Every Officer Needs to Know About Identity Crime

A wide range of behaviors as well as many crimes can put a person’s identifying information at risk. Law enforcement officers at all levels should be informed about identity crime, so that they can be on the lookout for signs that such activity may be a factor in another situation or investigation.

Types of activities often used in identity crimes include:

- Stealing information from businesses and organizations that store victims’ personal and financial information in their files, such as retailers, banks, hospitals and universities. This activity is commonly known as committing “data breaches.”
- Stealing information from transactions such as retail purchases, school enrollments, doctor visits, hospital admissions, insurance applications, etc.
- Going through trash and looking for straight cut or unshredded papers. This activity is commonly known as “dumpster-diving.”
- Stealing mail or wallets.
- Gaining access to vital documents such as birth/death certificates, driver’s licenses or Social Security cards through accessing employer records.
- Listening to public conversations.
- Tricking victims into giving information over the telephone or by e-mail.
- Buying the information either on the Internet or from someone who may have stolen it.
- Getting it from the victim’s computer, especially one that lacks firewalls.
- Obtaining it from a friend, relative, or someone who works with the victim and has access to the victim’s information.
- Using skimming devices designed to get information from the magnetic strip on credit cards.
- Completing a change of address form with the U.S. Postal Service to divert mail to another location.

Identity Crime Must be a Priority for Investigators

There are a number of reasons that investigators need to prioritize identity crimes. It may be helpful to note that the investigation of identity crime can be integrated with the investigation of other types of crimes, and this can make it more manageable within small departments.
Specifically, the reasons why these crimes must be prioritized include:

1. The excessive damage to credit, financial well-being and reputation experienced by many victims.
2. The likely links to other types of criminal activity including terrorism, drug and gun trafficking and theft.
3. The importance of linking apparently small identity crimes to larger criminal enterprises as a tool for investigating them.

Additionally, because links to other crimes are likely, investigators must work closely with other law enforcement and government agencies.

Identity Crime is Multi-Jurisdictional

While the first response by law enforcement must be to help victims recover losses or damages by taking a report and helping identify next steps, another important goal includes investigating the crime and making an arrest which leads to a conviction. It is extremely rare that this will all take place within the same local jurisdiction, and so, it is important that local law enforcement participate in coordinated investigative efforts with other government agencies and financial institutions across jurisdictions.

Investigations can be difficult because they may involve jurisdictional issues. For example, the victim may live in one state, but the charge on the victim’s account may have originated in another state. Jurisdiction issues can be confusing for law enforcement agencies that are not familiar with identity crime law or do not have departmental procedures for receiving and investigating complaints of identity crime. Many state laws allow jurisdiction to be based on the location of the victim, not just where the criminal act took place.

In light of this, investigators should take the following steps:

1. Identify the lead agency within the investigation.
2. Determine who within partnering agencies will be the point of contact.
3. Set up protocols for working together and sharing information from an early stage.
4. Address every lead physically accessible within the initiating jurisdiction including, but not limited to:
   - Rapid contact with credit granting agency to obtain official copies of any documents used to open the account (possibly protecting for latent evidence);
   - Rapid contact with merchants where property was physically purchased (including gift cards) for video records;
   - Rapid contact with online merchants to preserve electronic evidence and obtain computerized ordering data (including the IP address of the purchaser, which can be traced back to an actual phone line with a little effort);
   - Surveillance of the delivery location for other deliveries (and coordination with road officers in that patrol zone who actually know the community);
   - Immediate coordination with UPS/FedEx to determine if there is an increased frequency of delivery to the suspect’s address and who is receiving property there;
   - Coordination with money transmitters for their physical or video evidence.
5. Establish a paper trail through legal processes (court order, subpoena, FACTA requests) pointing to a location in the jurisdiction you are requesting to take over the investigation.
6. Build rapport by working with a lead agency unit or individual early in the investigation to request local data on subjects, locations, businesses, etc.
7. Link other cases in that jurisdiction - this might hold the possibility of increasing clearance rates too.
8. Build loss value.
The Victim is a Partner in the Investigation

Identity crime investigations are complex because there are usually no witnesses or physical evidence at the crime scene, which may be on the other side of the world. That said, the victim is a source of much of the most important information in the investigation, and is often motivated to help law enforcement by supporting it.

Victims have an overwhelming need to be actively involved in the case because ultimately it is their reputation, their credit, and their family’s livelihood on the line. Although this is the investigator’s case and the officer must maintain control, giving the victim some sense of empowerment will help develop information and evidence for a successful conviction.

“Nuts & Bolts” of Investigation:

1. Stages of Identity Crime

When initiating an investigation of identity crime, it may be helpful to consider the four major stages of the crime:

<table>
<thead>
<tr>
<th>Crime Stage</th>
<th>What Happens</th>
<th>What the Victim May/ May Not Notice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Victim’s information is collected by the criminal (theft)</td>
<td>Victim’s personal information and identity are compromised.</td>
<td>• Lost wallet, purse, credit card, driver’s license, luggage, passport, etc. • Credit card, mortgage, bank statement or other bill missing from or never received in the mail • Had wallet or purse stolen, car/house broken into • Personal computer security has been compromised • Company that had its data breached notifies the victim</td>
</tr>
<tr>
<td>Criminal converts that information</td>
<td>Information becomes new false identity.</td>
<td>• No noticeable event</td>
</tr>
<tr>
<td>The information is passed along</td>
<td>The victim’s identity is attached to a new individual.</td>
<td>• Not noticeable until used</td>
</tr>
<tr>
<td>The new identity is put to use (fraud)</td>
<td>The identity is used for committing fraud and other crimes.</td>
<td>• Contacted by debt collectors • Funds are missing from checking or savings accounts • Fraudulent charges on credit cards, etc. • New accounts they did not open appear on their credit report, or they receive the bills • Arrested for crime they didn’t commit</td>
</tr>
</tbody>
</table>
2. Investigative Steps

Not all criminal investigations require in-depth documentation, but the nature of identity crime is such that it warrants superior organization not only to help investigators make progress toward arrests, but also for the purposes of helping victims and preparing for prosecution.

Remember that you will have to explain the case to a prosecutor who will in turn have to explain it to a jury. Due to the complexity of the cases, it is very helpful to keep detailed and organized case files to make sure that it is possible later to tell a coherent and logical story about the crime and the suspect’s involvement.

The organizational methods often will benefit by use of a spreadsheet or other case management software. There are courses available through federal and regional law enforcement agencies that teach these methods. They are not designed solely for identity crime investigations but are significant in the investigation of all organized criminal enterprises.

The following basic investigative steps are recommended once a reported complaint moves into an identity crime case.

Investigative Steps:

- Review the case
- Re-interview the victim
- Authenticate the crime
- Begin analysis
- Pursue initial leads
- Gather evidence - be timely and careful with it
- Create a timeline
- Build the cast of characters
- Conduct link analysis
- Create an evidence book with an index
- Look for common points of compromise across different crimes and/or additional victims
- Collaborate & share information
## Investigative Steps (cont’d)

<table>
<thead>
<tr>
<th>Step</th>
<th>What Happens</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Review the Case</strong></td>
<td>The investigator reviews the details provided in the initial interview with the victim. If the detective was the initial interviewer he/she is re-checking known facts. If he/she is tasked with the follow-up investigation, he/she will want to become familiar with the facts reported. The review is also intended to discern that the facts meet the elements of the crime classification and help decide what information is needed from the victim in the next interview.</td>
</tr>
<tr>
<td><strong>Re-Interview the Victim</strong></td>
<td>The follow-up interview is conducted to determine if the facts have changed (like in an incident of false reporting), or new facts have been learned by the victim. The victim can clarify any information in the initial report that may be unclear. The detective will also have the opportunity to establish that the victim has in fact followed up on the steps he/she was advised to take at the initial interview.</td>
</tr>
<tr>
<td><strong>Authenticate the Crime</strong></td>
<td>The re-interview may have provided more information to help determine the true nature of the complaint and identify whether or not the incident involves: • False reporting • Civil dispute • Domestic dispute • Misidentification • Another (additional) crime</td>
</tr>
<tr>
<td><strong>Begin Analysis</strong></td>
<td>Based upon the known facts, begin to state the “who, what, where, when, why, and how” of the case. Like in any investigation, this will be a continuous process as evidence and leads are tracked down and results are analyzed. <strong>Who:</strong> Victim information and suspect information, if known <strong>What:</strong> Purchase, theft, etc., using victim’s identifiers. Which identifiers were used? <strong>Where:</strong> Merchant locations or IP addresses logged, delivery addresses, land line phone numbers, etc. <strong>When:</strong> As per billing/account statements, etc. <strong>Why:</strong> Motive <strong>How:</strong> Were the identifiers compromised? Were the identifiers used? e.g., Internet, phone purchases, benefits</td>
</tr>
<tr>
<td><strong>Pursue Initial Leads</strong></td>
<td><strong>What point in the criminal enterprise is exposed?</strong> Where do the facts thus far put us in the criminal enterprise? Merchandise drops may indicate the location or a place to start looking for those involved in passing off the identities for profit. IP addresses may indicate where the computer was located that was involved in the passing of identities. If the locations are outside your jurisdiction what is the next step?</td>
</tr>
</tbody>
</table>
Investigative Steps (cont’d)

<table>
<thead>
<tr>
<th>Step</th>
<th>What Happens</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gather Evidence - Be Timely and Careful with It</td>
<td>Through victim’s consent or through subpoena/court order, investigators will need documentation from financial institutions and government agencies.</td>
</tr>
<tr>
<td></td>
<td>The investigator will begin creating a paper and digital trail of physical evidence. Do not overlook the traditional investigative skills learned through training and experience. Not all documents in the trail will be digital. Paper document evidence will exist and is subject to forensic treatment. Security surveillance video of the target and surrounding businesses still exists and suspect photo arrays still need to be shown to witnesses. The investigator/detective still needs to hit the streets and look for witnesses and other physical evidence that may put a subject at the scene where an ATM skimmer may have been employed, or a computer used at an Internet café.</td>
</tr>
<tr>
<td>Create a Timeline</td>
<td>Timelines are important in that they produce a visual concept of the incident as dates and time are concerned. Identity crimes are complicated, and a timeline releases the investigator from committing these details to memory when it comes to evaluating data and conducting interviews. An examination of the timeline reveals any lack of detail that may need to be addressed and eventually gives supervisors and the prosecutor the ability to understand the case. Each entry into the timeline should note the source of the information and should only deal with event time.</td>
</tr>
<tr>
<td>Build the Cast of Characters</td>
<td>Keep track of all the actors, locations and businesses involved. Each needs to be identified by their various identities or appearances. Listing out this information frees up the investigator from memorizing all the individual details and connections and where the information is located for reference during the investigation.</td>
</tr>
<tr>
<td>Conduct Link Analysis</td>
<td>Use your department resources as well as FTC’s ID Theft Clearinghouse on Consumer Sentinel <a href="https://register.consumersentinel.gov/">https://register.consumersentinel.gov/</a> and the U.S. Attorney’s Office NICLE program <a href="http://www.usdoj.gov/ao/PAE/News/Pr/2008/jul/niclerlease.pdf">http://www.usdoj.gov/ao/PAE/News/Pr/2008/jul/niclerlease.pdf</a>. Putting all the information together in a manner that relates persons, places and events through phone records, IP addresses, etc., is a challenge that can overwhelm a single detective assigned to a complex case. Nevertheless, it is an important aspect that is required in some cases to take down a whole criminal organization right to the top.</td>
</tr>
</tbody>
</table>

---

As more commerce is being conducted on the Internet it is important to act immediately to preserve evidence or information that may be stored on digital media. Information may have a short shelf life in these circumstances due to the ever expanding need for increased storage media. Security video is also subject to the demands of storage needs as it too becomes more digital based. Older technology such as video tape may have an even shorter life span as equipment ages and becomes obsolete. Paper documents as well as other physical evidence should be treated as in other crimes to preserve it for prosecutorial value.
# V. Investigating Identity Crime

## Investigative Steps (cont’d)

<table>
<thead>
<tr>
<th>Step</th>
<th>What Happens</th>
</tr>
</thead>
</table>
| Create an Evidence Book with an Index | - Include your timeline and cast of characters.  
- Note any follow-up steps on missing or newly important documents including:  
  - Customer record  
  - Signature card  
  - Credit application  
  - Transaction history  
  - Payment history and method (online or mail)  
  - Addresses and telephone numbers associated with the account  
  - Additional authorized users  
  - Videos of any in-person transactions |
| Look for Common Points of Compromise Across Different Crimes and/or Additional Victims | Remember that these crimes are rarely isolated, and that they often have companion crimes, as they are instrumental in concealing another crime or in creating financial gain for the perpetrator. |
| Collaborate & Share Information | As the case progresses, the requirement for outside agencies and investigators from financial institutions assisting the investigation will become necessary. This necessity will be based on your agency’s jurisdiction or an element of the crime or ability to access persons, places or things outside its authority. In some circumstances a federal agency may be the correct organization to conduct the primary investigation. |
3. How Information is Obtained and Used

How do perpetrators acquire identifying information belonging to victims? It may be helpful to consider the many ways that the information is obtained:

<table>
<thead>
<tr>
<th>Method</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stealing</td>
<td>Purses, wallets containing credit cards, driver’s license, Social Security card. Mail: perpetrators complete a false change-of-address form, obtaining credit information, convenience checks, etc., from the victim’s mail or the victim’s financial institution. Trash/Dumpster Diving: Identifying information from discarded documents, e.g., credit card statements.</td>
</tr>
<tr>
<td>Breaking and Entering, Burglary</td>
<td>Financial records and other personal information about accounts. Stolen computers have personal information stored inside.</td>
</tr>
<tr>
<td>Impersonating</td>
<td>Posing as a landlord, potential employer, etc., the perpetrator gains access to a credit report. Obtaining information through friends or employers of the victim (e.g., gaining access to HR files).</td>
</tr>
<tr>
<td>Pretexting</td>
<td>Contacting the victim or their financial institution under a pretext and asking for, and gaining, the personal information.</td>
</tr>
<tr>
<td>Shoulder Surfing</td>
<td>Observing the victim while he/she uses personal information and making a copy of it.</td>
</tr>
<tr>
<td>Skimming</td>
<td>Using an electronic device to lift data from a credit or debit card and “swiping” the information for transfer to a counterfeit card.</td>
</tr>
<tr>
<td>Purchasing</td>
<td>Perpetrators may purchase information, even legally, and use or sell it for identity crime.</td>
</tr>
<tr>
<td>Gaining Unauthorized Electronic Access</td>
<td>Exploiting computer network vulnerabilities to obtain unauthorized access (steal) sensitive personal information. Vulnerabilities include things such as weak passwords, poorly protected wireless transmissions, personal information that is not adequately segmented from the rest of a network or the Internet, or not adequately logging access to networks or monitoring logs.</td>
</tr>
</tbody>
</table>
V. Investigating Identity Crime

Once obtained, how is the information likely to be used?

Here are some of the most common ways that perpetrators use stolen information:

<table>
<thead>
<tr>
<th>Personal Information: Name, Date of Birth, Social Security Number</th>
<th>This is sufficient to open a new credit card account, which could be mailed to a false address, and therefore used until the victim becomes aware of it. Other uses include: opening a new bank account and writing bad checks, obtaining loans, signing leases, and filing for bankruptcy in the victim’s name (to avoid paying debts incurred, or to avoid eviction from house/apartment obtained in the victim’s name), mortgage fraud, medical and/or other insurance fraud, etc. Also used for criminal concealment, fraudulent obtaining of employment or government benefits as well as committing tax fraud. Many of these crimes can include creating altered or forged driver’s licenses, Social Security cards, passports and other identity documents.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card Numbers</td>
<td>Making purchases, sometimes including calling the credit company and changing the mailing address to delay the victim’s knowledge of bad charges. Requesting “convenience checks” which can be written for cash against a credit card account. Again, often after changing the mailing address or having access to the victim’s mailbox. Committing balance transfer fraud - using the victim’s account to do a balance transfer to an account opened and controlled by the defendant, then using the cash feature of the card to withdraw funds. This method allows a $5,000 credit limit card to suffer a $100,000 loss.</td>
</tr>
<tr>
<td>Counterfeited Debit and/or Credit Cards</td>
<td>Enables the perpetrator to deplete all accounts.</td>
</tr>
</tbody>
</table>

4. Investigative Tools and Techniques

**Tools**

In identity crime, it is rare that the perpetrator is caught on his/her first offense and is highly likely that the crime the victim is reporting is not an isolated incident. It may also be helpful to remember that the victim often knows the perpetrator and/or has provided him/her with the information in the first place, believing it was to be used for a legitimate purpose.

According to an FTC survey from 2006, in 16% of all cases, the victim personally knew the person who had misused their personal information. Of those who could personally identify the perpetrator, 6% said a family member or relative had misused their personal information; 8% named a friend, neighbor, or in-home employee; and 2% said the thief was a co-worker.18

---

The first step will be identifying the perpetrator. To aid in identification, study the crime and determine the two weak points for an identity crime - the contact point, or means by which the perpetrator contacted the victim, and the drop point, or physical location where an item, record, card or merchandise was sent. For example, if the victim information was used at a bank Web site to open a credit card account, the bank site will record the IP address of the computer used to open the account, and will have a verified e-mail to send account information. A search warrant for records can help reveal the suspect’s Internet service provider and physical location of access.

If the account was opened over the phone, most bank sites will record the ANI or caller ID number of the call made to open the account. The telephone number provides a basic place to start the investigation.

Drop points can be shipping addresses for merchandise, mailing addresses for statements, stores where the cards were or are being used, or ATMs where money is withdrawn. The drop point helps to identify the physical location of the thief and can provide valuable working points for search warrants. Don’t forget to check these locations for video of the transactions or for the records of delivery.

In addition, it is important that in any investigation all of the computer forensic evidence is gathered and analyzed. The hard drive of a computer (and other digital media) offer important evidence that can be quite fragile. It is helpful to reach out to specialists to help with the seizure and analysis of such evidence. Contact the National White Collar Crime Center for help online http://www.nw3c.org or by calling (804) 273-6932.

Many of the investigative techniques useful in other criminal investigations can serve to gather evidence in identity crimes as well. Important information can be found in:

- Suspect’s trash.
- Suspect’s residence or automobile.
- Suspect’s computer, cellular phone, PDA or other wireless device.
- If you are able to get IP addresses linked to the application for fraudulent new accounts, it may be possible to get a court order for the subscriber information from the financial institution.

Investigators should not overlook using officers from other agencies as a resource when they hit a roadblock in an investigation. Each identity crime case has different nuances, and working collaboratively can leverage the collective wisdom, skills and experiences of many of your colleagues in neighboring agencies.

Sometimes identity crimes are deceptively low-tech. Consider the suspect who writes down a credit card number and name, then uses the phone book to get a matching address, then uses that information to buy things over the telephone.

Investigators may also want to pay special attention to mapping the small crimes in a jurisdiction. Using a pin map, it may be possible to see patterns in where credit information is routinely swiped, stolen and used. Postal inspectors can be brought in to help as well.
Other agencies can help to gather information leading to the suspect:

**National Crime Information Center (NCIC)**

Has the suspect been arrested using the victim's identity? Has he/she been arrested for any other identity crimes? A check of NCIC, a computerized index of criminal justice data such as criminal record history, fugitives, stolen properties, missing persons, etc., may provide useful information. It is available to federal, state, and local law enforcement and other criminal justice agencies and is operational 24 hours a day, 365 days a year: [http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm](http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm).

**U.S. Postal Inspection Service**

A mail cover is the process by which a nonconsensual record is made of any data appearing on the outside cover of sealed or unsealed mail; or by which a record is made of the contents of any unsealed mail, as allowed by law, to obtain information to protect national security; locate a fugitive; obtain evidence of the commission or attempted commission of a crime; obtain evidence of a violation or attempted violation of a postal statute; or assist in the identification of property, proceeds, or assets forfeitable under law. A mail cover may be helpful in investigating identity crimes. Visit this Web site for more information on requesting a mail cover: [http://www.usps.com/privacyoffice/intelligentmail.htm](http://www.usps.com/privacyoffice/intelligentmail.htm).

Postal Inspectors can also help with information about change of addresses the suspects may have made using the victim’s information or their own. Also, if the suspect is using a Post Office Box at either the Post Office or with a Commercial Mail Receiving Agency (CMRA), a Postal Inspector will be able to help you obtain the information used to open the P.O. Box.

**Registry of Motor Vehicles**

Did the suspect obtain a driver’s license under the victim’s name/information?

**Privately Operated Databases**

Techniques

The Preliminary Investigation

Identity crimes are rarely contained in one jurisdiction. Every case requires investigators to determine the point of compromise of the victim’s identity - that is where the offender may have obtained the victim’s identification information. This will help lead to possible suspects, and often to additional victims.

Properly structured preliminary investigation saves investigative time, involves the victim in resolution of the theft, and lays the foundation for prosecution.

The investigation starts with the victim’s report of the crime. As mentioned in previous sections, victims need to help prepare for the investigation by gathering the following:

• Date of birth, driver’s license number, Social Security number, telephone numbers (work, home, and cellular), and e-mail addresses of every victim in the household;
• A recent copy of at least one of their credit reports generated since the crime occurred;
• Account numbers involved in the theft and the names of primary and secondary account holders;
• When and how the fraud or theft was discovered, and under what circumstances the victim became aware of the identity crime;
• Exact locations (addresses, businesses, persons involved) where fraudulent use of the identity occurred;
• Name, addresses (home and work), phone numbers, date of birth of every person involved in the incident;
• Names of financial institutions the victim has notified of the theft, along with the names, addresses, and phone numbers of customer service representatives or investigators who accepted the report, the dates and times of the reports, a brief summary of the conversation, and copies of any e-mail messages or faxes sent to or received from the financial institutions;
• Photocopies of any letters, account statements, and other documents associated with the case;
• A chronological log of the theft and the victim’s actions since discovering it, to include information about the discovery of theft or fraud, possible locations of the theft, and names or descriptions of persons around when the theft might have occurred.

The Federal Trade Commission has created a Universal ID Theft Complaint Form to record most of the details listed above that the victim knows about the crime. This form can be completed online at www.ftc.gov/idtheft.

During the early stages of the investigation it is important to determine the motive. The motive will help direct the investigation. The motive for financial crimes is usually greed, drugs or revenge. Determining the motive requires investigators to conduct a detailed interview with the victim.

The U.S. Secret Service has developed a questionnaire filled with a variety of useful information to the investigator for victims to fill out that can be used as a valuable tool at this stage of investigation. It is available as part of Appendix A of this toolkit.
The Continued Investigation

Next steps taken by the investigator should be to examine all financial and credit bureau documents. These documents are useful and vital pieces of evidence to tie suspects to the crime and eventual prosecution. For help with this step, the investigator can contact appropriate state and local agencies, as well as the following federal agencies:

- Federal Bureau of Investigation
- Secret Service
- Social Security Administration
- Postal Inspection Service
- Bureau of Immigration and Customs Enforcement

The Secret Service has a program called the eInformation Network, an Intranet site that is available, for free, to law enforcement agencies and investigators. It is an important tool for investigators in accessing bank and credit card information. For more information, go to www.einformation.usss.gov. The resources available on the Secret Service eInformation Network include the following:

- Bank identification number search
- Credit card and skimming information
- Counterfeit check database
- Genuine and counterfeit identification document database
- Cyber crime resources
- Fraudulent document database

Financial Crimes Enforcement Network (FinCEN) is another excellent network for investigating identity crime and other financial crimes. FinCEN links databases maintained by the law enforcement, financial and regulatory communities. Its purpose is to collect, analyze, and share information with law enforcement agencies. FinCEN accesses approximately 37 different and independent databases in three main categories: law enforcement, financial and commercial. The databases include AutoTrack, LexisNexis, the Social Security Administration Death Master File, and the Drug Enforcement Administration, Federal Bureau of Investigation, and Internal Revenue Service databases, to name a few. Visit the FinCEN Web site at http://www.fincen.gov.

Another valuable tool for investigators is the use of informants. Investigators should develop informants from potential suspects during the investigation. Investigators should also identify possible informants by using intelligence from other law enforcement agencies or the private sector.

A good technique to develop informants is using other people who participated in some capacity in the identity crime, such as a store employee who sold goods knowing the suspect was using someone else’s identity.

Investigators should consider using other means to gain access to privileged information, including obtaining federal cooperation and funds, seeking state and federal RICO statute investigations, or using forfeiture statutes to gain access to financial records. Above all, investigators should always follow the money - this is an appropriate investigative technique in any financial crime.
Other things to remember:

- Contact the FTC Consumer Sentinel Network and search the database for investigative leads at www.ftc.gov/sentinel.
- Contact other involved or potentially involved law enforcement agencies for collaboration and avoidance of duplication.

Obtaining Financial Information

Accessing financial information for any fraud case can be a daunting task for the investigator, especially when cooperation is lacking. It is imperative that the investigator gains cooperation from both the victim and the financial organization(s).

There are three ways of getting the financial information needed for an identity theft case: (1) search warrant, (2) subpoena power (3) or consent. Consent is the simplest and most cost-effective.

Ask the victim to begin gathering and providing documentation to include the following:

- Bank and credit card statements
- Letters from creditors
- Merchant account statements
- Any other financial documentation related to the crime

Ask the victim to obtain and voluntarily provide the credit reports from the three major credit bureaus (Equifax, Experian and TransUnion). Under the 2003 amendments to the Fair Credit Reporting Act, the victim must contact their creditor’s fraud or security department in writing to request that they send transaction records related to the crime to the investigator. Otherwise, a subpoena is needed from the courts.

Advise the victim to keep a log or a diary of everything they do or everyone they talk with regarding the crime. This can be used as part of the victim impact statement during any subsequent court proceeding. The FTC or ID Theft Resources Center provides valuable information on how victims can organize their identity crime cases.

The investigator should contact the financial institution or merchant security departments and ask for (or subpoena) documentation on all fraudulent or suspect accounts.

Identifying Additional Victims

There are many reasons why an investigator should locate and identify additional victims, but among the most important is to ascertain if there is a larger, organized ring victimizing the community. One way of doing this is by querying the FTC Clearinghouse for other reported complaints that may be related to the case. Investigators can also contact other agencies in the area to determine if there have been similar crimes reported and possibly connected. If that is the case, these agencies can combine resources and personnel into a task force to combat the crime.
Case Preparation

Filing the case criminally can be another daunting adventure. However, if the case is well prepared, the criminal prosecutor will be better equipped to file the case. As noted earlier, the best way of preparing the case is having the victim play a role by taking and keeping notes or a diary, requesting and collecting financial information regarding the crime and taking an overall interest and partnership in the case.

The key to getting an identity crime case filed and getting a successful conviction is organization. It is also helpful if the investigator has an outline of the particular law that is sought for filing when dealing with district attorneys who are unfamiliar with the law. List the requested charges and enhancements on the charging sheet, along with any additional charges.

A case synopsis is also a good way to give the prosecutor a summary of your case. It is your case’s “facts-at-a-glance” sheet. Tailor this sheet to match what the prosecutor looks for in a case. This is helpful when your prosecutor is trying to decide whether to prosecute your case, and also when you share your case information with other agencies.

Interrogating an Identity Crime Suspect

Because of the prevalence of identity crime, many investigators find themselves having to interrogate a suspect on this issue. Identity crime is an unusual offense because it is not only a crime but also an MO to commit other crimes. The first consideration, therefore, is to determine in what offense to accuse the suspect of involvement. The general guideline here is to base the accusation on the strongest evidence. For example, if there is strong evidence indicating that a suspect (using someone else’s identity) made fraudulent credit card purchases, the confrontation statement should only address the illegal purchases. At a later stage the investigator can develop the details of how the suspect obtained the fraudulent credit card. This approach is similar to the one investigators would take in an arson-homicide case, in which it is best to confront the suspect with the killing and later develop the details of starting the fire to cover up the homicide.

When dealing with multiple crimes, it is easier to persuade the suspect to tell the truth about one crime at a time. Once a suspect confesses to one crime, information about other illegal activity is usually forthcoming. On the other hand, an investigator is making this task much more difficult by initially confronting the suspect on both crimes: “Brian, our investigation clearly indicates that you fraudulently obtained a loan using someone else’s identity and then illegally defaulted on the loan.”

When the strongest evidence does point to identity crime, this should then be the focus of the interrogation: “Mark, our investigation clearly indicates that you obtained a passport and driver’s license using someone else’s information.” In this example, it would be appropriate to use a transition statement that addresses the purpose for the suspect’s actions: “I wanted to talk to you about this because, right now, we don’t know why you got these documents.” A theme can then be developed. Is the suspect linked, for instance, to international terrorists who sought to use the documents to board an airplane that they then would hijack and crash into the White House? Or did the suspect want to use the documents to establish a separate identity for tax purposes, to hide assets in a divorce, to escape government intrusion, or to escape from gambling debts or a vindictive ex-wife? The investigator can follow whatever line the facts of the case suggest.
Another theme investigators can touch on during interrogations of identity crime suspects is the carelessness of the credit card companies and banks that make identity theft so easy and so tempting: “George, I realize this thing is not entirely your fault. Banks and credit card companies are so eager to get customers that they rush applications through without really properly checking on information. In addition, they entice honest people like you to do something like this through their advertisements where they promise quick approvals and an application that asks for practically no information. A lot of these companies don’t even meet with their customers, and everything is done over the Internet or through the mail. If they really cared about something like this happening they would not make it so easy to do.”

One more angle to consider is how the suspect got the victim’s personal information. In most cases this information is obtained through the victim’s carelessness or sold on the street or over the Internet. If interrogators believe the suspect happened upon the victim’s personal identifying information, they can blame the victim who left important documents in plain view where the suspect couldn’t help but see it and then act on it. If they believe the suspect purchased the information, they can blame the person who sold it to the suspect for approaching the suspect and putting pressure on him to buy it.

In other cases, it may be appropriate to blame curiosity and the media. The line of questioning would go something like this: “Joe, I think what happened here is that you heard on TV or read in the newspaper how easy it is to get a credit card using someone else’s personal information. Just out of curiosity you decided to test the system to see if it was as easy as everyone said it was. After submitting the simple application, to your amazement, they issued you a card. Under normal circumstance you probably would have thrown the card away and never used it, but just when the card arrived so did other bills and you gave in to temptation and put charges on your new credit card. I would hate to think that you went into this whole thing with the greedy intent of maxing out the card by buying frivolous things that you didn’t really need.”

The following are possible alternative questions to consider for identity crime cases:

- “How many false identities (false credit cards, fraudulent loans) have you established? Dozens or just a few?”
- “How much have you charged to this card? Did you charge the maximum limit, $10,000, or was it less than that?”
- “Are you a member of an organized network, perhaps with a terrorist affiliation, or did you just do this to hide from your ex-wife?”
- “Did you pay money to bribe people to get this credit card, or did they simply accept your application at face value?”

Confessions follow a hierarchy. It is psychologically easiest for a guilty suspect to admit what they did. Second, they may or may not truthfully acknowledge the method or planning involved in their crime. The most difficult aspect of a crime to reveal is the true motive behind the act. For this reason, interrogators ought to focus on the crime that was committed through identity fraud and develop secondary issues after the suspect has confessed to the original issue.

Source: “Interrogating a Suspect on the Issue of Identity Theft” (December 2003) was prepared by John E. Reid and Associates Inc., and published online as part of the firm’s Monthly Web Tip series www.reid.com. It is revised and printed here with the firm’s permission.
### 5. Troubleshooting

<table>
<thead>
<tr>
<th>Obstacle</th>
<th>Solutions, Tips, Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks and credit companies won’t release the financial information and</td>
<td>FCRA Section 609(e) states that it is the victim’s right to get copies of applications and business records that relate to the victim’s identity theft without a subpoena from any company that transacted any business with the thief who was using the victim’s identity. The victim can also require the company to provide a copy of all of the records to a law enforcement officer. All copies must be provided at no charge to the consumer or the officer. ANY request, if it contains the enclosures required by law (including a law enforcement report), triggers the Section 609(e) requirement on the company.</td>
</tr>
<tr>
<td>records needed for the investigation to anyone but the victim</td>
<td></td>
</tr>
<tr>
<td>We have no dedicated investigators and/or specialized units to help with</td>
<td>• Consider the VIPS solution - using citizen volunteers including retired law enforcement and bank security officials. For example, the city of Pasadena (CA) C.R.E.D.I.T. program expanded the department’s resources to deal with these crimes and provides much needed support to both victims and investigators. <a href="http://www.cityofpasadena.net/police/media/MediaReleases/2004/2004%20-%20C.R.E.D.I.T.%20Program%208-3.pdf">http://www.cityofpasadena.net/police/media/MediaReleases/2004/2004%20-%20C.R.E.D.I.T.%20Program%208-3.pdf</a></td>
</tr>
<tr>
<td>these crimes</td>
<td>• Work closely with affected financial institutions; bring their investigators in as partners that will expand your resources and improve your access to key information.</td>
</tr>
<tr>
<td></td>
<td>• Contact the National White Collar Crime Center [NW3C] <a href="http://www.nw3c.org/isupport/overview.cfm">http://www.nw3c.org/isupport/overview.cfm</a> that provides support services for member agencies who are involved in the investigation or prosecution of a white collar, high tech or cyber crime. Services include analytical support, public database searches and case funding. Analysts can assist in establishing financial transaction patterns, developing links between criminal targets and associated criminal activity and providing link charts, timelines and graphs for court presentations.</td>
</tr>
<tr>
<td></td>
<td>• In cases of skimming and other high tech crimes, partner with your local IT companies as an additional resource.</td>
</tr>
<tr>
<td>These crimes take too much time to investigate</td>
<td>Visit <a href="http://www.gethuman.com">www.gethuman.com</a> to get quickly to an agent (instead of a voice mail menu). This should save some time and assist smaller departments to get more quickly to the people within financial institutions who can help.</td>
</tr>
<tr>
<td>The department does not collect information on these crimes; makes it</td>
<td>The U.S. Secret Service eInformation Network <a href="http://www.secretservice.gov/le_resources.shtml">http://www.secretservice.gov/le_resources.shtml</a> has contacts to many of the fraud investigators at financial institutions.</td>
</tr>
<tr>
<td>hard to track progress</td>
<td>As of now, the UCR coding for identity crimes is fraud. Departments seeking to report identity crime through UCR forms can attach information as comments, within the “open section,” on the crime report form.</td>
</tr>
</tbody>
</table>
6. Sharing Information

<table>
<thead>
<tr>
<th>Responding</th>
<th>Investigating</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local law enforcement must:</strong></td>
<td>Local law enforcement in partnership with:</td>
</tr>
<tr>
<td>a. take a detailed report</td>
<td>• Federal Bureau of Investigation <a href="http://www.fbi.gov">www.fbi.gov</a></td>
</tr>
<tr>
<td>b. provide victims with copies of the report</td>
<td>• The Federal Trade Commission <a href="http://www.ftc.gov">www.ftc.gov</a></td>
</tr>
<tr>
<td>c. help victims identify areas where they can turn for help with the recovery process</td>
<td>• Immigration and Customs Enforcement <a href="http://www.ice.gov">www.ice.gov</a></td>
</tr>
<tr>
<td></td>
<td>• Internal Revenue Service <a href="http://www.irs.gov">www.irs.gov</a></td>
</tr>
<tr>
<td></td>
<td>• Social Security Administration, Office of Inspector General (OIG) <a href="http://www.ssa.gov">www.ssa.gov</a></td>
</tr>
<tr>
<td></td>
<td>• U.S. Department of Justice <a href="http://www.usdoj.gov">www.usdoj.gov</a></td>
</tr>
<tr>
<td></td>
<td>• U.S. Department of Defense <a href="http://www.defenselink.mil">www.defenselink.mil</a></td>
</tr>
<tr>
<td></td>
<td>• U.S. Department of State <a href="http://www.state.gov">www.state.gov</a></td>
</tr>
<tr>
<td></td>
<td>• U.S. Postal Inspection Service <a href="http://postalinspectors.uspis.gov">http://postalinspectors.uspis.gov</a></td>
</tr>
<tr>
<td></td>
<td>• U.S. Secret Service <a href="http://www.ustreas.gov/usss">www.ustreas.gov/usss</a></td>
</tr>
</tbody>
</table>

The FTC has an Identity Theft Data Clearinghouse [www.ftc.gov/sentinel](http://www.ftc.gov/sentinel), a national database of more than 1.6 million identity crime complaints that allows search for suspect, identity theft victim, or defrauded company information across the country. Using the Consumer Sentinel Network, investigators can reach out to federal, state or local law enforcement officers in other jurisdictions to assist in your investigations or with your victims. Sentinel users can place alerts on suspects, companies or victims to let other law enforcers know that you have an active investigation on those targets. Users can schedule automatic searches on specific suspect information or companies they you are interested in and get e-mail notifications. Sentinel users can download the complaint data to their desktop to manipulate it or bring into their own data system.

The FBI hosts n-DEx - Law Enforcement National Data Exchange to facilitate information sharing among investigators [http://www.fbi.gov/hq/cjisd/ndex/index_home.htm](http://www.fbi.gov/hq/cjisd/ndex/index_home.htm).

The United States Secret Service offers a database of information, which includes contacts at financial institutions, a check fraud database, and a database of various electronic tools used by identity thieves, as well as free online training in electronic crimes Forward Edge II. [http://www.forwardedge2.com/](http://www.forwardedge2.com/).

The IACP and Bank of America have an award-winning forum for law enforcement to share ideas and information on [www.id safety.org](http://www.id safety.org).

- Sharing information is essential.
- Multiple agencies have a role in responding to, investigating and prosecuting crimes.

These crimes cannot be solved, and the victims cannot be restored, unless law enforcement is willing and able to participate in sharing information with each other as well as with other government agencies and financial institutions.

As a general rule, identity crimes cross the jurisdiction of multiple agencies, which underscores the necessity of good collaborative working relationships between local law enforcement and federal agencies.

Law enforcement networking sites and distribution lists are of great investigative value. The best way to get the sites from your area is by talking to other officers and investigators from financial institutions in your region. Most network with each other and would be happy to include you.

Visit Regional Information Sharing Systems (RISS) [http://www.iir.com/riss/default.htm](http://www.iir.com/riss/default.htm) to find your regional information sharing network. Recently, the United States Attorney’s Office, Eastern District of Pennsylvania and USPS launched the National ID Theft Law Enforcement Network (NICLE) which is available over RISSNet to all RISS members.

To identity thieves, everyone is just a number.