reducing victimization. This toolkit will help law enforcement agencies make such systemic changes, and ultimately, reduce victimizations by identity crimes.

These changes might include:

- **Assuming Leadership.** Police chiefs are uniquely positioned to influence the behavior of both crime-fighters and potential victims. By providing local level leadership that demonstrates the importance of preventing and responding to identity crime, police chiefs can significantly reduce victimizations in all of our communities.
- **Training Officers** on the pervasive nature of identity crimes; state and federal laws; how to spot other criminals who may have links to identity crimes; how to help victims; and how to investigate a crime effectively.
- **Creating Agency Partnerships** to enable collaboration with other law enforcement agencies, prosecutors' offices, the business community, and the public on prevention, investigation, and response.
- **Educating the Public** about how to avoid becoming a victim and how to respond at the first signs of becoming a victim of identity crime. Public education might, in some cases, include helping your legislature understand how to improve state laws to protect victims better and/or supporting your state associations in lobbying for legislative action on these crimes.

It is noteworthy that most departments will need to embrace a different way of thinking about crime when focusing on identity crime. The goal in investigating identity crimes must include restoring victims to their pre-crime status. Police have a central role in helping to do this, and without police participation, victims will be frustrated in their attempts to restore their good credit and their good names. Clearance rates, normally a central concern of police in investigating crimes, are less important in this arena for a variety of reasons, including that the arrest may well happen outside the police department's jurisdiction and also that identity crimes do not count against a jurisdiction's Unified Crime Reports (UCR) statistics<sup>2</sup>. For these reasons, it is critically important that cultural shifts occur in departments around this issue to prevent and investigate these crimes.

**The purpose of this toolkit is to help police leaders take the first steps in leading a change in police culture to expand the role of local law enforcement in preventing, investigating, and responding to identity crimes.**

<sup>2</sup> Currently 22 states, plus the District of Columbia, have laws mandating law enforcement agencies to take police reports from identity crime victims. Of these 22 states, seven also have language that explicitly states that such reports are not required to be counted as an open case file: Arkansas, Delaware, Georgia, Maryland, New Hampshire, New Jersey and North Carolina.



The toolkit is divided into four sections:

**Leadership and Management:** to help police executives become leaders of a cultural shift in policing

**Officer Training:** to help identify what training your officers need and where to get it

**Agency Partnerships:** to identify the key partners and how to connect with them

**Community Outreach:** to help you work with communities to reduce victimizations

Each section provides a brief introduction to the concepts covered, and then follows with a short self-assessment tool to help you determine your own agency's strengths and potential challenges or areas for improvement. Following the assessment tool, you will find additional resources or tools to help improve your agency's work in this area, and finally, a section with further information for additional research on topics which may be of particular interest.

### III. Leadership and Management

Police chiefs are in a tough position when it comes to addressing identity crimes in their jurisdictions. For one thing, the crime often begins elsewhere - the link to the local police department is simply that the victim resides there. In addition, identity crime is not as visible as street crime, and the local media rarely produce bold headlines which announce the rising rate of local victimization in identity crime, in effect, forcing departments to channel limited resources to those crimes drawing the most fervent public outcries.

The problem is that identity crimes affect more people each year in the United States than burglary and motor vehicle crimes combined<sup>3</sup>. Plus, the victims can lose a lifetime's worth of savings, their retirement plans, and their good names.

The purpose of this part of the toolkit is to help police executives examine and strengthen their departments' capacity to address identity crime.

#### A. Assessment of Current Status

**Identity crimes are extremely challenging for police to prevent and investigate.** Most departments are just beginning to identify how they can do so. Some of the challenges to overcome include these:

- Police are not aware of the importance of taking a report from a victim.
- Identity crimes are multi-jurisdictional, with locations including the victim's place of residence, the location of the bank or credit agencies affected, and the location of any secondary crimes, such as purchases with stolen credit cards.
- The crime is anonymous—there are no witnesses and no crime scene.
- There are multiple victims, including the person whose identity was stolen, the credit agency or bank who provided the credit, and merchants who sold goods or services to the identity criminal. Perpetrators of identity crime often have multiple victims in many locations.

<sup>3</sup> A 2003 Federal Trade Commission survey estimated that almost 10 million people in the United States were victims of identity crime during that year. Although many identity crimes go unreported, complaints to the Federal Trade Commission (FTC) have skyrocketed in the past few years (see Table 1).

- Businesses often have lax security measures regarding use of confidential customer information, and have not made a priority out of helping law enforcement during criminal investigations.
- Police officers lack experience in recovering and analyzing financial and electronic documents.

**How well is your department equipped to prevent, investigate, and respond to identity crimes?**

Use the Assessment Tool below to identify your current strengths and areas for improvement.

Departmental Capacity to Address Identity Crime: Questions	Yes	Somewhat	No	Not Sure
Do we know which officer(s) in this department are responsible for preventing, investigating, and responding to identity crimes?				
Do we provide officers with training on the prevention, investigation and response to identity crime?				
Are our officers aware of the growing risk of identity crime victimizations and the importance to top management that they take reports on these crimes?				
Are our officers aware of the importance of taking reports of identity crimes from all victims?				
Are our officers coding reports of identity crime in ways which are consistent with our overall policy on this topic?				
Do we provide sufficient information to victims to help them understand their next steps after reporting a case of identity crime?				
Do we utilize national resources/information sharing resources in investigating identity crimes?				
Are we engaged in any joint task forces related to identity crimes?				
Do we have a strategy for preventing identity crime?				
Do we have a way to measure our progress in learning to investigate and respond to identity crime?				

*To conduct an in-depth assessment, see "Understanding Your Local Problem," from Graeme R. Newman, "Identity Theft" Problem-Oriented Guides for Police, Problem-Specific Guides Series No. 25.*

*U.S. Department of Justice, Office of Community Oriented Policing Services. pp.21-28*

[www.popcenter.org/Problems/PDFs/Identity%20Theft.pdf](http://www.popcenter.org/Problems/PDFs/Identity%20Theft.pdf)



## B. Tools for Improving Effectiveness

When police executives are educated on the extent, methodologies, and criminals involved with identity crimes, it becomes possible to expand the capacity of local law enforcement to reduce victimization in the area of identity crime.

Despite the growing evidence that police departments can successfully increase arrest rates and reduce victimizations in their communities by working toward improved response to identity crime, it is still common for some officers within police departments to be resistant to adopting new practices in this area. In addition, community members, business leaders, and legislators may not be doing their part.

To successfully address identity crime, police leaders have to prioritize these crimes within the department and help all of the officers within the department come to a deeper understanding of their role in preventing and responding to these crimes. As noted, this is a difficult undertaking as the crime is much less visible than violent crime, is far less likely to be reported to police by victims, and is extremely difficult for police to investigate.

Given these hurdles, how can you let your officers know that this is a top priority? Here are some ways you can send the message.

### Allocate resources

- **Apply for grant funds** to strengthen your department's response. Check [www.ojp.usdoj.gov/funding](http://www.ojp.usdoj.gov/funding) regularly to identify new sources of funding from the Department of Justice, many of which provide support for prevention and response to identity crimes.
- **Provide training.** See Section III (Officer Training) of this workbook for some ideas on how to train your officers and your community members in prevention, investigation, and response to identity crime.
- **Allocate responsibility.** By designating particular individuals to have responsibility for improving the department's response to identity crime, you will be clearly stating that this problem is important and worthy of an investment of time and effort. See **Attachment A** for a sample job description for an Identity Crime Specialist.

### Develop Practices, Policies, and Procedures

- **Make sure that officers are taking reports from victims.** A police report is the baseline for any identity crime investigation. Victims of identity crime are required to file police reports to dispute fraudulent transactions, correct compromised records and accounts, and place fraud alerts. The report should be filed in his/her home jurisdiction, even when the precipitating incident (for example, a purse-snatching) happened elsewhere. See **Attachment B** for IACP guidelines on taking the report and what it should include.



- **Expand the investigative tools available to your officers.** The Federal Trade Commission (FTC) provides law enforcement agencies with secure online access to a database of consumer complaints dealing with fraud, called Consumer Sentinel. This helps investigators track patterns, work across jurisdictional lines, and identify clusters of victims. Registration is required but is free. Visit [www.ftc.gov/sentinel/cs\\_signup.pdf](http://www.ftc.gov/sentinel/cs_signup.pdf) to sign up.
- **Track the rate of identity crime victimizations in your jurisdiction.** If possible under state law, utilize the broad federal legislative definition of identity crime, until the UCR develops a formal definition for UCR purposes. Visit [www.idsafety.org](http://www.idsafety.org) and click on your state to read state legislation affecting your jurisdiction.

### C. Further Information

#### CASE STUDY: Beaverton, Oregon

The City of Beaverton, with 2.1M residents, is the fourth largest city in the Portland metropolitan area. To combat identity crime, the Beaverton Police Department (PD) began a multi-pronged approach in 2003 that has resulted in more than \$700,000 in loss prevention, 494 arrests and the recovery of more than \$33,000. Chief of Police David Bishop commented that "word on the street showed that Beaverton was no longer an easy target. Many criminals chose to go elsewhere to set up their schemes." What did Beaverton do to achieve these results? A few things that are replicable in other jurisdictions:

##### Got help.

Beaverton applied for and was awarded a federal grant (\$250,000) to infuse energy into the project.

**Figured out who would do the work.** The Beaverton PD created the Special Enforcement Unit (SEU), with one sergeant and two officers, to investigate street level identity crime and fraud crimes with a monetary value under \$5,000. SEU officers also provide

community education and collaborate with interagency fraud and narcotics task forces. Identity fraud cases with a monetary value greater than \$5,000 are investigated through an interagency task force described below.

##### Trained all officers.

Patrol officers received identity crime and fraud training to help shape their responses to victims across the board, learning to ask questions and offer advice which can prevent identity crime following other forms of crime, etc.

##### Worked with businesses.

Through presentations to the business community and proactive outreach to high-risk businesses such as large retailers, SEU asked businesses to improve security measures in order to reduce identity crime and fraud, and to report all fraudulent transactions.

For additional details, see The Police Chief May 2007 article by Beaverton Chief of Police David Bishop.

1. CASE STUDY: Beaverton, OR

2. The FACT Act [FACTA]

Visit [www.ftc.gov/os/statutes/031224fcra.pdf](http://www.ftc.gov/os/statutes/031224fcra.pdf), to see the entire text of the law.



#### IV. Officer Training

Police officers receive a lot of training - from the Academy to In-Services; there are always new skills and knowledge needed to keep ahead of the changes in crime trends. Identity crime poses new challenges in training, as technological advances come quickly and often offer new avenues for both the commission and the investigations of crimes.

Officer training in identity crime is difficult to provide because of the complexity and variety of identity crimes, and also because of the competing demands for police officers' time and attention to other crimes.

The appropriate level of training for your officers will vary depending on how much direct investigatory responsibility they have for identity crimes. However, it is important for all patrol officers, as the department's first responders, to have at least a basic understanding of identity crimes for two reasons:

- A) Understanding identity crime will help them understand the potential significance of street-level activity such as dumpster diving. In some states (check [www.idsafety.org](http://www.idsafety.org) and click on your state to see your state's identity crime laws), simply possessing another person's identity information is a crime.
- B) Ensuring that patrol officers are aware of the importance of local law enforcement's response to victims, particularly because the police report provides the necessary groundwork for future investigation and damage control for victims' property, and his/her ability to restore his/her good name and credit. It is notable that for many victims, especially seniors, their hard earned credit history is the most valuable commodity that they have lost in this crime.



The purpose of this part of the toolkit is to help police executives by providing help in identifying and meeting training needs for their officers in tactics to prevent, investigate, and respond to identity crime.

**A. Assessment of Current Status** (circle one)

1. Does our police academy curriculum include training on identity crime?

Yes          No          Not Sure

2. Do our officers know the state and local laws pertaining to identity crime?

Yes          No          Not Sure

3. Do we have routine in-service trainings on new and emerging technologies used in identity crimes?

Yes          No          Not Sure

4. Do all of our officers (patrol and commanders) know the following?

- The serious, pervasive nature of identity crimes and the impact on the community, methods of crime and types of perpetrators?
- To always take police reports from victims of identity crimes?
- Protocols and procedures for taking reports of identity crimes?
- The potential relationship between identity crimes and other criminal activity?
- The tools commonly used by identity crime perpetrators, such as laminating machines, color copiers and blank checks?

Yes          No          Not Sure

5. Do our investigators know how to:

- Collect electronic evidence?
- Analyze financial documents?
- Find additional victims?
- Interrogate identity crime suspects?
- Use informants in these kinds of cases?
- Present material effectively to prosecutors?
- Use national databases?

Yes          No          Not Sure



## B. Tools for Improving Effectiveness

The assessment on the previous page is intended to help identify areas where further training will be useful. There are many good training resources available for low- or no-cost. Consider using or adapting these based on your assessment above.

If instituting a new training program is not practical immediately, it may be helpful to provide officers with briefings on how to a) help victims who report crimes which are connected to identity crime and/or report that they have been a victim of identity crime and b) initiate investigations on identity crime.

See **Attachments C and D** for one-page briefing sheets which can be modified, copied, posted, and distributed within your department.

Training materials available online:

- Visit [www.idsafety.org](http://www.idsafety.org) for archived Webinars addressing different aspects of the issues.
- Visit the President's Identity Crime Task Force site to learn about the federal agencies responses to identity crimes<sup>4</sup>.
- Visit the FTC's law enforcement site to see the resources available to law enforcement officers<sup>5</sup>.
- The Secret Service and IACP jointly published Best Practices for Seizing Electronic Evidence<sup>6</sup>.
- The Secret Service also published A Pocket Guide for First Responders for seizing electronic evidence<sup>7</sup>.
- Request a free copy of Forward Edge II, an interactive software training program that trains officers in investigative techniques for electronic crimes<sup>8</sup>.

### Identity crime units for police academy curriculum or for in-service training:

The IACP can design and deliver a customized program for your department. Contact the IACP ID Safety Project for more information.

In addition, many states have developed officer training modules related to this issue. Check the map at [www.idsafety.org](http://www.idsafety.org) for training center locations and types of training available.

### Roll-Call Training

A roll-call video produced by the Secret Service is available to provide an introduction to identity crime issues for all officers with a minimum investment of training time<sup>9</sup>.

<sup>4</sup> [www.idtheft.gov/index.html](http://www.idtheft.gov/index.html), <sup>5</sup> [www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/index.html](http://www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/index.html),  
<sup>6</sup> [www.secretservice.gov/electronic\\_evidence.shtml](http://www.secretservice.gov/electronic_evidence.shtml), <sup>7</sup> [www.forwardedge2.com/pdf/bestpractices.pdf](http://www.forwardedge2.com/pdf/bestpractices.pdf),  
<sup>8</sup> [www.forwardedge2.com/](http://www.forwardedge2.com/), <sup>9</sup> [www.forwardedge2.usss.gov/](http://www.forwardedge2.usss.gov/)

### C. Further Information

The FTC and IACP have held regional one-day seminars for law enforcement managers, bringing together police officers, prosecutors, representatives of state department of motor vehicles, and industry fraud investigators. More than 1,800 participants have benefited from these trainings. See the article in *Police Chief Magazine*, "A Chief's View: Identity Theft: Resources for Police," by Stephen White and Monique Einhorn, vol. 72, no3, April 2005.

#### **Commonwealth of Pennsylvania Training**

The Pennsylvania Municipal Police Officers' Education and Training Commission has a course entitled, "Identity Crimes," which is part of the mandatory in-service training program for 2007. For a copy of the training guide or for further information, contact Charles Crow, Director of Training at 717.346.4086

#### **State of Michigan Training**

The Michigan State Police, in cooperation with the Michigan Association of Chiefs of Police and the Michigan Sheriff's Association, has developed a four-hour training program for police and sheriff's departments throughout the state. This training draws on work with prosecutors throughout the state to ensure that officers have a good understanding of what is needed to prosecute a case, including such technical issues as how to authenticate business records for preliminary hearings and trial and how to substitute witness affidavits for in-person trial appearances.

**National White Collar Crime Center (NW3C)** offers free training for law enforcement personnel and prosecutors. Identity Theft Investigations (IDTI) is a three-day course that teaches students to recognize identity crime indicators, the relationship between identity crimes and terrorism, drug and arms trafficking and organization crime, and the value of public-private and interagency partnerships. The course also teaches best practices in investigation of these crimes to facilitate successful prosecutions. There are a range of other options, including online courses, to suit your particular department's needs for training.

**The Federal Law Enforcement Training Center**, run by the Department of Homeland Security, offers a variety of courses, including First Responder to Digital Evidence Program (FRDE), which trains law enforcement personnel in assessing, acquiring and analyzing digital evidence. The Training Center exports its two-day training session at alternate locales, such as local police departments, at a cost of \$2,500.

**The National Computer Forensic Institute** is scheduled to open in January 2008. The Institute, run by the U.S. Secret Service, will train 900 state and local police officers, prosecutors, and judges each year on investigating electronic crimes and computer forensics.





## V. Agency Partnerships

By their nature, identity crime investigations require partnerships and cooperation among multiple agencies. Generally, the criminal activity is not limited to one local jurisdiction—a credit card stolen in California may be used in many other states and even across international borders.

In addition to the victim himself or herself, credit companies and other financial institutions may be key parties to the investigation. Furthermore, because of the potential connections of identity crimes to federal concerns such as mail fraud, interstate commerce and national security, an array of federal agencies have potential jurisdiction over aspects of these crimes.

In addition to the usual coordination necessary with state and municipal police departments and with district attorneys, federal agencies that may have jurisdiction over parts of an identity crime investigation include:

- The United States Postal Service
- The United States Secret Service Criminal Investigations Division
- The United States Department of Justice Computer Crimes and Intellectual Property Section
- The Internal Revenue Service
- The Social Security Administration
- The Federal Trade Commission
- The Federal Bureau of Investigation
- The Immigration and Customs Enforcement Agency

The purpose of this part of the toolkit is to help local law enforcement create and sustain partnerships that can help to prevent, investigate, and respond to the growing problem of identity crime.

### A. Assessment of Current Status

How well is your agency connecting to partners who can help you to prevent, investigate and respond to identity crime in your jurisdiction? Take this short quiz to find out:

Does your agency do the following:	Yes	No
Participate in a multi-jurisdictional task force on identity crime?		
Include local, state, and federal law enforcement officers and prosecutors on a task force?		
Have standard reporting protocols for identity crimes that are consistent with the FTC complaint database?		
Input information on identity crimes into the Consumer Sentinel database run by the FTC?		
Belong to the Law Enforcement Retail Network?		
Make an effort to get to know managers and executives at your local financial institutions?		

## B. Tools for Improving Effectiveness

If you answered no to any of the questions above, here are some ideas for expanding your agency's partnerships with the institutions that can help improve your agency's ability to prevent, investigate and respond to identity crime.

### 1. Joining or establishing multi-jurisdictional task forces on identity crime:

Task forces allow agencies to share resources and expertise, and avoid duplicate efforts. U.S. Department of Justice publications suggest that, if possible, such task forces be at the state level, and that they include, at a minimum, motor vehicle departments and local and state government agencies that keep public records.

The Secret Service has primary responsibility for investigating identity crime, but it "does not accept cases unless there is a financial loss over \$200,000 and a multi-state fraud ring is involved."<sup>10</sup> This leaves most identity crime cases without an investigating entity, unless local agencies can pool their investigation efforts.

To find a task force operating in your area, visit [www.ectaskforce.org/regional\\_locations.htm](http://www.ectaskforce.org/regional_locations.htm).

### 2. Developing standard reporting protocols that are consistent with the FTC complaint database:

It is important that the first report taken from a victim be brief and that the victim immediately gets a copy of the report that he/she needs in order to report the crime to banks, debt collectors, credit card companies, etc. See "Guidelines for Taking a Police Report on Identity Crime" on page 20 of this document for reporting protocol.

### 3. Inputting information into the FTC database (Consumer Sentinel):

The number of complaints entered into Consumer Sentinel grows each year - showing the growth of the problems, but also the increased savvy among law enforcement professionals who are inputting the data about the crimes for the benefit of investigators.

The FTC manages the Identity Theft Data Clearinghouse as part of its Consumer Sentinel system. This system includes more than 700,000 records of identity crime complaints from victims, police officers, and state and federal agencies. This resource is intended to aid investigators in spotting cross-jurisdictional trends and sharing information.<sup>11</sup>

### 4. Joining the Law Enforcement Retail Network:

The Law Enforcement Retail Partnership Network (LERPnet) is used by loss prevention industry experts and law enforcement to share information and help stop crime by criminal organizations. LERPnet was developed by the Department of Justice and the FBI in conjunction with the National Retail Federation (NRF) and the Retail Industry Leaders Association (RILA). To join, visit [www.ectaskforce.org/regional\\_locations.htm](http://www.ectaskforce.org/regional_locations.htm)

### 5. Getting to know the major financial institutions (and their leadership) in your area:

Police departments need to be proactive about linking with the banking, financial services, and credit institutions in the local area. These entities also have their own task forces and investigators and can be a real resource in preventing, investigating, and responding to identity crimes. Consider hosting a networking breakfast, joining the Rotary Club, or scheduling a meeting with the industry representatives just to begin the conversation about working more closely together. They will appreciate the outreach; they know the vital role law enforcement plays in preventing future victimizations and in restoring victims to pre-crime status.

<sup>10</sup> "Identity Theft," Problem-Oriented Policing Series, p. 31

<sup>11</sup> Information on the Identity Theft Data Clearinghouse comes from "A Chief's View: Identity Theft: Resources for Police," by Stephen White and Monique Einhorn, *The Police Chief*, vol. 72, no. 3, April 2005.



### C. Further Information

Task forces allow agencies to share resources and expertise, and avoid duplicate efforts<sup>12</sup>. U.S. Department of Justice publications suggest that, if possible, such task forces be at the state level, and that they include, at a minimum, motor vehicle departments and local and state government agencies that keep public records.

Some examples of successful task forces include these:

#### **Metro-Richmond Identity Theft Task Force:**

The work of the Metro-Richmond Identity Theft Task Force, established in 2004, resulted in the indictment of 51 defendants in November 2006. There were 45 indictments, some on charges with mandatory prison terms upon conviction. The task force includes 15 federal, state and local law enforcement agencies. For more information, contact:

Jim Rybicki Public Information Officer  
Phone: 703.842.4050 Fax: 703.549.5202  
E-Mail: usavae.press@usdoj.gov

Check out the Task Forces' Web site at [www.richmondidtheft.com/](http://www.richmondidtheft.com/).

#### **Sacramento Valley Hi-Tech Crimes Task Force:**

A Metropolitan Approach to Identity Theft By Robert F. Berardi, Sergeant, Los Angeles County Sheriff's Department, Whittier, California [www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article\\_id=1188&issue\\_id=52007](http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=1188&issue_id=52007).

#### **Florida Statewide Task Force:**

Excerpt from Identity Theft Literature Review, Graeme R. Newman and Megan M. McNally, published by the U.S. Department of Justice, July 2005. "In 2001, the Florida Attorney General's Office of Statewide Prosecution and the Florida Department of Law Enforcement (FDLE) created a statewide task force to target the perpetrators of identity crime. Operation LEGIT (Law Enforcement Getting Identity Thieves) consists of five full-time special agents (as of 2001), and other regional personnel from both local and federal agencies, who investigate cases of identity crime and conduct educational seminars on the investigation of identity crime-related cases for law enforcement audiences across the state. The investigation of one case by the Hernando County (Florida) Sheriff's Office, the Florida Department of Law Enforcement, the Office of Statewide Prosecution, and the SSA/OIG led to the capture of one Florida suspect who had used the identity of a California victim for more than 12 years. Between 1987, when the victim lost his wallet on vacation in Daytona Beach, and 2001, when the investigation was initiated, this offender had purchased and sold homes, opened bank and utility accounts, obtained credit and had been arrested at least three times using the victim's name. The victim had been wrongly arrested in California (on a Florida warrant), been held in jail for more than one week, and had several civil judgments against him before the criminal was captured through the efforts of this task force."

This task force put itself out of business by training the membership to do this work as part of routine operations, and it is no longer operational.

<sup>12</sup> See the discussion of task forces in Graeme R. Newman and Megan M. McNally's *Identity Theft Literature Review*, published by the U.S. Department of Justice, July 2005.



## VI. Community Outreach

One of the challenges facing local law enforcement is helping community residents and businesses become less vulnerable to crime, and better at preventing it. In the case of identity crime, it is rare that local law enforcement takes the lead on educating citizens in this area, and yet, local law enforcement is well positioned to help prevent identity crime by taking an active role in building community awareness.

Community residents need to learn both how to protect themselves from identity crimes, and what to do in the event they become a victim - starting with reporting the crime to their local police department. Posting prevention tips and victim action steps on your Web site, along with links to the FTC, Social Security Administration, and other relevant federal agencies can help residents become better partners in prevention. Developing brochures on identity crime prevention, giving presentations at community meetings, and hosting identity crime prevention events can also build community awareness.

Finally, it is crucial that residents know to file a police report when they have been victimized; yet few community residents do so. Approximately nine million people in the United States were victims of identity crime in 2005 (Better Business Bureau, 2006). However, barely one-third of these victims contacted police (source: Identity Theft Literature Review). This makes the job of preventing future victimization much more difficult, and it is important that community residents realize that filing a report is their best defense against further losses as well as their first step to recovery.

In addition to residents, the business community is a valuable resource and ally in the fight against identity crimes. Outreach to industries and local businesses affected by identity crimes, such as retailers and the finance and credit industries, can help police to capitalize on their expertise in customer transaction data-collection and management. Police can also help businesses by assisting them in adopting business practices that will lower their risk of identity crimes.

The purpose of this part of the toolkit is to help identify areas where community outreach and education can prevent identity crimes in your jurisdiction and to provide tools for that outreach and education.

### A. Assessment of Current Status

#### Did you know...?

- That older victims are less likely to report identity crime than younger victims?<sup>13</sup>
- That MasterCard® and Visa® had estimated losses in 2000 of \$114 million?<sup>14</sup>
- That the Identity Theft Resource Center reports that victims perceive that police “do not care” about this crime?<sup>15</sup>

<sup>13</sup> Newman and McNally, *Identity Theft Literature Review*, p. 16.

<sup>14</sup> Newman and McNally, p. 31.

<sup>15</sup> See the Identity Theft Resource Center for summaries of victim perceptions in this area: [www.idtheftmostwanted.org/artman2/publish/v\\_fact\\_sheets/Fact\\_Sheet\\_112\\_Identity\\_Theft\\_victim\\_-\\_Investigator\\_Communications.shtml](http://www.idtheftmostwanted.org/artman2/publish/v_fact_sheets/Fact_Sheet_112_Identity_Theft_victim_-_Investigator_Communications.shtml)



What has your department done to help prevent your residents and businesses from becoming victims?

Check all that apply:

- Developed print materials to explain identity crimes to citizens
- Hosted, sponsored, or promoted a Shred-a-Thon
- Provided information for area businesses on safe business practices
- Consulted with businesses on the location of video surveillance cameras
- Offered presentations to business groups on how to decrease losses due to fraud
- Created a Web site (or parts of a Web site) with local information on how to file a report in case of identity crime
- Developed special outreach strategies for target high risk groups, like seniors
- Worked with local media to help expand coverage of identity crimes
- Provided media information on the impact of identity crime at the local level
- Notified victims of crime that they are also at risk of identity crime

#### B. Tools for Improving Effectiveness

Do not worry - if you have not done the outreach above, here are some tools to get started:

##### 1. Develop materials to explain identity crimes to citizens

Visit [www.idsafety.org](http://www.idsafety.org) to request copies of the Identity Crime Prevention Kit - available for distribution at community meetings and events.

See **Attachment G** for a flyer, adapted from the Los Angeles Sheriff's Department, that can be modified, put onto your department's letterhead, and distributed at community events.

You may also want to use a free and excellent PowerPoint presentation at community crime watch meetings. Visit [www.mc.vanderbilt.edu/medschool/finaid/docs/Grand\\_Theft\\_Identity.pdf](http://www.mc.vanderbilt.edu/medschool/finaid/docs/Grand_Theft_Identity.pdf).

##### 2. Shred-a-Thons

Many communities host shred-a-thons; a fun way to raise awareness about identity crime and publicize prevention tips. One resource for your community in putting on a shred-a-thon is the National Association of Professional Organizers. This group has chapters all over the country and they have volunteered in some communities to organize these events as a promotional opportunity for their members and as a public service. Visit NAPO's Web site at [www.napo.net](http://www.napo.net) for more information and consider contacting your local chapter for help in organizing an event.

### 3. Provide information for area businesses on safe business practices

The FTC has a concise primer for businesses on how to prevent their customers' information from becoming compromised. Print this Web page and give it to the businesses in your community, or consider sending the link, [www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm](http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm) to your local Chamber of Commerce.

### 4. Consult with businesses on the location of video surveillance cameras

Your officers may already do this with banks and other businesses concerned with crime. Consider expanding your outreach to businesses by offering to help position cameras to capture the images you need for investigations.

### 5. Offer presentations to business groups on how to decrease losses due to fraud

At Chamber of Commerce meetings or similar groups of businesses, you can talk about the prevalence of identity crimes in your community, and also offer tips on how businesses can protect themselves and their data.

Visit this page, [http://i.i.com.com/cnwk.1d/i/bnet/BNET\\_10\\_Ways\\_To\\_Protect\\_Your\\_Data1.pdf](http://i.i.com.com/cnwk.1d/i/bnet/BNET_10_Ways_To_Protect_Your_Data1.pdf), for a downloadable information sheet on how businesses can protect confidential data.

### 6. Create a Web site (or parts of a Web site) with local information on how to file a report in case of identity crime

There are many excellent web resources for victims and businesses to help guard against, or recover from, identity crime. Visit these examples for inspiration:

- The Michigan State Police<sup>16</sup>
- The City of Tempe, Arizona<sup>17</sup>
- The University of Oklahoma<sup>18</sup>

### 7. Develop special outreach strategies for target high risk groups, such as seniors

The Senior Journal has a great article aimed at helping seniors protect themselves; it is worth emailing to groups who work with the elderly.<sup>19</sup>

### 8. Work with local media to help expand coverage of identity crimes

An excellent, easy-to-use guide to getting media coverage for your cause can be found at [www.causecommunications.com/diy/getnewscoverage.html](http://www.causecommunications.com/diy/getnewscoverage.html). It is directed at nonprofits but works just as well as a guide for small police departments seeking to promote prevention for identity crime.

<sup>16</sup> [www.michigan.gov/msp/](http://www.michigan.gov/msp/)

<sup>17</sup> [www.tempe.gov/cpu/IdentityTheft.htm](http://www.tempe.gov/cpu/IdentityTheft.htm)

<sup>18</sup> [www.ou.edu/oupd/inetmenu.htm](http://www.ou.edu/oupd/inetmenu.htm)

<sup>19</sup> [www.seniorjournal.com/NEWS/Money/Valentine/6-10-05-GreatIdeasForSenior.htm](http://www.seniorjournal.com/NEWS/Money/Valentine/6-10-05-GreatIdeasForSenior.htm)



## C. Further Information

### 1. Legislative Changes

As you take time to educate your community, you may also want to educate public officials about the seriousness of these crimes and laws that are needed to prevent identity crimes, protect victims, assist in investigations, and punish criminals.

Visit [www.idsafety.org](http://www.idsafety.org) to see a compendium of up-to-date state laws and a matrix that offers an analysis of how each state's laws compare to the most effective legislative efforts. As community leaders, it is important that police executives take a leadership role in educating legislators and policy makers in this area. Legislators rely upon police for information about emerging crime problems, and also take the advice of police officials when new legislation is under consideration. Police officials have a unique, critical role in helping to create legislative momentum to protect people from identity crime and to build legislative capacity to help victims be restored to their pre-crime status.

Learn more about advocacy for improved legislation on identity crime at the U.S. Public Interest Research Group's (USPIRG) Web site at [www.uspirg.org/financial-privacy-security/identity-theft-protection](http://www.uspirg.org/financial-privacy-security/identity-theft-protection).

### 2. Examples of Successful Initiatives

#### WinCo Foods

WinCo Foods is an Oregon grocery retailer that had become a susceptible fraud target because it lacked fraud prevention training and the accompanying systems and processes. The Beaverton Police Department established a partnership with WinCo Foods and provided important staff training tools. As a result, WinCo Foods adjusted its customer transaction process and now requires photo identification from customers paying by check. The company also altered the position of surveillance cameras to obtain better footage of individuals who cash checks. This repositioning helped identify the suspect when a crime occurred. Crime reporting also increased.

*From The Police Chief, vol. 74, no. 5, May 2007. Copyright held by the International Association of Chiefs of Police, 515 North Washington Street, Alexandria, VA 22314 USA.*

#### Using Volunteers for Community Outreach

Charlotte-Mecklenburg Police Department created a victim alert program to prevent theft victims from also becoming victims of identity crime. Citizen volunteers receive training on identity crime and how personal information is compromised. They are taught to pull crime reports on the types of thefts (stolen wallets, thefts from autos, etc.) that are a precursor to identity crimes. Volunteers contact the theft victims and advise them of the actions they should take to avoid becoming victims of identity crime, such as canceling lost or stolen credit cards and activating a fraud alert with the three credit reporting agencies. (Contact: Charlotte-Mecklenburg Police Department, Fraud Unit, 704.336.2311).

## VII. Attachments

### A. Sample Job Description for an Identity Crime Specialist

The XYZ Police Department seeks support for its work in preventing, investigating and responding to identity crimes; a growing problem in our jurisdiction and across the country.

The Identity Crime Specialist will be working closely within the department with investigators and externally with victims, the business community, and policy makers. He/She must have the following skills, knowledge and experience:

#### Skills

Excellent communications skills, particularly for working with other law enforcement agencies and businesses; be a creative, innovative worker, and be a self-starter - able to envision and implement new approaches; ability to use computers, databases, and to conduct research.

#### Knowledge

Familiarity with law enforcement resources internally and externally to support investigations

A working knowledge of our local, state, and federal laws

Ability to recognize evidence

Understanding of the search warrant writing and serving processes

Understanding of department policies

Understanding of courtroom procedures

Familiarity with the elements of identity crime and related crimes

Understand the difference between identity crimes and other forms of fraud

Understanding or ability to learn the ways that credit companies, credit bureaus, banks, and online services (including shopping, banking, financial transactions, etc.) work and interact

#### Experience

Proven ability to plan and execute tactical operations, including:

- Developing a tactical plan
- Coordinating activities associated with controlled deliveries or surveillances
- Coordinating resources for search warrant operations
- Briefing the operations plan
- Executing the plan
- Planning for contingencies
- Coordinating post investigative activities
- Debriefing personnel
- Working with multiple agencies at all levels of government

The Identity Crime Specialist will  
*(list particular duties here)*

and will report to:  
*(list appropriate supervising officer here)*



## B. Guidelines for Taking a Police Report on Identity Crime

Victims are required to file a police report to start their recovery from identity crime. One of the primary purposes of this toolkit is to encourage law enforcement to take the report for their residents to help start them on the long road to recovery to their pre-crime status.

An identity crime victim must provide a copy of the police report to banks, creditors, other businesses, credit bureaus, and debt collectors. The initial investigative report should only include a brief but thorough summary of the complaint information so that a copy of the initial report can be easily and promptly provided to the victim.

If the victim suspects who may have committed the offense, obtain as much identifying information on the suspect as possible and document why they believe this.

**Police should advise victims to obtain a copy of their credit report** from one of the three credit bureaus. They can be obtained at no cost:

**Equifax**                      [www.equifax.com](http://www.equifax.com)  
P.O. Box 740241, Atlanta, GA 30374-0241  
800.525.6285

**Experian**                      [www.experian.com](http://www.experian.com)  
P.O. Box 9530, Allen TX 75013  
888.EXPERIAN (397.3742)

**Trans Union**                      [www.transunion.com](http://www.transunion.com)  
Fraud Victim Assistance Division  
P.O. Box 6790, Fullerton, CA 92634  
800.680.7289

**Free Annual  
Credit Report**                      [www.annualcreditreport.com](http://www.annualcreditreport.com)

The victim should review their credit reports and close any unauthorized or compromised credit or charge accounts.

The FTC has prepared an "ID Theft Affidavit" that is accepted by many banks, creditors, other businesses, and credit bureaus. Provide the victim with a copy of the ID Theft Affidavit and the form's instructions, or direct them to [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/) for a copy they can print themselves.

The affidavit is NOT for the police department or other law enforcement agency. The victim should be told to copy the police report and attach it to a copy of this ID Theft Affidavit and file a copy of both with each credit bureau, collection agency, credit card company, or charge account that was compromised.

The creditor is also required by law (Fair Credit Reporting Act, Section 609(e)), to provide the victim with a copy of the fraudulent credit application or other business transaction, free of charge, within 30 days of receiving the victim's request.

The victim may give law enforcement permission to obtain these records by providing written permission to the creditor. The victim should be instructed to contact the creditor's fraud department by telephone and ask if the creditor has a specific address for the victim to make this request.

Since this entire recovery process can be long and drawn out, officers should **advise the victim to prepare a journal to document who they contacted for every step of the way** and what actions they have taken. Documentation is essential to a successful recovery and eventual prosecution.

**Police should also instruct the victim that the creditor is entitled to ask the victim for proof of identity**, such as a government-issued ID card, and request a copy of the police report and a completed affidavit, such as the FTC ID Theft Affidavit.

The victim must contact one of the three credit bureaus to report the crime. When contacted, the credit bureaus will put a fraud alert on the victim's credit report to prevent any further fraudulent accounts from being opened. As soon as one of the credit bureaus places a fraud alert, the other two bureaus are automatically notified to do the same.

In addition to providing a wealth of information on how to cope with identity crime, the FTC maintains a database to assist law enforcement. Known as the Consumer Sentinel, it is a law enforcement only collection of identity crime-related crimes. For their complaint to be part of this database, victims should be instructed to access this FTC consumer complaint form online at [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/).

Police should compare new information with the other reported incidents in the FTC's Consumer Sentinel database for possible tips, other agency involvement, and recommended actions. Your police department can register its police officers with the FTC at [www.ftc.gov/sentinel/](http://www.ftc.gov/sentinel/).

Because victims may be overwhelmed by the possibly long and tedious process, you should encourage them to contact their local Network of Victim Assistance (NOVA) for assistance in handling their recovery from this crime.

You should also encourage the victim to obtain the FTC's guidebook, "Take Charge: Fighting Back Against Identity Theft." He or she may obtain a copy at [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/). It is a point-by-point outline of things to do to assist in the recovery from identity crime. In addition, he or she can visit [www.idsafety.org](http://www.idsafety.org) to find the Bank of America/IACP ID Crime Recovery Kit.

**Remember:**

**Take the report to put victims on the path back to their pre-crime status!**



### C. Guidelines for Helping Residents Affected by Identity Crimes

#### 1. Take the report

The victim of identity crime is required to file a police report prior to contacting banks, creditors, other businesses, and the credit bureaus. The initial investigative report should only include a brief summary of the complaint information so the department can easily and promptly provide a copy of the initial report to the victim. The victim needs a copy of the report, coupled with a copy of an affidavit, to start the process promptly to stop the continuing identity crimes and start the long recovery to his or her pre-crime status.

#### 2. Give the victim an Identity Crime Restoration Kit. Visit [www.idsafety.org](http://www.idsafety.org) for a copy.

#### 3. Help the victim cancel any fraudulent or compromised accounts

The victim must immediately close and dispute any new, unauthorized accounts whether they are credit cards or charge accounts. The Federal Trade Commission has prepared an "ID Theft Affidavit" that is accepted by many banks, creditors, other businesses, and the credit bureaus. Direct the victim to [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/) for a copy.

The victim should be told to photocopy the police report and attach it to a copy of the ID Theft Affidavit and file a copy of **both** with each credit bureau, collection agency, credit card company, or charge account that was compromised.

It is important for the victim to know that the creditor is entitled to ask the victim for proof of identity, which would be a government issued ID card, a copy of the police report, and a copy of a completed affidavit, like the FTC ID Theft Affidavit.

#### 4. Help the victim get a fraud alert placed on their credit report

The victim must contact one of the three credit bureaus to report the problem. When contacted, the credit bureaus put a fraud alert on the victim's credit report to prevent any further fraudulent accounts from being opened and stop the identity crime from continuing. For instructions and help, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), sponsored by Equifax, Transunion and Experian.

#### 5. Help the victim file a complaint with the FTC

In addition to providing a wealth of information on how to cope with identity crime, the FTC maintains a database to assist law enforcement called the Consumer Sentinel, a law enforcement only collection of identity crime-related crimes. The victim should be instructed to access this FTC consumer complaint form at [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/) so his or her complaint will be part of the database for law enforcement. If the crime involves regular mail, recommend he or she also contact the U.S. Postal Inspection Service at [www.usps.com/postalinspectors/fraud/MailFraudComplaint.htm](http://www.usps.com/postalinspectors/fraud/MailFraudComplaint.htm).

#### 6. Alert the victim to resources available to help with recovery

The Network of Victim Assistance (NOVA) can assist in the recovery process: <http://trynova.org/>. The FTC also offers a guidebook for those affected by identity crime. Direct victims to [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/) for this step-by-step guide to recovery.



## D. Guidelines for Investigating Identity Crimes

Once a victim has reported a suspected identity crime, there are a few steps that officers can take to improve the odds of conducting a successful investigation and also in identifying additional victims.

### 1. Compare the incident with Consumer Sentinel database.

Our department has registered for access to a database owned and operated by the Federal Trade Commission, called Consumer Sentinel. Visit this site [www.ftc.gov/sentinel/](http://www.ftc.gov/sentinel/) to get your own username and password, and to enable use of the database for investigating this crime.

### 2. Know our local laws

Visit [www.idsafety.org](http://www.idsafety.org) and click on your state on the map to get up-to-date information on your local laws in this area.

### 3. Use additional investigative tools as necessary.

**Overview of Identity Crime - help in understanding the scope and nature of these crimes**  
IACP/Bank of America - [www.idsafety.org/](http://www.idsafety.org/)

**Explanation of the Consumer Sentinel Database and how to use it**

Federal Trade Commission (FTC)

1.877.IDTHEFT (1.877.438.4338)

[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

**Information on latest scams, and how to work with the USPS to prevent/respond to crimes**

United States Postal Inspection Service

[www.usps.com/postalinspectors/](http://www.usps.com/postalinspectors/)

**Bank and Credit Card Information**

Use E-Information, an intranet site operated by the Secret Service. Free for law enforcement agencies and investigators.

**Links among databases**

FinCEN (Financial Crimes Enforcement Network)

### 4. Checklist (see page 24-25)



### E. Checklist for Investigating Identity Crimes

The purpose of this checklist is to provide law enforcement officers and agencies with a generic guide for investigating cases of identity crime. Law enforcement administrators should ensure that their agencies have established effective policies and procedures for the handling of identity crime investigations. Compliance with an agency's standard operating procedures, by agents/investigators, can result in efficient operations and successful resolution of the incident.

This checklist is not intended to be followed step-by-step by agents/investigators in every reported identity crime investigation. It is meant to provide the agent/investigator with a basic framework of actions, considerations, and activities that can assist them in performing competent, productive and successful investigations.

- ✓ Ensure that the date of the incident falls within the statute of limitations for prosecution.
- ✓ Based on amounts of theft or victims, agency makes a determination to investigate the crime.
- ✓ If agency agrees to investigate the crime, assign a case agent/investigator and analyst.
- ✓ Notify the victim(s) of the identity and contact information for the case agent/investigator.
- ✓ Refer the victim(s) to other Web sites or contact numbers that can assist them in restoring their identity and credit.
- ✓ Advise the victim of any Victim Advocacy Program that may exist within their city, county or state.
- ✓ Direct victim(s) when contacting their creditors or others regarding the crime to maintain a written log of all phone conversations with dates, times, person whom they spoke with, and the contents of their discussions.
- ✓ Direct victim(s) to maintain a central file of all paperwork, documents, police reports and correspondence pertaining to the crime.
- ✓ Direct the victim(s) to follow up on all requests they receive from creditors.
- ✓ Have the victim(s) gather all documents (bank and credit card statements, letters from creditors or collection agencies, etc.) that would assist in the investigation.
- ✓ Obtain authorization from the victim(s) under the "Fair Credit Reporting Act" to obtain transaction records from their creditors without subpoena.
- ✓ Explain to the victim the potential long and short-term consequences of being a victim of an identity crime.
- ✓ If a social security number was used by the subject(s), contact the Social Security Administration's Office of Inspector General and obtain the accurate biographical information for the SSN that was used and compare it to the information that was provided by the subject(s).

- ✓ Interview victim(s) to establish spending patterns and attempt to identify other victims.
- ✓ Attempt to identify other associated victims through the use of Fraud-Net, and Consumer Sentinel at [www.ftc.gov/sentinel](http://www.ftc.gov/sentinel), and share intelligence with other law enforcement agencies.
- ✓ Review all documents provided by the victim(s) (i.e., ATM receipts, bank statements, recently opened store or bank accounts, credit reports and credit card information).
- ✓ Communicate with other law enforcement agencies to ascertain if they have similar reported crimes, victims, or possible suspects.
- ✓ Subpoena all relevant records (bank, computer/Internet account information, credit card information, and victim(s) credit information).
- ✓ Have an analyst or agent/investigator review all victim documentation in an effort to establish victim's spending patterns and attempt to identify possible suspect(s) by establishing common themes where fraudulent information was used.
- ✓ Attempt to identify source of compromise such as accountant, lawyer, dentist, school, employer, insurance carrier, or anyone else who may have access to the victim's identifiers.
- ✓ Once a suspect is identified, use traditional investigative techniques (i.e., tracking devices, mail covers, surveillances, trash pulls, telephone toll records, and forensic analysis) to obtain evidence.
- ✓ Contact banks or other financial institutions where illegal transactions occurred and attempt to obtain video recordings or surveillances of the transactions, and obtain all personal victim identifiers to include mailing address.
- ✓ If applicable, contact merchant security departments and solicit their assistance.
- ✓ Obtain available information from Postal Inspectors' reference post office boxes, associated applications, and forwarding instructions.
- ✓ Contact credit card security departments.
- ✓ Contact the Secret Service E-Information Network at: [www.einformation.uss.gov](http://www.einformation.uss.gov).
- ✓ Utilize spreadsheets for the purpose of building account/victim databases and maintain a leads database.
- ✓ Periodically meet with prosecutor and other investigators to review case investigation and discuss future investigative steps to include the use of a grand jury.
- ✓ Periodically brief your supervisors and investigative staff on the status of the investigation.
- ✓ Conduct a legal search of the suspect's home and seize all relevant documents and evidence.

## F. Typical Fraud Schemes

### Pigeon Drop or Lottery Scam

In this type of scam, the suspects work in pairs. One befriends an unsuspecting citizen, the "pigeon," claiming to have either a large sum of money he/she just found or the winning lotto ticket. He/she cannot go to a bank because he/she is an immigrant or another plausible sounding reason. As the first suspect is talking with the victim, the second suspect approaches and gets involved. One of the suspects will go to phone and call a lawyer. The suspect returns and says they can keep the money and split it three ways but to get their share, all have to put up some "good faith" money. The second suspect shows he/she has his/her money with a roll of what appears to be cash. Everyone agrees to get the money then meet at a designated place to divide the proceeds. The victim contributes his/her "good faith" money, as well as the second suspect, by putting the money into a bag. You are then given the bag to hold while the two suspects go to collect the money. Covertly, a switch has been made and you are left holding a bag containing only shredded paper.

### Charity Switch

Very similar to the pigeon drop, but with a slight variation: You are approached by one suspect who claims to have recently come to America with a large amount of cash to be delivered to a church, but no one is at the church. The suspect tells you he must leave the country soon and asks you and another person (a second suspect) to deliver the money later. You are asked to put up "good faith" money to show you are honest. The suspects switch the money and disappear.

### Advance Fee Scams

In these types of frauds, you are contacted, usually by telephone, and told you have won a grand prize which is a very large sum of money. To collect the winnings, you must pay the taxes/fees up front for the money to be sent to you. The money you send is usually to a location out of state or another country such as Canada or Africa. After a short period you are contacted again and told there were problems with the winnings and you must send additional money to collect your prize. The prize never comes, and you realize you have been scammed.

### Endless Chain

Also known as a pyramid or ponzi scheme. This is any scheme whereby a participant pays a valuable consideration for the chance to receive compensation for introduction of one or more additional persons into the scheme. In reality, the only people who get the money are those who are at the top, usually the organizers or suspects. Those towards the bottom get nothing.

### Planned Insolvency (Bust Out)

A business fraud where the suspects request credit, via a fraudulent credit application, for small quantities of goods or services. They initially pay as agreed. The credit line and order is subsequently increased with the suspects receiving 30 to 45 days to pay. After receiving a large order, the suspects and their business disappear. Sometimes, the suspects will pay with a bad check in order to gain more time to make their escape.

### Theft by False Pretenses

A form of theft whereby the possession and title to money or other valuable property is voluntarily transferred from the victim to the suspect who has made a misrepresentation (a lie). The suspect never had any intention of holding up his or her end of the bargain. Before you realize their dishonesty they are long gone with your money.

### Bank Examiner

The suspect approaches you or may call you on the phone claiming to be a police officer who is investigating bank employees for embezzlement. You are asked to go to your bank and withdrawal cash so the officer can watch the bank employees. You are told to give the money to a "detective" who will return the money to the bank for you. The suspect disappears with your money.

### Sweetheart Swindle

This scam often involves an elderly man who is befriended by a young woman. She convinces him she truly cares about him and implies a romantic interest. She tells him she needs money for rent, food, furniture, her business, or she needs surgery. She may swindle him out of his life savings, often causing him to file bankruptcy. This is a very common fraud among Gypsy women.

**Fortune-Telling / Psychic Fraud**

You may be approached at stores, hotels, restaurants, etc., or when you go to a psychic reader. The psychic convinces you that you have an evil curse or evil spirits that must be "cleansed." Cleansing is an ongoing process that requires you to pay thousands of dollars in cash, jewelry, vehicles, etc.

**Lost Pet or Lost Property Scam**

You place an ad in a local paper about a lost pet or lost property. You then receive a call from a long haul truck driver who says he found your lost item but he is now hundreds of miles away. He will return your property (or advise of the location of your pet) after you send a "reward" by Western Union.

**Lost / Stolen Purse**

A "police officer" calls you to advise he/she found your purse (often before you realize it is missing or have reported the crime). The "officer" needs your personal information for his/her report. You, believing a police report is being taken, provide your personal information to the suspect and do not report the crime or cancel your accounts. The suspect then uses your personal information and credit cards to run up very large bills.

**Mail Theft**

Both incoming and outgoing mail can be stolen from your mailbox. Your checks can be "washed" to remove payee and amount information and altered so the suspect can cash them for more money. The criminals can obtain your name and credit card numbers from your outgoing bills and use this information to charge new purchases. Credit card applications can be stolen and altered. The suspect then applies for a new credit card in your name and goes shopping.

**Home Repair**

These suspects go door-to-door offering you a great deal on yard work, roof repair, chimney sweeping, house painting, etc. They may have "extra" supplies left over from their last job so they say they can save you money. Usually their products and labor are inferior. At the completion of the work, they claim to have used more supplies or there was more work than anticipated so they demand more money from you. They can be very intimidating.

**Distraction / Impostor Burglary**

A suspect comes to your house claiming to be from a city or county agency such as water or power. He/she needs to come into your house to check for problems. Once inside the suspect distracts you and steals cash and other valuables.

**Canadian Sweepstakes**

You receive a call from someone who says you have won a Canadian sweepstakes, but you must pay Canadian taxes before your winnings can be claimed. You are told to send a cashier's check or wire money via Western Union to them in Canada. It is a scam, your winnings never arrive. Also be advised, it is illegal for U.S. citizens to enter foreign lotteries (US Code Title 18, Part 1, Chapter 95).

**Purchase of Lottery Tickets**

You receive mail or calls from a company representative who will purchase lottery tickets for you in another state (usually Florida) and send you copies of your tickets. He or she keep the originals so they can collect for you if you win. You may even be conned into writing them monthly checks or allowing them to debit your checking account so they can purchase lottery tickets for you on a weekly basis. You have been scammed. The only one collecting anything is them.

**Phishing**

This is a term used when the identity criminals send out a very official looking e-mail to try and get you to provide them with your personal information. They will try to fool you into thinking your bank has sent the e-mail by placing the bank's logo in the message. The e-mail will ask you to "verify" your personal information, i.e. your social security number or account number. Once the identity criminals have this information they may use it to apply for new credit in your name, or make a withdrawal from your account. Your bank already has this information and will never ask you to verify this information via e-mail. Be very aware of this type of scheme. Do not ever respond to this type of e-mail, and it is not necessary to report this alone as a crime. If you have sustained a loss immediately contact your local police or sheriff's station to report the crime.



### G. Community Outreach Flyer

IDENTITY CRIME is the fastest growing crime in the United States with over nine million victims annually. **This crime will impact one out of every four people.** Visit [www.idsafety.org](http://www.idsafety.org) today to get your FREE IDENTITY CRIME PREVENTION KIT.

Identity crime is when a suspect gains access to your personal information and/or account numbers then assumes your identity and goes on a spending spree, commits a crime in your name, or does any of a number of things while posing as **you**.

It is an unusual crime in that you often do not realize you are a victim until long after the perpetrator has started to use your identity to do his/her crimes. Often victims discover the crime after they receive a bill, collection notice or attempt to make a large purchase, such as a car, and then realize their credit has been destroyed.

Once victimized, people end up spending money out-of-pocket to clear up their records, but they also must devote their time - up to hundreds of hours in some cases - doing so. In the meantime, victims are unjustly harassed by debt collectors, denied credit or employment opportunities, and in some cases even lose their cars or homes.

#### Discovering you have become a victim

You do not have to be a victim of identity crime for personal information to fall into the wrong hands. In the course of a busy day, how often might you share information about yourself in person, on the phone, or over the Internet? Although it is impossible to guarantee that identity crime will not happen to you, there are ways to reduce your chances of becoming a victim. Most victims do not discover the crime until it is too late. It can take a long time to reverse the damage these criminals can do to your credit rating.

Any of these indicators could mean that you have become a victim of identity crime:

- Mysterious bills for accounts you are not aware of
- Phone calls from creditors about delinquent payments you do not recognize
- Mail from unknown lenders asking for additional information



### What to do if you believe you are a victim

If you believe you are the victim of a fraud or an identity crime contact your local police department IMMEDIATELY to report the crime. Then,

- Notify your financial institutions and ask if they have an identity crime assistance program.
- Contact the three major credit bureaus and request a fraud alert be placed in your credit file.
- Complete an affidavit with information regarding you as the victim, how the fraud occurred, law enforcement's actions, documentation checklist, and fraudulent account statement(s).  
Note: Some creditors may have their own affidavit for you to complete.
- Send a blocking letter to the credit bureaus asking them to block the fraudulent activity from your file.
- Contact the fraud unit of the company that opened the fraudulent account. Request copies of documentation related to the account, such as a copy of the contract, statements or transaction records, and signatures.
- Send a dispute letter to the company that issued your misused account asking them to remove the charge.
- If you believe any legitimate accounts have been compromised, contact the financial institution immediately.
- As a victim, it is highly recommended that you contact the FTC to report the fraud and file a complaint. The FTC is the national repository for tracking identity crime.
- Keep a record of the credit bureaus, banks, and law enforcement agencies you have contacted while attempting to clear up your credit file. Keep this chart in a safe place. This information is one of the first things the detective investigating your case will request from you. It also proves to your creditors that you have been diligent in your efforts to clear up the fraudulent activity from your credit file.
- If you suspect social security number misuse call the Social Security Fraud Line at 800.269.0271. You may also file a complaint online at [www.socialsecurity.gov/oig](http://www.socialsecurity.gov/oig).



### Tips on how to avoid becoming a victim

Avoiding identity crime is not simple but there are several common sense things consumers can do:

- Keep personal information in a safe place and avoid storing important documents in easily accessible places like glove boxes or day planners.
- Do not give your social security or account number over the phone to anyone who has called you, or to anyone you do not know. Do not be afraid to ask why your personal information is needed and how it will be used.
- Shred all documents that contain personal information before tossing them out. Never simply toss documents that contain your social security number in the trash can.
- Cancel your paper bills and statements wherever possible and instead check your statements and pay bills online from financial institution secure Web sites.
- Monitor your account balances and activity electronically (at least once per week).
- If you do not have access to online accounts, review your paper bank and credit card statements monthly.
- Refrain from carrying unnecessary information such as PINs, passwords, or social security numbers in your wallet or purse.
- Retrieve paper mail from your mailbox promptly and deposit outgoing mail containing sensitive information in a secure mailbox.
- Check into putting a fraud alert on your credit file. A fraud alert is a message that an identity crime victim can place on his or her credit file, which alerts credit issuers who are doing a credit check in response to an application for new credit that your identity has been compromised. An initial fraud alert lasts for 90 days and is intended to prompt the credit issuer to call a given phone number or ask for additional proof of identity to verify that the applicant is not the impostor.





NOTES:




NOTES:



In partnership with:  
**Bank of America** 

**Protecting the Real You and Only You.**

The International Association of Chiefs of Police  
515 N. Washington Street, Alexandria, VA 22314  
Telephone: 1.800.843.4227 [www.theiacp.org](http://www.theiacp.org)



Identity crimes are among those new, emerging types of crimes that are just beginning to show their impact on communities.