Office for Victims of Crime
Training and Technical Assistance Center

Identity Theft

1 in a series of 8 resource papers:

- *Child Abuse and Neglect*
- *Elder Abuse*
- *Homicide*
- *Human Trafficking*
- *Identity Theft*
- *Impaired Driving*
- *Intimate Partner Violence*
- *Sexual Assault*

OVC TTAC
OFFICE FOR VICTIMS OF CRIME Training and Technical Assistance Center

Identity Theft*

Identity theft has been called the fastest growing consumer crime in America.[1] In 2011, identity theft was the top consumer complaint reported to the Federal Trade Commission (FTC). Fifteen percent of consumers who contacted the FTC complained of identity theft.[2] Identity theft complaints increased tenfold between the years 2000 and 2008.[3] Millions of Americans become identity theft victims each year, and it is expected that identity theft rates will continue to rise.

From the perpetrator's perspective, identity theft is a low risk, high reward crime. Local law enforcement agencies have few resources dedicated to the investigation of identity crimes. As a result, the vast majority of identity thefts are not investigated. Most identity thieves are neither arrested nor charged. The initial acquisition of personal information may be as simple as rummaging through a victim's trash. Once personal information is obtained by identity thieves, they will continue using it until the victim takes action to make his or her personal information difficult to use. At that point, the identity thief simply stops using the information. For example, police in Lubbock, Texas arrested members of a husband and wife identity theft ring who kept stolen information from hundreds of victims stored in file cabinets.[4] Thieves may also sell stolen information on various Web sites accessible only to vetted criminals. In 2012, the Department of Justice shut down 36 Web sites where personal identifiers such as credit card numbers were bought and sold.[5]

The harsh reality is that millions of Americans will continue to become victims of identity theft each year with little hope that the perpetrators will be brought to justice. Identity theft leaves victims a legacy of frustration and financial problems with few services available to help.

Statistics

The following statistics come from "Crime Victimization in the United States: Statistical Overviews," which the Office for Victims of Crime prepared for National Crime Victims' Rights Week, 2012, and from the *Consumer Sentinel Network Data Book for January–December 2011*.[6]

- In 2010, an estimated 8.1 million adults, or 3.5 percent of the population, became victims of identity fraud, down from about 11 million in 2009.[7]

---

* This resource paper was authored in 2009 by Paula Pierce, Managing Attorney for the Victims Initiative for Counseling, Advocacy, and Restoration of the Southwest (VICARS) program. Reviewers included Linda Foley and Jay Foley, Identity Theft Resource Center, and Jaimee Napp, Identity Theft Action Council of Nebraska. Paula Pierce reviewed and updated content in 2012.

- In 2010, 14 percent of identity fraud victims knew the perpetrator. Of the over 5,000 people surveyed, 470 were victims of fraud and 29 percent had their Social Security number stolen.[8]

- In 2011, the Network received over 1.8 million complaints from consumers of which 15 percent were identity theft complaints, 55 percent were fraud complaints, and 30 percent were other types of complaints. Identity theft was the number one consumer complaint received by the FTC in calendar year 2011.[9]

- In 2011, 45 percent of identity theft victims who made complaints to the FTC reported that they contacted law enforcement, and of those, 70 percent notified a municipal police department; 57 percent indicated that a report was taken.[10]

- In 2011, scammers' use of the Internet to make initial consumer contact remained consistent (43% by e-mail and 13% through Web sites); however, scammers' use of telephone contact increased from 19 percent in 2010 to 29 percent in 2011.[11]

- In 2011, 23 percent of victims were ages 50 to 59, 20 percent were ages 40 to 49, 22 percent were age 60 or older, and 2 percent were 19 or under.[12]

- In 2011, the largest groups of identity theft victims were ages 20 to 29 (23 %) and 30 to 39 (21%). Fifteen percent of victims were age 60 and older, and 8 percent were under the age of 20.[13]

- In 2011, Florida ranked highest in the rate of identity theft complaints reported to the FTC (178.7 for every 100,000); Colorado ranked highest in the rate of fraud and other complaints reported to the FTC (573.7 for every 100,000).[14]

- In 2010, on average, it took a victim 33 hours to resolve identity fraud, up 12 hours from 2009.[15]

- For the first time, the largest number of identity theft complaints involved government documents fraud (27%). This represents an 11 percent increase from calendar year 2009.[16]

The Role of Victim Service Providers in Assisting Identity Theft Victims

It is important for victim service providers to know about identity theft because so many Americans become identity theft victims each year. It is also important that victim service providers be aware that victims of other crimes are at risk for becoming victims of identity theft. For example, victims of sexual assault, burglary, and robbery can become identity theft victims when personal information such as their wallet, purse, or documents are stolen in the course of the other crime; stolen information can be used by the primary

criminal or it can be sold. Domestic violence victims become identity theft victims at the hands of their abusers in order to keep them under control. Some identity thieves assume the identities of homicide victims. Identity theft is also used to perpetrate expansive crimes. Identity theft is connected to terrorism—e.g., the persons arrested in connection with the 9/11 attacks were also identity thieves. Stolen identities are used by human traffickers to shield their own identities and to provide working documents for trafficking victims, and stolen identities are used in every step of the drug trafficking process, from manufacture to laundering proceeds of sale. Because so many Americans become victims of identity thieves, victim service providers are increasingly likely to be asked to assist identity theft victims.

Victim service providers are called upon to assist identity theft victims in preserving their rights in the process of criminal investigation and prosecution as well as to assist identity theft victims in recovering their identities.

What Is Identity Theft?

The Federal Trade Commission defines identity theft as follows: Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes.

Many types of personal information have value to identity thieves including names, addresses, dates of birth, social security numbers, driver's license numbers, passport numbers, health insurance policy numbers, auto insurance policy numbers, checks, bank account numbers, credit card numbers and expiration dates, PIN numbers and access codes, and answers to security questions. As biometric identifiers (e.g., facial features, finger prints, iris scans) become more commonplace, thieves will undoubtedly attempt to find ways of stealing biometrics.

There are many kinds of identity theft. A description of some of the most common types of identity theft follows.

Existing account fraud happens when an impostor makes unauthorized charges on a victim's existing account. The accounts used by an impostor include bank accounts, credit card accounts, utility accounts, phone accounts, wireless accounts, and brokerage accounts.

New account fraud happens when an impostor uses a victim's personal identifying information to open new accounts. Like existing account fraud, the types of new accounts that impostors open using victim information include bank accounts, credit card accounts, utility accounts, phone accounts, wireless accounts, brokerage accounts, loans, mortgages, and home equity lines of credit.

Criminal identity theft is committed when an impostor gives a victim's identifying information to evade arrest. This type of identity theft results in the victim being charged with crimes that he or she did not commit and is usually discovered when the victim is arrested, is denied renewal of a driver's license, is denied employment on the basis of a criminal record (i.e., the impostor's), or is listed on a citation. Increased auto insurance or denied auto insurance is another indicator of criminal identity theft.

Employment identity theft is committed when an impostor uses a victim's identifying information, usually a social security number, in order to get or keep work.

Benefit fraud happens when an impostor obtains benefits using a victim's identifying information. Impostors may attempt to get food stamps, SSI, SSD, Medicare, or Medicaid by committing benefit fraud. It encompasses government documents fraud such as obtaining a driver's license using a victim's information or claiming a victim's federal income tax refund.

Medical identity theft is committed when an impostor uses a victim's identifying information or medical insurance in order to get medical care. Medical identity theft can be dangerous because it can result in the merging of a victim's medical record with that of an impostor.

Identity cloning is a means of committing identity theft that happens when an impostor assumes a victim's complete identity.

Synthetic identity theft is a means used by identity thieves to create a new identity by combining bits and pieces of personal information from more than one victim. For example, an impostor might use one victim's name and date of birth, a second victim's social security number, and a third victim's driver's license number.

The Federal Trade Commission collects and disseminates data on identity theft derived from consumer complaints. The table below illustrates the major types of identity theft that victims reported to the FTC in 2011.[17]

Type of Identity Theft	2011		Type of Identity Theft	2011
Credit card fraud	14%		Bank fraud	9%
Government document/ benefit fraud	27%		Loan fraud	3%
Employment related	8%		Criminal identity theft	1.2%
Utilities fraud including phone and cell phone	13%		Medical identity theft	1%

Anyone can become a victim, but certain groups are more adversely affected because they have access to fewer resources. The elderly, persons with limited English proficiency, minors, persons with disabilities, and the mentally ill are targeted by identity thieves and have more difficulty recovering their identity. For these victims, the assistance of a victim advocate is crucial.

What Is the Impact of Identity Theft on Victims?

Victims of identity theft suffer a range of problems. Victims are denied credit, employment, public benefits, driver's license renewal, and medical care. They can be arrested for crimes they did not commit, and they may be sued over debts they did not incur. Victims' credit ratings are lowered, and they may be harassed by creditors because of charges they did not incur or accounts they did not open. At a minimum, identity theft victims spend hours attempting to clear their records and repair the harm caused by impostors. Many victims spend months trying to mitigate the damage done, and some victims live with the consequences of identity theft for years. In its 2008 survey of identity theft victims, the Identity Theft Resource Center found that victims of existing account fraud spent an average of 58 hours attempting to repair the damage, while victims of new account fraud spent an average of 165 hours trying to recover.[18]

Identity theft may be committed by a family member, friend, or caregiver, or the crime can be committed by organized rings of identity thieves. Organized identity thieves treat victim-identifying information as a commodity to be bought and sold, which puts their victims at risk of repeated victimization. These victims clear their records from the initial identity theft; then, months or years later they are victimized again.

In addition to devastating financial harm, identity theft victims suffer emotionally. For several years, the Identity Theft Resource Center performed a yearly survey on the emotional impact of identity theft. Respondents to the 2008 survey reported feelings of frustration, embarrassment, anger, hopelessness, betrayal, loss of innocence, rage, and suicidal feelings.[19] Family and friends rarely understand the strong emotions that victims experience, which compounds a victim's frustration. When the impostor is a victim's friend or family member, the emotional impact of the crime is heightened. Elderly victims and child victims are most often victimized by caregivers or relatives. Having to depend on the identity thief for personal care is especially traumatizing to elderly victims.

Identity theft is a form of financial exploitation. When the victim is a minor or elderly, identity theft may trigger the duty to report the crime to adult or child protective services agencies.

How Does Identity Theft Occur?

Thieves steal personal identifying information in a number of ways, both low and high tech. Thieves rummage through trash and unlocked mailboxes looking for documents or mail containing account numbers and social security numbers. Stealing wallets, purses, and laptop computers is another method used to gain personal identifying information. Thieves use fraudulent schemes such as phishing, e-mails, or telephone calls to trick consumers into providing their personal identifying information. High tech devices called skimmers can be used to capture the information contained in the magnetic strips of credit, debit, and ATM cards. Skimmers are so prevalent in the restaurant industry that some states require restaurants to post signs warning employees that skimming credit cards is illegal. Computer hackers harvest personal identifying information from unprotected computer networks. Additionally, thieves may obtain information by wardriving, that is, searching for unprotected wireless Internet connections by driving around in vehicles outfitted with specialized equipment.

Once thieves gain access to personal identifying information, they use it to purchase goods and services using victims' existing accounts, open new financial accounts or credit card accounts, change mailing addresses on victim accounts, get loans and mortgages, file bankruptcy, obtain employment, evade law enforcement, obtain public benefits or medical care, and finance other types of criminal activity.

How To Respond to Identity Theft

Identity theft intersects the criminal and civil justice systems. Victims must avail themselves of both criminal and civil laws to be made whole. Criminal laws define identity theft and prescribe punishments for the crime, whereas civil laws provide the means to repair the victim's credit and recover his or her identity.

Rights of Victims in the Criminal Justice System

Prior to 1995, most individual victims of identity theft were not considered victims under the law. Instead, law enforcement agencies and courts considered banks, credit card issuers, and creditors to be the victims of identity theft. This changed in 1998 with the enactment of the Identity Theft and Assumption Deterrence Act. This law makes identity theft a federal crime against both consumers and businesses. The statute defines identity theft as when a person knowingly possesses, transfers, or uses another person's identification without authority and with the intent to commit, aid, or abet unlawful activity. A few years later, Congress passed the Identity Theft Penalty Enhancement Act of 2004. This statute imposes tougher penalties when identity theft is committed in conjunction with terrorism and upgraded identity theft committed in conjunction with certain federal offenses to aggravated identity theft. The Identity Theft Enforcement and Restitution Act of 2008 eliminated causation of $5,000 or greater in damages as a

prerequisite for the prosecution of computer crimes. It makes it a felony to damage 10 or more computers used by the federal government or financial institutions in 1 year. The statute also allows identity theft victims to recover restitution for their time spent remediating the harm caused by identity thieves.

The Justice for All Act guarantees crime victims the right to be reasonably protected from the accused; to receive reasonable, accurate, and timely notice of court proceedings; not to be excluded from court proceedings; to be reasonably heard at any public proceeding; to confer with the government's attorney; to full and timely restitution; to proceedings free from unreasonable delay; and to be treated with fairness and with respect for their privacy and dignity.[20] These rights apply to identity theft victims as they do to any other crime victims; however, some states exclude identity theft victims from the rights granted in their state crime victims' rights statutes.[21] Additionally, most states do not allow identity theft victims to receive crime victim compensation to reimburse their losses.

Fewer than 1 percent of identity thieves are arrested or charged. In those cases where an arrest is made, the victim advocate's role in the federal system is similar to the advocate's role for victims of violent crimes. The advocate should inform the victim of his or her rights under the Crime Victims' Rights Act and assist the victim in invoking those rights. Victim service providers should be especially alert to assisting identity theft victims in making victim impact statements and in making requests for restitution. Identity theft victims have the right to obtain restitution for both their monetary losses and the time spent recovering their identity and repairing their credit. However, victims must submit proof of their expenses and their time in order to receive restitution. The guidance of a victim service provider is invaluable to these victims.

Civil Laws – The Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) gives guidance to credit reporting agencies regarding their handling of consumer credit information. In 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACTA), which added identity theft protections to the FCRA. FACTA—

- Requires credit reporting agencies to provide consumers one free credit report per year.
- Allows consumers to request that the first five digits of their social security numbers be removed from their credit reports.
- Requires creditors and other businesses to take reasonable steps to protect consumer information from unauthorized access.
- Allows identity theft victims to place a fraud alert on their accounts and credit reports for 90 days extendable to 7 years.

- Allows identity theft victims to block any portion of their credit report attributable to identity theft.
- Allows active duty military personnel to place an alert on their accounts and credit reports renewable yearly while serving outside the U.S.
- Requires credit reporting agencies to give identity theft victims a written summary of their rights upon request.
- Requires businesses that issued accounts or credit to an imposter to provide account documentation to the identity theft victim if requested in writing.
- Requires collection agencies to report identity theft to creditors and provide information about the alleged debt to the identity theft victim.
- Prevents a creditor from placing a debt for collection after being notified that the debt was incurred through identity theft.

Using the Fair Credit Reporting Act To Assist Victims

The FACTA amendments to the FCRA outline a basic procedure that can be used by victims to remove fraudulent information from their credit reports. Early in the process, the victim should contact one of the three major credit reporting agencies by telephone or online and request two things: a fraud alert and a free credit report. The credit reporting agency must notify the other two agencies of the fraud alert. A fraud alert is a notation on a victim's credit report. Potential creditors that see a fraud alert must take reasonable steps to verify the identity of the credit applicant before giving credit. An initial fraud alert expires in 90 days; however, an identity theft victim may extend the fraud alert to 7 years by making a written request that includes a copy of the victim's police report. When ordered while placing a fraud alert, an identity theft victim's free credit report should arrive in a couple of weeks.

If an impostor has opened new accounts using the victim's identity, the victim should notify the businesses or financial institutions and request that the accounts be closed. If an impostor made unauthorized transactions on the victim's existing accounts, the victim should notify the businesses or financial institutions of the unauthorized activity. Telephone conversations should be followed up in writing. Federal banking laws limit the consumer's liability for unauthorized transactions when the unauthorized activity is reported in a timely fashion.

Once the credit report arrives, the victim should note all accounts and inquiries that do not belong to him or her, and gather all documents relevant to the identity theft so that a police report can be made. Prior to making a police report, every victim should be encouraged to make an online complaint to the Federal Trade Commission at www.ftc.gov/idtheft. The victim should print a copy of the online complaint and sign it in front of a notary public or in front of two witnesses. This document becomes an identity

theft affidavit. Victims can make complaints to the FTC by mail or by telephone; however, the victim will not be able to get a copy of the complaint.

Reporting Identity Theft to the Authorities

Many states have statutes that require police or sheriff departments to take identity theft reports where the victim resides. It is important to note that victims should report identity theft to their local law enforcement, and the victim should arrange to obtain a copy of the police report. In enacting FACTA, Congress envisioned that victims would receive an "identity theft report" that listed each account fraudulently opened or used by an impostor and that could be sent to credit reporting companies and creditors to support a victim making disputes. In reality, few police departments provide a comprehensive identity theft report to victims. More often, the victim gets a page that simply verifies that the victim reported the identity theft to police. In that case, the victim can attach a copy of his or her signed FTC complaint (identity theft affidavit) to the police report, and this will suffice as an identity theft report.

In addition to local law enforcement, victims can report identity crimes to a variety of federal and state agencies depending on the circumstances including the United States Postal Inspection Service, state attorneys general, the Secret Service, or the Internet Crimes Complaint Center.

Removing Impostor Accounts From a Victim's Credit History

To remove impostor accounts from a victim's credit history, the victim must follow the process prescribed by Congress in the FACTA amendments to the FCRA (FCRA section 609e or FCRA 605b). The victim must write letters to the credit reporting companies and to businesses that gave credit to the impostor. All letters written by the victim should be sent by certified mail, return receipt requested or in a manner that allows the victim to track the letters. Letters should include a copy of the identity theft report or police report and identity theft affidavit as well as a copy of the victim's current government issued identity card or driver's license.

In a victim's letters to credit reporting companies, the victim should dispute all accounts, inquiries, and other information in the credit report that does not belong to the victim. Additionally, the victim should request that fraudulent accounts be blocked from the credit report and that the first five digits of the victim's social security number be blocked. Sample letters are available from several Web sites including www.ftc.gov/idtheft, www.idtheftcenter.org, and www.idvictim.org.

Upon receipt of this type of correspondence, the credit reporting companies must block the first five digits of the victim's social security number from the victim's credit report. The companies must also notify businesses that furnished information regarding disputed accounts to request an investigation and account verification. The credit reporting companies must block disputed information from the victim's credit report within 4 days of receiving the dispute letter subject to verification of the information.

At the same time, the victim should also write businesses that gave credit to impostors using the victim's personal identifying information. The letters should be sent in a manner that allows the victim to track receipt such as certified mail, return receipt requested. The victim should enclose a copy of his or her government issued identification card or driver's license and a copy of the identity theft report or police report and identity theft affidavit. The letter should dispute the validity of any accounts given to an impostor based on identity theft and should ask the recipient to provide a copy of all documents related to the fraudulent account. The documents must be sent to the victim within 30 days. The victim should receive written confirmation that accounts have been closed and that items have been removed from the credit report.

Recovering From Other Types of Identity Theft

Medical identity theft, employment identity theft, and criminal identity theft are not covered under the Fair Credit Reporting Act. Identity theft advocates have developed strategies for assisting these victims.

Responding to Medical Identity Theft

Medical identity theft presents special challenges because the victim must be careful not to invoke the impostor's rights under the Health Insurance Portability and Accountability Act, a federal law that protects the privacy rights of persons who receive medical care.

Clearing a medical record must be done in several stages. The victim should report the medical identity theft to his or her local law enforcement and obtain a copy of the police report. The victim should also request a copy of his or her medical record from the victim's primary health care provider. This medical record is used as a baseline that accurately reflects the victim's current state of health and any past medical problems. At the same time, the victim should alert his or her primary care doctor to the identity theft and ask for assistance in clearing impostor information from the medical record. The victim's doctor can write a letter stating that the patient is a victim of medical identity theft, listing any medical conditions of the victim that might conflict with the impostor's information such as blood type or a chronic condition like diabetes, and asking that the medical records be corrected.

Victims who do not regularly see a doctor or other health care provider need not be alarmed. The following steps can be taken to clear an impostor's information from a victim's medical record. Write the health care providers that gave care to the impostor. Request a copy of two things: their privacy policy and a copy of the victim's medical records. Medical providers are allowed to charge a reasonable fee for copying the records. If the cost is too high, the victim may view the records in person at the office where the records are kept.

The victim should review the records and mark everything that is not accurate. When viewing the records in person, the victim may request a copy of only the pages that contain errors. The victim should also read the privacy policy of each health care provider where the impostor received care. The privacy policy should outline the steps to take to correct information in a medical record. Follow the instructions in the privacy policy.

If a provider's privacy policy does not address how to correct a medical record, the victim should request that the incorrect information be deleted from the medical record. The request should be made in writing, and the victim should attach a copy of the police report, the victim's driver's license or other government issued ID, and his or her genuine medical record or letter from the victim's doctor. The victim should obtain a copy of the corrected medical record and request that a copy of the corrected records be forwarded to any party with whom the impostor's medical providers shared the impostor's medical record.

Some health care providers are reluctant to delete items from medical records. In that case, the victim should demand that the record be amended and that a "red flag" be placed in the record to alert future health care providers to the amendment. If the health care provider denies a victim's request to amend a file, the victim should put a statement of disagreement in the medical record. This is accomplished by writing a short letter to the health care provider pointing out all of the inaccuracies contained in the record. The health care provider must include the victim's statement of disagreement in their medical file. When an impostor uses a victim's insurance to get medical treatment, the insurance carrier should be notified in writing and asked and to restore the victim's benefit limit.

When a Victim's Social Security Number is Being Used by Someone for Employment

Victims usually discover that an impostor is using their social security number to get or keep a job when they receive notification from the Internal Revenue Service that their income has been underreported. To remedy this type of identity theft, the victim must get a copy of his or her social security earnings record. Consumers can order a copy online at www.ssa.gov or by mail; however, a fee will be charged for this service. The statement will be mailed and may take several weeks to arrive.

For immediate assistance, the victim should visit his or her local Social Security office. There the victim can review the earnings record with a Social Security representative. The representative will issue a corrected earnings report. The victim should report the matter to local law enforcement and get a copy of the report. Then, the victim must send a copy of the corrected earnings statement, police report, and the victim's government issued identity card to the Internal Revenue Service at the address listed in the correspondence received by the victim. The IRS now has an Identity Protection Specialized Unit to assist victims of identity theft with tax related problems. The Unit can be reached toll free at 1-800-908-4490. Victims can also ask to have their social security numbers flagged so that they do not have to respond to the same issue every year.

Recovering From Criminal Identity Theft

Criminal identity theft is perhaps the scariest and most difficult type of identity theft to recover from because there is no federal law that directly addresses it. Victims must use their state laws to clear impostor convictions from their records. A few states have Identity Theft Passport programs that can be useful to victims of criminal identity theft. An identity theft passport is a wallet-sized card issued by a state attorney general that identifies the holder as a victim of identity theft. The following states have passport programs: Maryland, Ohio, Virginia, New Mexico, Oklahoma, Arkansas, Delaware, Iowa, Mississippi, Nevada, and Montana. If a criminal identity theft victim lives in a passport state, he or she should contact the state attorney general for instructions on getting an identity theft passport.

Some states such as Texas and California have specific procedures that victims must follow to obtain a stolen identity file or request that criminal records be expunged due to identity theft. If a state has no procedure or passport program, the victim must attempt to get a letter of clearance from the jurisdiction where the impostor was charged with a crime. Frequently, this is in a state other than where the victim lives. To get a letter of clearance, the victim should submit a photograph, fingerprints, and any documentation showing the victim's innocence to the jurisdiction where the impostor was charged with a crime. Local law enforcement agencies where the victim resides can assist the victim in obtaining a letter of clearance. This letter must be submitted to the state agencies responsible for keeping criminal records in the state where the crimes occurred with a request that the records be corrected. The letter would be a "factual declaration of innocence" that they need. Victims need to clear inaccurate criminal records at the local, state, and national level for complete coverage.

Many victims of criminal identity theft find out about the crime when they are denied employment based on a criminal background check. In such cases, the employer must give the job applicant a copy of the criminal background check upon request. The victim can write the background check company and request a record correction. Unfortunately, there are literally thousands of small companies that perform criminal background checks for employers. It would be virtually impossible for a victim to correct his or her record with every company. Consequently, victims of criminal identity theft who are applying for jobs must alert potential employers to their identity theft and provide a copy of their letter of clearance or identity theft passport before the criminal background check is performed so that employers will know the results are likely to be inaccurate. It may be helpful to obtain a detailed work history using the Social Security Administration Form SSA 7050 (available at www.ssa.gov/online/ssa-7050.html), which lists the employers and location of employment so that the person can determine which are true and which ones belong to others.

Preventing Revictimization

Identity theft is a crime that keeps on giving. Victims must be vigilant to minimize their chances of being revictimized. Victims should scrutinize their bank and credit card statements every month and monitor their credit reports to spot and dispute unauthorized activity as soon as possible. The Fair Credit Reporting Act gives consumers the right to get a free credit report every year from each of the three major credit reporting agencies (visit annualcreditreport.com). Many victim advocates suggest consumers stagger their requests by ordering a free report from one of the three major credit reporting agencies every 4 months.

Making a few changes in habit can reduce a victim's chances of becoming victimized again. The same strategies can be used by any individual to reduce the possibility of becoming an identity theft victim. Shredding documents with account or identity information before throwing them away or recycling them prevents thieves from obtaining personal information through trash diving. Bills, account statements, bank statements, federal and state tax returns, and credit card offers should be shredded. Thwarting mail theft is also an important prevention tool. Ways to minimize mail theft include using a locking mailbox, and stopping mail delivery during vacations. Leaving credit cards, social security cards, and Medicare cards at home unless one needs them will minimize the chance of losing personal information if a person is mugged or if items are stolen from a purse, wallet, or car.

Most states have passed credit freeze laws; those without the laws are being offered credit freeze by the credit bureaus. A credit freeze, sometimes called a security freeze, helps reduce instances of new account fraud because most creditors will not issue an account without being able to view a person's credit report. A credit freeze makes a person's credit report unavailable for viewing unless the consumer takes steps to unfreeze it. It takes about 3 business days to thaw a frozen credit report (depending on state law requirements, it could take from 15 minutes to 3 business days). When a potential creditor makes a request to see a credit report that is subject to a freeze, the reporting agency notifies the potential creditor that the report cannot be viewed unless steps are taken to release the credit report. Victims of identity theft generally incur no charge for placing a freeze. Other consumers may be charged a nominal fee. A credit freeze must be requested in writing from each of the credit reporting agencies. This is different from placing a fraud alert, which can be done by calling only one of the credit reporting agencies. Depending on state law, some states require Internet or phone placement as an option. Check with the state attorney general's office on specifics on state credit freeze law.

Another prevention measure is to opt out of pre-approved credit offers. Thieves who steal pre-approved credit offers are able to obtain credit using a victim's identity, and by changing the address to which statements are sent, thieves decrease the victim's ability to discover the crime. Individuals can opt out of pre-approved credit offers by visiting www.optoutprescreen.com and following the online instructions or by calling 1–888–5–OPT-OUT (1–888–567–8688).

To reduce marketing telephone calls, consumers can visit www.donotcall.gov. Both home and cell phone numbers can be registered. After telephone numbers have been placed in the registry for 31 days, most telemarketers should not call a consumer. Charities, political organizations, and businesses with whom a consumer currently does business are exempt and are allowed to call unless specifically requested otherwise.

Safe Internet surfing is another skill that can protect consumers from identity theft. Consumers should have updated anti-virus, spyware, and firewall personal computer security and protect e-mail and online accounts with passwords that cannot easily be guessed. Names, birthdates, anniversaries, or telephone numbers should not be used as passwords. Additionally, consumers should avoid keeping a list of passwords on or near their computers. Consumers should not open or respond to e-mails unless they know and trust the sender, and individuals should never respond to e-mails asking for passwords or personal information. A good way to avoid phishing scams is to ask, "Who initiated this conversation?" If a consumer contacts a credit card company, the company needs to verify the consumer's identity. However, if someone contacts the consumer claiming to be from a credit card company, then the caller should not have to ask for personal information such as an account number, security code, or routing number. Additionally, government agencies such as the Internal Revenue Service will never contact a consumer by e-mail unless the consumer has initiated contact first.

Resources for Victims

The following table lists a few of the resources available to victims of identity theft.

Name	Contact Information	What They Do
OVC-TTAC Online Identity Theft Training	www.ovcttac.gov/views/TrainingMaterials/dspOnline_IdentityTheft.cfm	Online training for victim service providers.
Identity Theft Resource Center	www.idtheftcenter.org	Provides victim support, prevention information, and consumer education about identity theft.
Federal Trade Commission	www.ftc.gov/idtheft Phone: 877–438–4338 600 Pennsylvania Ave. NW Washington, DC 20580	Takes complaints for inclusion in nationwide database for law enforcement; complaint form can be used by victims as an affidavit; and enforces the Fair Credit Reporting Act. Provides self-help information for identity theft victims.
U.S. Postal Inspector	http://postalinspectors.uspis.gov phone: 877–876–2455 U.S. Postal Inspector ATTN: MAIL FRAUD 222 S. Riverside Plaza, # 1250 Chicago, IL 60606-6100	Investigates identity thefts involving the mail.
Federal Bureau of Investigation	www.ic3.gov Phone: 202–324–3000	Investigates identity thefts involving computers or the Internet.
Secret Service	www.secretservice.gov Phone: 202–406–5708	Investigates identity theft involving large sums of money or multiple victims.
Internal Revenue Service	www.irs.gov Phone: 1–800–908–4490	Identity Protection Specialized Unit assists taxpayers with unresolved identity theft issues regarding taxes.
Opt Out of Credit Offers	www.optoutprescreen.com Phone: 1–888–5–OPT-OUT (1–888–567–8688)	Free service to opt out of pre-approved credit card offers.
Federal No Call List	www.donotcall.gov	Limits most telemarketing calls.

Contact information for the three major credit reporting companies follows.

Reporting Company	Fraud Alerts and Credit Reports	Credit Freezes
Equifax	800–525–6285 P.O. Box 740241 Atlanta, GA 30374 www.Equifax.com	P.O. Box 105788 Atlanta, GA 30348
Experian	888–397–3742 P.O. Box 9532 Allen, TX 75013 www.Experian.com	P.O. Box 9554 Allen, TX 75013
Transunion	800–680–7289 P.O. Box 6790 Fullerton, CA 92834 www.transunion.com	P.O. Box 6790 Fullerton, CA 92834-6790

Endnotes

[1] Federal Trade Commission, 2012, *Consumer Sentinel Data Book for January – December 2011*. Retrieved June 19, 2012, from www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf.

[2] Ibid.

[3] Federal Trade Commission, *Consumer Sentinel Data Book for January – December 2008.* Retrieved June 19, 2012, from www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf, 5. In 2000, 31,140 consumers made identity theft complaints to the FTC. In 2008, the number of consumers reporting identity theft increased to 313,982.

[4] KCDB.com, December 2007, "Lubbock Couple Behind Nationwide Identity Theft and Credit Card Scam." Retrieved June 19, 2012, from www.kcbd.com/Global/story.asp?S=7483542&nav=menu69_3_9.

[5] Office of Public Affairs, 2012, "Federal Courts Order Seizure of 36 Website Domains Involved in Selling Stolen Credit Card Numbers," Washington, DC: U.S. Department of Justice. Retrieved June 19, 2012, from www.justice.gov/opa/pr/2012/April/12-crm-544.html .

[6] Office for Victims of Crime, 2012, "Crime Victimization in the United States: Statistical Overviews," Washington, DC: U.S. Department of Justice. Retrieved June 19, 2012, from http://ovc.ncjrs.gov/ncvrw2012/pdf/StatisticalOverviews.pdf; see note 1 above, Federal Trade Commission, 2012.

[7] Javelin Strategy and Research, 2011, "2011 Identity Fraud Survey Report: Consumer Version," Pleasanton, CA: Author. Retrieved June 19, 2012, from www.identityguard.com/downloads/javelin-2011-identity-fraud survey-report.pdf, 5.

[8] Ibid., 10.

[9] *Consumer Sentinel Network Data Book for January-December 2011*, Federal Trade Commission, February 2012, p. 3; http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf.

[10] See note 6 above, Office for Victims of Crime, 2012; see note 1 above, Federal Trade Commission, 2012, 3.

[11] See note 1 above, Federal Trade Commission, 2012, 9.

[12] See note 1 above, Federal Trade Commission, 2012, 10.

[13] See note 1 above, Federal Trade Commission, 2012, 14.

[14] See note 1 above, Federal Trade Commission, 2012, 15.

[15] See note 7 above, Javelin Strategy and Research, 2011, 5.

[16] See note 1 above, Federal Trade Commission, 2012, 3.

[17] See note 1 above, Federal Trade Commission, 2012, 12.

[18] Identity Theft Resource Center, 2009, *Identity Theft: The Aftermath 2008*. Retrieved June 19, 2012, from www.idtheftcenter.org/artman2/uploads/1/Aftermath_2008_20090520.pdf.

[19] Ibid.

[20] 18 U.S.C. § 3771.

[21] See *United States v. Kiefer*, 2008 U.S. Dist. Lexis 16384, S. Dist. Ohio (extended federal crime victim rights to victims of identity theft). For a list of state victims' rights laws, see National Crime Victim Law Institute, www.ncvli.org.