

INTRODUCTION

This curriculum is presented in a total of five modules:

1. Identity Theft 101 – provides a basic primer on identity theft in two lessons, Understanding Identity Theft and Assisting Victims.
2. The Emotional Impact of Identity Theft – introduces common reactions to identity theft in two lessons, Common Reactions to Identity Theft and Variations in Victim Reactions.
3. Strengthening Resilience in Identity Theft Victims – introduces five traits of resilience along with strategies advocates can use to help identity theft victims build resilience.
4. Screening and Referring Identity Theft Victims to Professional Therapy – describes the symptoms of depression, anxiety, and post-traumatic stress disorder distinguishing these symptoms from natural trauma reaction and provides suggestions for making professional referrals.
5. Assisting Identity Theft Victims in Emotional Recovery – provides information for mental health professionals who work with identity theft victims.

The instructor may use one or more of the modules depending on audience needs. An audience comprised of law enforcement officers and victim advocates would use Modules 1-4. An audience comprised of mental health professionals would use Modules 1-5. An audience of victim advocates who are highly skilled at assisting victims in their financial recovery may choose to omit Module 1 and use only Modules 2-4.

You will need an LCD projector, a laptop with the slides pre-loaded, a flipchart with blank paper or a whiteboard and markers, 3 x 5 index cards, and copies of the handouts.

Module 1: Identity theft 101

Time Required

1 hour

Purpose

The purpose of this module is to provide a basic primer on identity theft including what identity theft is, how thieves steal and use information, and how to assist victims in recovering.

Lessons

- Understanding Identity Theft (15 min.)
- Assisting Victims (45 min.)

Learning Objectives

By the end of this module, participants will be able to:

- Define the crime of identity theft
- Describe ways personal information may be acquired and used by identity thieves
- Describe steps for victims to take to recover their identity and repair their credit using the Action Plan
- Identify resources available to victims

Participant Handouts

Copies of PowerPoint slides

Identity Theft 101 handout

Action Plan for Victims of ID theft

Equipment and Materials

LCD projector and laptop with powerpoint presentation loaded

Preparation for the Instructor

Thoroughly review the curriculum. Time allotted is approximately 2 minutes per slide, excluding title slides and resource slides.

Review the Action Plan for Victims of Identity Theft

☞ As participants enter, show *Slide 1.1* (Title slide)

Introduction:

☞ *Slide 1.2*

Review the learning objectives for Module 1.

☞ *Slide 1.3*

Disclaimer: Note that the curriculum was developed with funding from the US Department of Justice, Office for Victims of Crime through a subgrant from Maryland Crime Victims Resource Center and that the contents reflect the points of view of the authors only and do not necessarily reflect the opinions of the Department of Justice or MCVRC.

☞ *Slide 1.4*

Activity – True or False

The slide shows 5 possible identity theft facts. By show of hands, which are true and which are false?

Answer Key:

- Data breach is a form of ID theft. **False. Data breach is a separate crime. Every data breach does not result in identity theft; although, every data breach puts consumers at a high risk of identity theft.**
- Brownsville, Texas is a national ID theft hotspot. **True. Brownsville is consistently in the top 10 cities in the U.S. for identity theft complaints according to the Federal Trade Commission's Consumer Sentinel database.**
- An estimated 5 million Americans were victimized by identity thieves in 2009. **True.**
- A felon can exit prison with a clean criminal history. **True. This has happened. The thief assumes a false identity upon arrest and keeps that identity throughout the criminal justice process. Then, he exits prison with his own identity clean leaving a victim with a felony record.**
- More ID theft happens by computer hacking than through old fashioned stealing or dumpster diving. **False. This is a common misconception. While millions of consumer records are compromised every year by hackers, most identity theft happens closer to home and is committed either by someone known to the victim or by local identity theft rings who steal information from trash, dumpsters, or unlocked mailboxes.**

Note: If you are using this curriculum outside Texas, you might replace the first slide bullet point to reflect the metropolitan area in your state where consumers report the highest rates of identity theft.

Lesson 1: What is Identity Theft?

☞ Slide 1.5

Paraphrase the following:

Identity theft is the theft or misuse of personal identifying information for personal gain or to facilitate criminal activity.¹ Identity Theft happens when a criminal, called an imposter or an identity thief, takes or misuses the personal identifying information of another for personal gain, to facilitate other criminal activity, or to evade law enforcement.

☞ Slide 1.6

Paraphrase the following:

Each state has a unique definition of identity theft that defines the crime for state level law enforcement and courts.

Under Texas law, identity theft is “to obtain, possess, transfer, or use a person’s ‘identifying information’ or ‘telecommunication access device’ with the intent to harm the person.”² Using either definition, identity theft has three elements: (1) to obtain, possess, transfer or use (2) personal identifying information (3) without permission.

Note: If using this outside Texas, replace Slide 6 with the definition of identity theft from your state’s penal code.

What information is stolen?

☞ Slide 1.7

Personal identifying information is the information that is valued by identity thieves. It is any information that is unique to an individual. This includes:

- One’s name
- Current or former addresses
- Telephone numbers
- Social Security number
- Driver’s license number
- Any government issued identification number
- Account numbers, date of birth, PINs, passwords, user names, access codes, and answers to security questions such as mother’s maiden name.

Under the Texas Penal Code, personal identifying information also includes “telecommunication access devices” such as ATM cards.

The most valuable information is “breeder documents”. That is a Social Security card, birth certificate, or passport. These documents can be used to clone a person’s identity.

¹ Fair Credit Reporting Act, 15 U.S.C § 1681a

² Texas Penal Code §

How do thieves acquire victims' personal identifying information?

☞ *Slide 1.8*

Paraphrase the following:

Thieves have developed myriad means of stealing personal identifying information. The most common method remains plain old stealing. This is low tech and may be as simple dumpster diving, stealing mail from unlocked mailboxes, or rooting through a person's unattended wallet or purse or as bold as mugging, burglary, or breaking into a victim's vehicle.

Thieves also have developed sophisticated, high tech, ways to steal information such as:
Skimming – using a device that reads the strip on the back of a credit card

Computer hacking, and

War driving - also called access point mapping, is the act of hacking into unsecured wireless local area networks – usually home wireless networks or free public wireless networks – while driving.

Thieves also commit fraud in order to obtain personal identifying information. For example, a thief may send a phishing email to potential victims promising the victims money if the victims provide their bank account and routing numbers.

How to keep up with current scams

There is a thriving black market for personal identifying information where thieves buy, sell, and trade the information they have stolen. There are several resources available to keep abreast of trends in consumer scams.

The Office of the Texas Attorney General- maintains a web page describing frauds and scams affecting Texas consumers.³

Snopes is another useful website that collects information on current scams.⁴

The Internet Crime Complaint Center maintains a web page on current computer related threats and scams.⁵

There are also a number of useful websites that provide consumer information on cybersafety such as the Federal Trade Commission's On Guard Online website.⁶
URL's for these resources are included on Slide 1.38.

What do thieves do with the information they steal?

☞ *Slide 1.9*

³ <https://www.oag.state.tx.us/consumer/scams.shtml>

⁴ <http://www.snopes.com/fraud/topscams.asp>

⁵ <http://www.ic3.gov/crimeschemes.aspx>

⁶ See, e.g., <http://onguardonline.gov/>; <http://www.cyber-safety.com/>.

Paraphrase the following:

Identity theft can take many forms. It can be as simple as unauthorized charges made to a consumer's credit card or as complex as setting up entire business enterprises using stolen identifiers.

Typically, identity theft falls into three categories:

Existing account fraud- when a thief acquires personal identifying information to gain access to a consumer's existing financial accounts. This includes existing credit cards, bank accounts, brokerage accounts, utilities, mortgages or other loans.

New account fraud- a thief opens new accounts using stolen personal identifying information. Synthetic identity theft is a type of new account fraud in which a thief combines the personal identifying information of several victims to open new accounts.

(Both existing account fraud and new account fraud are types of financial identity theft.)

Non-financial identity theft- takes many forms including criminal identity theft, theft of public benefits, employment identity theft, and medical identity theft. Identity theft has proven to be a low risk way for criminals to launder money or evade law enforcement.

Types of non- financial ID theft

Criminal- occurs when a person who has been stopped by law enforcement falsely supplies another person's information in place of their own.

Governmental- someone used the identity data of another person and supplies such data when interacting with a government agency or database usually to get benefits.

Medical- one person uses another person's information in order to obtain medical services or falsify insurance billing.

Identity Theft and Other Crimes

☞ *Slide 1.10*

Paraphrase the following:

Be aware that identity theft is linked with other crimes. So, when we are working, for example, with a victim of family violence, we should be alert to signs that the victim is also experiencing identity theft. It is a valuable opportunity to assist consumers in protecting themselves as well as assisting them to discover and deal with potential identity theft problems early.

Victim Experiences

☞ *Slide 1.11*

Paraphrase the following:

Identity theft is traumatic. It is a highly personal crime to the victim, yet it is a crime that many thieves view as victimless. Identity theft victims have the credit history that they worked hard to build compromised. Victims can be denied credit, harassed by bill collectors, and sued over debts they did not incur. They may lose or be denied public benefits, be denied medical care, lose or be denied employment, or be unable to renew their driver's license because of identity theft. Identity theft victims have been accused of and arrested for crimes committed by others. Because information brokers are largely unregulated, once an identity thief's arrest, conviction, or warrant appears on a victim's background check, the false information is virtually impossible to remove. Adding to victims' frustration, the debt buying industry has made it impossible for victims to have impostor activity permanently removed from their credit reports.

Short Break if desired. This point in the presentation is an ideal time to take a short break.

☞ *Slide 1.12*

Lesson 2: Assisting Victims with Recovery

Introducing the Victim's Toolkit

☞ *Slide 1.13*

Attached is a victim's toolkit developed by the Victims Initiative for Counseling, Advocacy, and Restoration of the Southwest that walks victims of financial identity theft step-by-step through the recovery process.

Note: Anyone can use the Victim's Toolkit developed by VICARS. However, if you are outside Texas, you might choose to replace Slide 13 with a reference to a different resource such as the Federal Trade Commission's Pro Bono Guide, www.idtheft.gov/probono.

☞ *Slide 1.14*

Paraphrase the following:

There are 3 pressing concerns identity theft victims face:

- Stopping the use of their information to halt further damage
- Reporting the crime because this is a prerequisite to recovery, and
- Repairing the damage that has been done.

Preparing the victim for the ordeal of recovery

☞ *Slide 1.15*

Paraphrase the following:

Pages 1-4 of the toolkit help victims prepare for the ordeal of recovery. Common victim reactions to the recovery process are that they are made to feel like a criminal, that they are frustrated by having to tell the same story repeatedly, and that they have to bear the time and hassle of recovery. Frustration is lessened

when victims know what to expect, and victims are more successful when they have written down the most important facts relevant to their situation so that they can tell their story succinctly and consistently. Encourage victims to use the boxes at the bottom of the pages of the toolkit to note their time and expenses. If their thief is caught, this information can form the basis for a request for restitution.

Note: If you are not using the Action Plan, delete the first bullet point from the slide.

Stopping Impostor Activity aka Stopping the Bleeding

☞ *Slide 1.16*

Paraphrase the following:

The steps a victim should take to prevent identity thieves from continuing to use their accounts are:

- Call businesses that sold goods or services to the identity thief and report the fraud;
- Ask businesses to close or renumber existing accounts that have been used without the victim's authorization;
- If a bank account in Texas is compromised, ask the bank to put the account in the Closed Account Notification System (CANS); CANS is a database maintained under state law that reports compromised bank account numbers to check verification companies. To get into the system, the victim executes an affidavit at their bank, and the bank submits the affidavit to the CANS.
- Call credit card companies, report the fraud, ask that for a new account number and a new card;
- Place a fraud alert.

Fraud Alerts

☞ *Slide 1.17*

Paraphrase the following:

The federal Fair Credit Reporting Act allows consumers to place fraud alerts on their credit reports. A fraud alert is a notation on the credit report that tells companies that the consumer may be a victim of identity fraud. When notified, the company viewing the report must take reasonable steps to verify the identity of the person requesting credit. This usually means making a telephone call to the consumer. To get a fraud alert the consumer places a telephone call to ONE of the credit reporting agencies. Some advocates encourage victims to go ahead and call all three; however, the CRAs are legally bound to notify each other when a fraud alert is placed. Warn victims that these are automated telephone systems, the victim will not talk to a live human being. Consumers should listen carefully to the automated phone options so that they are not diverted to an option where they must purchase a credit report or credit monitoring. The consumer should be given the option to receive a free credit report when placing the fraud alert. Initial alert is for 90 days and is renewable every 90 days. This can be extended to 7 years if the consumer provides a copy of their police report to the CRA.

Fraud Alerts vs. Credit Freezes

☞ *Slide 1.18*

Paraphrase the following:

Fraud alerts warn creditors to take reasonable steps to verify the identity of the person requesting credit, but they do not prevent creditors from issuing credit. Credit freezes are more effective at preventing new account fraud because they prevent creditors from issuing credit at all – even to the consumer. To get a credit freeze: consumer must write each CRA, and pay a fee unless the consumer produces a police report. To unfreeze, the consumer calls a toll free number and provides a PIN. Neither a credit freeze nor a fraud alert will protect consumers from creditors that do not perform credit checks.

Note: If you are outside Texas confirm whether your state allows CRAs to charge a fee for credit freezes.

Helpful intake questions

☞ Slide 1.19

Read the 5 questions on the slide. These questions help victims organize their thoughts when talking about their identity theft.

How to get a free credit report

☞ Slide 1.20

Paraphrase the following

Identity theft victims need to get in the habit of checking their credit regularly. This slide gives the information for getting free credit reports. The website www.annualcreditreport.com allows consumers to get a free credit report by diverting the consumer to the credit reporting agencies. The pirate is there to remind us that www.freecreditreport.com is not free. It is a website that requires the consumer to sign up for credit monitoring in order to get a credit report. The fourth item on the slide, Innovis, is a company that provides credit reports but that is not considered a credit reporting agency under the Fair Credit Reporting Act. Some victims have been denied credit based on reports by Innovis, so it is a good idea to have their contact information handy.

Reporting the crime

☞ Slide 1.21

Paraphrase the following

The slide shows the agencies that consumers most commonly report to. Every victim of ID theft should make an online report to the Federal Trade Commission, print it, and sign it in front of witnesses or a notary public. Victims should report the crime to their local law enforcement. In the past, victims were told to report in the jurisdiction where their identity was being used. This is no longer the case. The federal law enforcement agency charged with investigating identity theft is the Secret Service, protector of the nation's money supply. The FBI investigates identity theft if it involves large numbers of victims, large sums of money, or other crimes such as drug or human trafficking. IC3 is a consortium of federal agencies that investigate computer related crimes.

The Identity Theft Report

☞ *Slide 1.22*

Paraphrase the following

Identity theft reports are a creature of the Fair Credit Reporting Act designed to help consumers recover from identity theft by providing businesses and credit reporting agencies a means of verifying that the crime happened. The identity theft report is issued by a local law enforcement agency and includes details about the existing accounts used by the identity thief and new accounts opened by the thief. As a practical matter, many jurisdictions do not create identity theft reports that are comprehensive. An alternative is for the consumer to make a report to the Federal Trade Commission, print it, sign it in front of witnesses or a notary public, and attach a copy to the victim's police report.

Clearing Accounts

☞ *Slide 1.23*

Paraphrase the following:

The Fair Credit Reporting Act outlines a procedure to be used to clear impostor information from consumer accounts. Victims' biggest mistake in using this procedure is failing to follow-up their communications in writing. Clearing accounts is a two-step process involving both the credit reporting agencies and businesses that issued credit to identity thieves.

Contacting Credit Reporting Agencies

☞ *Slide 1.24*

Paraphrase the following:

The Fair Credit Reporting Act gives consumers the right to block fraudulent information from their credit report and to have the credit reporting agencies notify creditors that the consumer has reported fraud. The communication must be in writing with attachments: copy of identity theft report or police report and ID theft affidavit, and copy of victim's government issued identification card.

Writing businesses that gave credit to identity thieves

☞ *Slide 1.25*

Paraphrase the following:

The Fair Credit Reporting Act gives consumers the right to get a copy of records from fraudulent accounts and prevents creditors from placing disputed accounts with debt collectors. The request must be

in writing and attached must be a copy of the consumer's government issued identification card, an identity theft report, or a copy of the police report and identity theft affidavit.

Tips for helping victims

☞ *Slide 1.26*

Paraphrase the following:

Everything must be in writing. Send everything in a manner that provides proof of receipt. Be tenacious. Some victims must repeat the process many times. Report businesses that violate the law to the Federal Trade Commission.

Non-Financial ID Theft

☞ *Slide 1.27*

Medical ID Theft

☞ *Slide 1.28*

Paraphrase the following:

Victims most often find out when they are denied medical care or when their insurance refuses to pay for a procedure. It is dangerous because of the health implication of commingling medical records. Victims must:

- Report to local law enforcement, and get a copy of the report
- The victim should get medical records from his or her own doctor
- Request the victim's medical records from providers that gave care to the identity thief.
Important: Do not mention identity theft at this point. If you do, you will trigger the HIPAA rights of the thief. Plus, at this point you really cannot tell whether identity theft has happened or not. Some people think they are victims only to discover that the name they did not recognize is legitimately the billing company for a provider that gave them service.
- Write providers who gave care to the identity thief requesting correction or segregation and flagging of records. Attach: police report, victim's ID, relevant portions of genuine records.
- Confirm in writing that records have been corrected and review corrections.

Use of victim's SSN for employment

☞ *Slide 1.29*

Paraphrase the following:

- Get a copy of victim's earnings record from SSA
- Mark items that are not the victim's, provide supporting documentation, request corrected statement
- Provide corrected earnings statement and supporting documents to IRS
- Request that victim's SSN be flagged
- IRS Identity Protection Specialized Unit:

1-800-908-4490

Criminal ID Theft

☞ Slide 1.30

NOTE: If you are using this curriculum outside Texas, replace this slide with a slide that describes the law in your state.

To clear a crime from a victim's criminal record, the victim must get a stolen identity file:

- Local sheriff takes photo and fingerprints
- Verifies that victim is not the criminal
- Submits to DPS
- Victim receives confirmation letter and password
- If crime is in another state, contact law enforcement there, provide proof of victim's identity and alibi information, request letter of clearance
- Provide letter of clearance to relevant businesses, agencies, and data brokers. Ask that the stolen identity file be provided to the NCIC.

As a practical matter, crimes will still appear on the victim's background checks because companies will search records and see that while the victim has a clean record, his or her name is an alias of the identity thief. Background check companies will provide both records to requestors which will make it appear that the victim has a criminal record.

Application to be declared a victim of identity theft

☞ Slide 1.31

NOTE: If you are using this curriculum outside Texas, delete this slide.

Paraphrase the following:

The Texas Business and Commerce Code contains a procedure for victims to obtain a court order verifying that they are a victim. This is useful when thieves have created public records bearing a victim's information. See Texas Business and Commerce Code, sections 521.101 through 521.105. The Texas Attorney General has written self-help forms for victims to use to file this type of case without using an attorney. The forms are available on the website www.oag.state.tx.us.

Assisting victims through the criminal justice system

☞ *Slide 1.32*

Paraphrase the following:

Fewer than 1% of identity thieves are arrested. Only Pennsylvania currently allows identity theft victims to receive crime victims' compensation to get counseling; although, the Victims of Crime Act does not prohibit it. Some locales do not apply their Crime Victims Bill of Rights to identity theft victims because their laws define victims as being victims of violent crime. However, this should not prevent the victim from filling out and submitting a victim impact statement, requesting restitution, or asking for allocution if it is allowed to other victims in the jurisdiction.

The importance of follow-up

☞ *Slide 1.33*

Paraphrase the following:

It is easy for victims to become overwhelmed during the recovery process. Providing follow-up helps victims stay on track and gives the advocate an opportunity to look for signs that the victim needs referrals or extra help that sometimes may not be apparent in the first few contacts.

Minimizing Re-Victimization

☞ *Slide 1.34*

Paraphrase the following

Changing a few habits can minimize a victim's chance of re-victimization:

- Shred!
- Watch the mailbox;
- Surf safely;
- Don't carry it if you don't need it;
- Never give out personal information if you did not initiate the transaction.

Monitoring Credit

☞ *Slide 1.35*

Paraphrase the following

This slide shows an easy way for victims to continuously monitor their credit without paying fees. Victims will sometimes ask whether they should purchase credit monitoring. Caution victims that if they choose to do so, they should check the company carefully. Financially, the decision is similar to other consumer decisions, e.g., whether to change the oil in your car yourself. If you have the disposable income available and do not want to take the time or effort to do it yourself, then it might make sense to pay for the service; however, victims should realize that they would be paying for a service that they could provide for themselves.

Resources for victims and advocates and contact information for the author

☞ *Slides 1.36-1.39*

If time allows, the last few minutes of Module 1 can be used for questions.

Review the learning objectives and ask participants if they feel the learning objectives were met. By the end of this module, participants should be able to:

- Define the crime of identity theft
- Describe ways personal information may be acquired and used by identity thieves
- Describe steps for victims to take to recover their identity and repair their credit using the Action Plan
- Identify resources available to victims