ID theft and account fraud

Seminar lesson plan and class activities

Consumer Action Managing Money Project

ID Theft and Account Fraud: Prevention and cleanup

Seminar lesson plan and class activities

Lesson purpose:

To make participants aware of the risk of identity theft and account fraud, teach them how to safeguard their information, enable them to recognize the signs of ID theft and fraud, and provide them with the knowledge and tools to recover if they were to become victims.

Lesson objectives:

By the end of the lesson, participants will understand:

- The potential damage caused by ID theft and account fraud
- How ID theft and account fraud happen
- How to protect their personal data and avoid becoming a victim
- How to recognize when fraud has occurred
- What their rights are regarding responsibility for fraudulent debts and other fraudulent activity
- What steps to take if they are, or believe they may become, a victim of identity theft
- What resources are available to help consumers and victims

Lesson duration:

2½ hours (including a 10-minute break; not including 15-minute optional interactive quiz)

Materials:

For instructor:

- *ID Theft & Account Fraud: Prevention and cleanup* brochure
- *ID Theft and Account Fraud Backgrounder*
- Lesson plan (pages 3-31)
- Activities and worksheets (including answer keys) (pages 32-43)
    - ID Theft Prevention Checklist (page 32)
    - Test Your Knowledge About ID Theft and Account Fraud quiz and answer key (pages 33-41)
    - Savvy Consumer quiz and answer key (pages 42-43)
- Sample letters (pages 44-46)
- Training evaluation form (page 47)
- Visual teaching aid (PowerPoint presentation with instructor's notes)

Instructor will also need:

- A computer and projector for the PowerPoint presentation
- An easel and pad or a whiteboard and markers

For participants:

- *ID Theft & Account Fraud: Prevention and cleanup* brochure
- Worksheets and activities:
    - ID Theft Prevention Checklist (1 page)
    - Test Your Knowledge About ID Theft and Account Fraud quiz (2 pages)
    - Savvy Consumer quiz (1 page)
    - Sample letters (3 pages)
- Training evaluation form (1 page)
- OPTIONAL: Printout of the *ID Theft and Account Fraud Backgrounder* and the PowerPoint presentation

Lesson outline

- Welcome and training overview (5 minutes)
- How ID theft and account fraud happen (25 min)
- The effects of ID theft and account fraud (10 min)
- Identity theft prevention (includes *ID Theft Prevention Checklist*) (25 min)
- *Activity:* Test Your Knowledge About ID Theft and Account Fraud quiz (20 min)
- Break (10 min)
- ID theft cleanup (25 min)
- *Activity:* Savvy Consumer quiz (10 min)
- *Optional activity:* Identity Theft Interactive Quiz (downloadable)* (15 min)
- Identity theft resources (5 min)
- Questions and answers (10 min)
- Wrap-up and evaluation (5 min)

* The ID Theft Quiz game is an educational tool that can be used to complement and reinforce the ideas and concepts discussed in the ID Theft and Account Fraud training module. To use the game, download the instructions (PDF) and a PowerPoint presentation containing the game slides at www.consumer-action.org/outreach/articles/id_theft_quiz/.

© Consumer Action 2012
Rev. 6/19

Instructor's notes:

This training module consists of a brochure (*ID Theft & Account Fraud: Prevention and cleanup*); a backgrounder, written in question-and-answer format; a lesson plan that includes class activities; and a PowerPoint presentation. It was created by the national non-profit organization Consumer Action to be used nationwide by organizations providing personal finance, consumer and housing education in their communities.

Before conducting the training, familiarize yourself with the brochure, the backgrounder, the lesson plan (including activities) and the PowerPoint visual teaching aid.

The PowerPoint presentation contains notes for each slide (appearing below the slide when in Normal view or Notes Page view). These notes offer detailed information about the items appearing on the slide. The lesson plan includes indicators so you will know which slide corresponds to each part of the lesson, and when to move to the next one.

Why Adults Learn, a PowerPoint training for educators, provides tips for teaching adults and diverse audiences—it will be helpful to you even if you have taught similar courses before. The slide deck is available at the Consumer Action website (www.consumer-action.org/outreach/articles/why_adults_learn/).

WELCOME AND TRAINING OVERVIEW (5 minutes)

→**SLIDE #1** (onscreen as participants arrive; direct early arrivals to begin reading the brochure [and backgrounder, if provided])

Welcome participants and introduce yourself.

If you have a small group, you can ask individuals to introduce themselves (or, if time permits, ask them to pair off with someone seated near them and then introduce each other to the group) and tell you what they hope to get out of the training. In a larger group, invite a few volunteers to share their expectations. On your whiteboard or easel pad, jot down some of the specific things participants mention. You can come back to this at the end of the class to make sure you've covered these points. (This activity is designed to serve as a brief icebreaker. It will also give you an idea what participants' expectations and needs are.)

Review the contents of participants' packets. Ask the class to take a look inside their packets and make sure they have all the materials needed.

→**SLIDE #2**

Present the learning objectives of the training.

By the end of the lesson, participants will understand:

- The potential damage caused by ID theft and account fraud
- How ID theft and account fraud happen
- How to protect their personal data and avoid becoming a victim
- How to recognize when fraud has occurred
- What their rights are regarding responsibility for fraudulent debts and other fraudulent activity

- What steps to take if they are, or believe them may become, a victim of identity theft
- What resources are available to help consumers and victims

HOW ID THEFT AND ACCOUNT FRAUD HAPPEN (25 min)

Learning objective: Understand how ID theft and account fraud happen.

Key points (slides 3-11):

- Identity theft is surprisingly common, and anyone—from infants to the deceased—can be an identity theft victim.
- You might be a victim and not realize it.
- There are many types of identity theft with varying goals for the thief and varying consequences for the victim.
- Identity theft can happen in unexpected ways, including through an "insider" and as the result of a data breach.

Questions to generate discussion:

- What is identity theft? What is identity fraud?
- Why do you think it's important to learn about identity theft and account fraud?
- Do you think that identity theft is increasing or decreasing? *(It has been increasing.)*
- Is there a typical victim of identity theft? *(No. Victims now include virtually everyone, from babies to senior citizens—even the deceased.)*

Note: When generating discussion, allow a moment or two for participants to respond. You can jot down responses on your easel pad or whiteboard.

→SLIDE #3

Introduction: Identity theft (or "ID theft") is a fast-growing crime. Because the repercussions of identity theft can be so serious, it is crucial that you understand what identity theft is and how it can happen.

Go over slide notes.

Slide notes: Identity theft is rampant, resulting in millions of dollars of damage each year in the U.S. The 2018 Identity Fraud Report from Javelin Strategy & Research reveals that in 2017 the number of identity fraud victims increased by 8 percent, to 16.7 million U.S. consumers, and thieves stole nearly $17 billion.

The most troubling fact about identity theft is that you may be a victim of the crime and not even realize it until considerable damage has been inflicted. It is disturbing to know that newborn babies, senior citizens and even the deceased are often targeted for the crime. These individuals make perfect candidates because the fraudulent use of their personal information can go undetected for years.

The face of identity theft has also changed. Years ago, the most prevalent type of identity theft was "true name" identity theft. This is when a real person's identifying information is used without modification—the thief impersonates the victim when committing the fraudulent act. But this form of ID theft now accounts for only 10-15 percent of fraud because continuous credit monitoring, fraud alerts and credit freezes warn consumers of fraudulent activity. Thieves have responded by modifying their methods, or "wearing a different face." They now commit crimes such as child, medical, criminal or "synthetic" ID theft, which are harder to detect.

→SLIDE #4

Go over slide notes.

Slide notes:
Identity theft vs. identity fraud: What is the difference?
Most consumers use the terms ID theft and ID fraud interchangeably. However, it is important to distinguish between the two crimes. ID theft occurs when someone steals another individual's personal identification information, such as their name, Social Security number, credit card account number, mother's maiden name, driver's license number or medical information. It can start with a lost or stolen wallet, stolen mail, a data breach, a computer virus, a "phishing" scam or paper documents thrown out by you or a business (dumpster diving). The actual misuse of your information to commit a crime is identity fraud. A criminal can commit ID fraud in numerous ways.

Account fraud occurs when someone obtains your information and makes unauthorized charges or withdrawals on current accounts or opens new accounts in your name.

→SLIDE #5

Key points about medical ID theft:

- Medical ID theft occurs when someone obtains medical care or prescription drugs under your name, or files false insurance claims on your policy.
- Medical ID theft can result in more than just financial costs—your health and your life could be at risk because of inaccurate medical records generated from the theft.
- Suspicious medical bills or denied coverage by your health insurance company because you've already reached your benefits limit are signs of potential medical identity theft.
- You have the right to review your medical records and request that mistakes be corrected.
- You can reduce the chances of medical ID theft by being careful with your medical insurance card, shredding medical documents you no longer need and keeping your medical information private.

Go over slide notes.

Slide notes:
Medical ID theft: Medical identify theft occurs when a thief uses an individual's name and personal identity to fraudulently receive medical services, goods or prescription drugs, or in an attempt to commit fraudulent billing. Medical identity theft can have serious consequences, not only in monetary damages, but in compromised personal medical records that can result in misdiagnoses, wrong treatments or wrong prescriptions. Medical identity theft is a *non-credit* identity theft. Therefore, credit monitoring, fraud alerts or credit freezes will not alert you to it or stop it. However, if your credit report reflects a collection account for medical services that you did not receive, this is a useful tip-off that you may be a victim.

According to the FTC (https://www.consumer.ftc.gov/articles/0171-medical-identity-theft), you may be a victim of medical ID theft if: (1) You get a bill for medical services you didn't receive; (2) A debt collector contacts you about medical debt you don't owe; (3) You order your credit report and see medical debts you don't owe; (4) You try to make a legitimate insurance claim and your health plan says you have reached your benefits limit; or (5) You are denied insurance because your medical records show a condition you don't have.
Detecting medical ID theft: Read all medical and insurance statements because they can show warning signs of identity theft. Check the name of the provider, the date of service and the service provided. Check to see if the claims paid match the care you received.

Correcting mistakes in your medical records: The HIPAA Privacy Rule gives consumers the right to inspect, review and receive a copy of their medical and billing records. Consumers can use copies of their medical and billing records to determine the impact of a theft and to identify inaccuracies before seeking additional medical care. Start by obtaining a copy of the notice of privacy practices (NPP) that the HIPPA Privacy Rule requires each hospital and insurer to publish. It describes a consumer's rights, including their right to inspect and obtain a copy of their medical records There is no central source for medical records, so consumers need to contact each provider they do business with—doctors, clinics, hospitals, pharmacies, laboratories and health plans. For example, if a thief got a prescription filled in a consumer's name, the victim may want the records from the pharmacy that filled the prescription and the health care provider who wrote the prescription. There may be fees and mailing costs to get copies of medical or billing files.

Get an accounting of disclosures: Ask each of your health plans and medical providers for a copy of the "accounting of disclosures" for your medical records. The accounting is a log of who has received copies of your medical records. According to the FTC, the law allows you to order one free copy of the accounting from each of your medical providers every 12 months. The accounting includes details about: (1) what medical information the provider sent; (2) when it sent the information; (3) who received the information; and (4) why the information was sent. The accounting shows who has copies of your mistaken records and whom you need to contact.

Ask for corrections: The FTC suggests that you write your health plan and medical providers and explain which information is inaccurate. Send copies of the documents that support your position. You can include a copy of your medical record and circle the disputed items. Ask the provider to correct and/or delete each mistake. Remember to send your letter by certified mail, and ask for a "return receipt" so that you have proof that the plan or medical provider received it.
Patients have the right to file a complaint if they believe their privacy rights have been violated. For example, it would be a violation if a medical provider refused to provide someone with a copy of his or her own medical record. Patients can file a complaint with the U.S. Department of Health and Human Services' Office for Civil Rights (www.hhs.gov/ocr).

Protecting your medical identity: Guard your medical insurance card as you do your credit card. Carry it only when you'll need it. Resist sharing your medical identity in exchange for free gifts or services. Shred any medical documents and prescription bottle labels you no longer need. Contact your insurance company, Medicare or local Medicaid office if your insurance card is missing or stolen.

→SLIDE #6

Key points about criminal ID theft:

- Criminal ID theft occurs when an impostor commits a crime or misdemeanor and gives another person's name and personal information to a law enforcement officer or investigator.
- Because criminal ID theft doesn't show up in your credit report, it can be difficult to detect before it becomes a serious problem (for example, when you are notified there is a warrant for your arrest or you are denied employment).

Go over slide notes.

Slide notes:
Criminal ID theft: Criminal identity theft occurs when an impostor gives another person's name and personal information, such as a driver's license number or Social Security number (SSN), to a law enforcement officer during an investigation or upon arrest. Or, the impostor may present to law enforcement a counterfeit license containing another person's data. If the impostor is cited for a traffic or misdemeanor violation and is released, the impostor will be required to sign the citation and promise to appear in court. In some instances, the imposter may appear in court for the offense and plead guilty. If the impostor fails to appear in court, a bench warrant will be issued, but the warrant will be issued in the name of the innocent ID theft victim.

In other cases, the imposter is arrested and booked for a felony, such as a DUI or another serious offense, and provides the ID theft victim's name and personally identifiable information. This information can end up in one or more criminal records databases.

Similar to financial identity theft, the burden of clearing one's name within the criminal justice system falls primarily on the victim. Criminal identity theft is a *non-credit* identity theft crime. Therefore, credit monitoring services, fraud alerts and credit freezes will not inform you of it or stop the crime. Some victims first learn of the crimes committed by an impostor when stopped for a driving violation and told there is an arrest warrant in their name. Others may learn about the crimes committed in their names when trying to re-enter society after incarceration, or when denied employment or terminated from employment following a background investigation conducted by the employer. In this instance, the employer would have relied upon the criminal history found under the identity theft victim's name. (The employer is legally obligated to inform the victim of the reason for the rejection of employment.)

It can be difficult for a victim of criminal identity theft to clear his/her name. The steps required to clear an incorrect record depend on the laws of the jurisdiction where the crime occurred. Privacy Rights Clearinghouse has created a step-by-step guide to assist victims: "Identity Theft: What to

Do if It Happens to You" can be downloaded at https://www.privacyrights.org/consumer-guides/identity-theft-what-do-if-it-happens-you.

→SLIDE #7

Key points about child ID theft:

- Stealing a child's identity can be particularly attractive to a thief because the crime can go undetected for far longer since children are not actively applying for credit, insurance, employment, etc. (scenarios where they might be alerted to a negative credit report).
- Bills and pre-approved credit offers in the child's name are signs of potential identity theft, as are collection calls, notifications from the IRS that the child's Social Security number has already been used on another return, or denial of public benefits because the child is already listed on another household's account.
- You have the right to opt out of sharing certain information with your child's school.
- Child welfare agencies are required to check the credit reports of foster children age 16 and older.

Go over slide notes.

Slide notes:
Child ID theft: Child ID theft happens when someone uses a minor's personal information to commit fraud. A thief may steal and use a child's information to get a job, government benefits, medical care, utilities, a car loan or a mortgage. Avoiding, discovering and undoing the damage resulting form the theft can be a challenge. A thief who steals a child's information may use it for years before the crime is discovered, since most parents or guardians are not checking their child's credit file—they may not even realize they have one. The child victim may learn of ID theft only years later, when applying for credit, a job, an apartment or insurance.

According to the FTC, there are a few signs that can tip you off to the theft: (1) A child or a family is denied government benefits because benefits are being paid to another account that is using the child's Social Security number. (2) You are getting calls from collection agencies, bills from credit card companies or medical providers, or offers for credit cards or bank accounts in your child's name, even if your child has never applied for or used these services. (3) After you file a tax return listing your child's name and Social security number, you get a notice from the IRS that the same information is listed on another return, or your child gets a notice from the IRS stating that he or she failed to pay taxes on income, even though your child has no income.

If you think your child's information is at risk—specifically, you see warning signs, or you may have lost your child's Social Security card, had a break-in, or your child's information was compromised in a data breach at school or in a doctor/dentist office—you may want to check whether your child has a credit report. Follow the instructions at the CFPB website: https://www.consumerfinance.gov/ask-cfpb/how-do-i-check-to-see-if-my-child-has-a-credit-report-en-1865/.

Protecting your child's identity: The FTC's guide "Child Identity Theft" (https://www.consumer.ftc.gov/articles/0040-child-identity-theft) provides consumers with step-by-

step instructions for keeping a child's identity safe and steps to take if a child's identity has been compromised.

Protect your child's personal information at school: The federal Family Educational Rights and Privacy Act, enforced by the U.S. Department of Education, protects the privacy of student records. It also gives parents of school-age kids the right to opt out of sharing information. See the FTC's fact sheet "Protecting Your Child's Personal Information at School" (www.consumer.ftc.gov/blog/protecting-your-childs-personal-information-school) for more information.

Protecting foster kids' credit: Children and youth in foster care are particularly vulnerable to ID theft because their personal information is often shared among caretakers, service providers and schools. Under federal law, when a foster child turns 16, child welfare agencies are required to get the youth's annual credit report. In cases of ID theft, the agency must help the youth clear up their credit. The FTC and Child Focus, Inc. created a guide entitled "Youth and Credit: Protecting the Credit of Youth in Foster Care" to provide anyone working with these young people with the tools to help if their identity has been stolen, and to teach teens about credit, why it is important to their future financial stability, and how bad credit can derail their goals. A copy can be downloaded at https://www.aecf.org/resources/youth-and-credit/.

→SLIDE #8

Key points about theft of a deceased person's identity:

- Thieves sometimes target the deceased because it can be a long time before creditors learn of the death and close accounts or the credit bureaus deactivate the deceased consumer's files.
- Calls from a creditor or collection agency about an account opened or used in the deceased's name after death is a sign of possible identity theft.
- You can decrease the chances of this type of ID theft by limiting the details you provide about the deceased in the obituary and by taking the initiative to notify creditors, insurance companies, credit bureaus, financial institutions, government agencies, etc. about the death as soon as possible.

Go over slide notes.

Slide notes:
Theft of a deceased person's identity: The deceased are an irresistible target for ID thieves because it can take longer for the fraudulent activity to be detected. According to Fact Sheet 117: "Identity Theft and the Deceased: Prevention and Victim Tips" from the Identity Theft Resource Center (ITRC) (https://www.idtheftcenter.org/knowledge-base/identity-theft-and-the-deceased-prevention-and-victim-tips/), thieves might obtain information about the deceased by reading obituaries, stealing death certificates or even tapping into the Social Security Death Index.

Be proactive. Financial institutions are not immediately made aware that a customer is deceased. In most cases, a funeral director will report the person's death to the Social Security Administration (SSA) (Statement of Death by Funeral Director). Delays in the SSA's transmission of the Death

Master File to the financial industry can provide time for ID thieves to collect enough personal information to open credit accounts or commit other fraud using the deceased's information. Until the credit reporting agencies and creditors are notified of the death, the accounts of the deceased will remain open. The ITRC reports that a credit account can remain open for up to 10 years without activity.

Steps to take when a loved one dies: The following steps are recommended by the ITRC for all deaths, regardless of age:

1. Obtain at least 12 copies of the official death certificate when it becomes available. You'll need the copies to notify each creditor, insurance company, bank or credit union, brokerage house, SSA, VA, DMV, pension issuers and any professional licensing agencies (Bar association, medical board, notary (secretary of state), real estate board, cosmetology board, etc.). Consider sending everything by certified mail, return receipt requested.

2. If there is a surviving spouse or other joint account holder, that individual should immediately notify credit companies, banks, stock brokers, loan/lien holders and mortgage companies of the death. The executor or surviving spouse will need to determine how open accounts and outstanding debts will be dealt with. You may need to transfer the account or close it. If you close the account, ask the creditor to list it as "Closed—Account holder is deceased."

3. Order a copy of the decedent's credit reports. If you suspect fraud, place a "Deceased alert" on the reports. If you have evidence of fraud (collection calls and notices, bills, fraudulent accounts on the credit report, etc.), notify the police department as well as the affected credit issuers, collection agencies, utilities, telecommunications companies, etc. Provide each with a copy of the death certificate and other supporting documents as proof. In the event that the thief is a family member, it may be best to seek professional advice on a course of action from a family law attorney.

Limiting the details about the deceased in the obituary and any newspaper articles can help reduce the chances of identity theft. Don't include the decedent's exact address, maiden name or any other information that would likely be needed to apply for a credit card, open a bank account, apply for insurance, etc.

→SLIDE #9

Key points about how thieves get their victims' information:

- Thieves can steal personally identifiable information in a variety of ways, including finding or stealing your wallet, phone or computer; taking the mail out of your box or filing a change of address to reroute your mail; rummaging through your trash (called "dumpster diving"); watching as you punch in your password or PIN or listening as you say your credit card number; sending "phishing" messages that purport to be from legitimate agencies and companies; buying customer information from a dishonest employee; intercepting your information as you shop online at unencrypted sites or use social media; and accessing your phone rcords.
- "Familiar fraud" is what ID theft is called when the thief is a person known to the victim.
- You can reduce the chances of a thief getting your private information by taking precautions to protect it.

Go over slide notes.

Slide notes:

How do thieves get your information? Many identity thefts are cases of "familiar fraud," in which a person known to the victim has access to the victim's statements or other documents. But skilled ID thieves can steal your identity through a variety of methods. For example, they steal wallets, purses and cell phones containing your personally identifiable information and credit and bank cards. They steal your mail, including your bank and credit card statements, pre-approved credit offers, new checks and tax information. They complete a "change of address" form to divert your mail to another location. They rummage through your trash (dumpster diving) or the trash of businesses for sensitive paper documents. They fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate need for, and legal right to, the information. They get your information through a practice known as "business record theft," by stealing files out of the offices where you're an employer or employee, customer, patient or student. They find the personal information that you shared about yourself on the internet. They "shoulder surf" or eavesdrop on your cell phone calls or send tricky phishing emails (emails designed to look like messages from a legitimate business, but which lure you into revealing your login or other confidential information, often at a bogus—or "spoofed"—website, or clicking on a link that downloads malicious software onto your computer that captures your online banking credentials as they are typed).

They access your phone records: Phone records are a treasure trove of information for identity thieves. Your telephone records may include your billing address and, if different, your home address; long distance and local toll numbers called; calls billed to a calling card or credit card; and numbers from which collect calls were accepted. ID thieves can also use the dates and lengths of calls outside your local calling area. In addition, your wireless phone records may include the numbers of all phone calls made or received by you and other family plan members. Your phone account online may also include bank or credit/debit card information you provided to pay your bills automatically. Information the company keeps about you may also include your birth date, your Social Security number, and all telephone and data/internet services you subscribe to.

How to protect yourself when using a mobile device:

- *Use a strong passcode.* Although a four-digit passcode is better than nothing, a longer code that utilizes letters and symbols is far stronger.
- *Install apps cautiously.* Vet the apps you install.
- *Be alert when using public Wi-Fi.* Before conducting any online transactions in a "hotspot" (public Wi-Fi, usually in places such as airports, coffee shops, etc.), check its privacy policy to see if it secures wireless transmission of your data.
- *Use antivirus/anti-malware software.* Guard your information from malicious applications by keeping your antivirus/anti-malware up to date.
- *Be responsible.* Do not reveal sensitive or personal information on social networking sites.

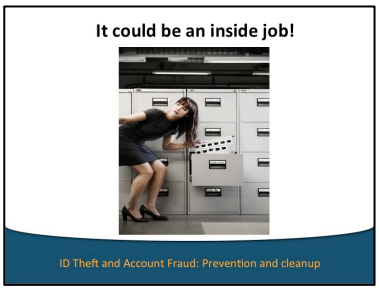
→SLIDE #10

Key points about "insider" ID theft:

- ID theft often is an "inside job," perpetrated by an employee, employer, family member, friend or acquaintance.

- If the ID thief is a family member or friend, you must decide whether or not to involve police.

Go over slide notes.



Slide notes: According to most security experts, ID theft often is an "inside job." Specifically, when a data breach or ID theft of a business occurs, it is often not the result of a hacker breaking into a secure data system and pilfering sensitive information, but is likely the work of an employee. Business ID theft perpetrators are often former or current employees with direct access to accounting "books" and other financial documents. Inside jobs are becoming more difficult to detect and prevent due to outsourcing.

Family secrets: What if you're related to the thief?
The information most likely to be taken in familiar fraud includes name, Social Security number, address and checking account number. But what do you do when you know your thief? The Identity Theft Resource Center's "Fact Sheet 115: When You Personally Know the Identity Thief" (https://www.idtheftcenter.org/knowledge-base/when-you-personally-know-the-identity-thief-what-are-your-options-when-you-know-the-imposter/) offers three courses of action that a victim can take when the imposter is someone they know:

1. Cooperate with law enforcement's investigation. (Proceed as if this were a regular case of ID theft and file a police report—this is not the same as pressing charges against the person.)
2. Work with creditors to see if a resolution can be made without police involvement.
3. Pay the debt and live with the consequences.

As noted by Privacy Rights Clearinghouse in its Fact Sheet 17a: "Identity Theft: What to Do if It Happens to You" (https://privacyrights.org/consumer-guides/identity-theft-what-do-if-it-happens-you), in most jurisdictions, to get the protection of federal and state laws, you must have a police report.

→SLIDE #11

Key points about data breaches:

- There are many ways a security breach can occur—all of which are out of your control.
- A majority of states have laws requiring that individuals be notified when a breach compromises their personal information. In some cases, even if your state does not have a security breach notification law, you may be entitled to notification under federal law.
- Data breach victims are at higher risk to become fraud victims, so pay attention to any notifications you receive and take advantage of any offer from the company for free credit monitoring.

Go over slide notes.

Slide notes:
Data breaches: Have you ever received a letter from a university, a bank or a company that you're doing business with informing you that your personal information—date of birth, Social Security number (SSN) or driver's license—may have been stolen? Or you were watching the news and learned about a security breach at a company you do business with? Your odds of becoming an identity theft victim are increased with a breach that reveals your confidential information.

There are many ways a security breach can occur, including:

- A thief hacks computer files containing the personal information (Social Security number, driver's license number, etc.) of the customers, account holders, students, etc. in the database.
- A dishonest employee obtains your private records and sells them to criminals.
- A company's laptop that contained account data with the personal information of its customers was stolen.

As the victim of a data breach, what are your rights? A majority of states have laws requiring that individuals be notified when a breach compromises their personal information. If your state does not have a security breach notification law, you may be entitled to notification under federal law. The Gramm-Leach-Bliley Act (GLB) requires that financial institutions subject to the Act notify customers when there has been unauthorized access to customer data if, after an investigation, the institution determines the data has been or is likely to be misused.

Steps to take if you're the victim of a data breach: If you receive a data breach notification, take it very seriously. If the company or organization whose database was breached offers you a free monitoring service, you should take them up on it. Consumer Action, the National Consumer Law Center and U.S. PIRG created an alert that lists the steps that a victim of a data breach can take: www.consumer-action.org/index.php/alerts/articles/data_breach_victim_steps_you_can_take_now.

THE EFFECTS OF ID THEFT AND ACCOUNT FRAUD (10 min)

Learning objective: Understand the effects of ID theft and account fraud, including financial and other (non-financial) costs.

Key points (slide 12):

- The effects of ID theft can be financial, emotional and legal. Victims can lose hours of their time trying to clean up the mess. They may even pay the fraudulent debts just to end the ordeal. ID theft can take an emotional toll (stress resulting from collection calls, rejected applications, etc.). It can result in missed opportunities, higher costs for credit, and affect job performance. You could even be mistakenly arrested.
- You are not held liable for fraudulent debt. However, there may still be some out-of-pocket expenses.

Questions to generate discussion:

- What are the costs to victims of identity theft and account fraud? **Hint:** Don't think only in terms of financial costs. (*Encourage learners to think of more than just the cost in dollars—the cost in hours [to do all the legwork to clear your name], the cost in lost opportunities [for*

example, if your damaged credit causes you to be rejected for a rental home, a loan or a job], the emotional toll, etc.)

- How/why does it pay to put some effort into preventing identity theft?

→SLIDE #12

Introduction: While there may be some financial costs of ID theft, the non-financial costs can be far greater. The crime can cost victims many frustrating hours reporting the theft, disputing fraudulent accounts and preventing future fraud. In the worst cases, identity theft can cause consumers to be denied loans, refused employment or even arrested for a crime they didn't commit.

Go over slide notes.

Slide notes:
The costs of ID theft and account fraud: Typically, consumers are not held liable for fraudulent debt—the banks and credit card companies generally absorb the allowable $50 of liability under their zero-liability policies. However, many fraud victims end up with some out-of-pocket expenses, for thing like phone calls and postage and, in rare cases, legal fees (for example, if the criminal's actions under the victim's name led law enforcement officials to come after the wrong person). Victims can also spend hours completing paperwork, such as filing a police report, filling out and submitting an ID theft affidavit to creditors, obtaining and reviewing credit reports, disputing fraudulent accounts or charges, etc.

In addition, through no fault of their own, victims also can face:

- Increased credit card fees
- Higher interest rates
- Higher insurance premiums
- Closure of bank/credit union accounts
- Declined rental, job and/or credit applications

Though many of these outcomes can be undone eventually, they can result in extreme hardship and expense for some period of time, and can cause irreparable damage in the form of missed opportunities.

IDENTITY THEFT PREVENTION (25 min)

Learning objective: Understand how to avoid becoming a victim of identity theft and account fraud.

Key points (slides 13-21):

- Protect your information: There are many steps you can take—track your mail, shred documents, monitor your account transaction statements, keep your PINs and passwords secret, notify agencies (IRS, DMV, SSA) if you have reason to be concerned, place a

deceased alert when a loved one passes, etc.—to make it harder for identity thieves to get your sensitive personal data.

- Monitoring your credit and specialty reports regularly is one of the best ways to catch identity theft early. (You are entitled to a free copy of each report every 12 months.)

Questions to generate discussion:

- What are some ways you could make it more difficult for identity thieves and scammers to get your information? *(List responses on your easel pad or whiteboard.)*
- How many of you already do one or more of these things?

→SLIDE #13

Introduction: While experts agree that you can't entirely eliminate the possibility of identity theft, you can greatly reduce your risk by taking steps to protect your information.

Go over slide notes.

Slide notes:
Financial and account information: Check bills and account information immediately. Track mailed statements, new credit/debit cards and printed check orders. Shield the ATM pad when entering your PIN. Beware of shoulder surfers and eavesdroppers when using your cell phone. Shred all documents with your Social Security number before discarding. Notify the Social Security Administration and credit bureaus of the death of a loved one. If you believe that your driver's license has been compromised, contact the fraud department of your state's DMV to learn your options. Regularly install and update firewall, antivirus and antispyware on your computer. Use secure websites. (Look for the padlock symbol and an "s" after "http" in the browser's address bar.)

As with all financial ID theft crimes, checking your credit report for inaccuracies and using a credit monitoring service will allow you to detect signs of "true name" ID fraud.

How do I get a copy of my credit report? You are entitled to one free credit report every 12 months from Equifax, Experian and TransUnion through AnnualCreditReport.com (877-322-8228/Annual Credit Report Request Service, PO Box 105281, Atlanta, GA 30348-5281). There are many similarly named credit report services, but AnnualCreditReport.com is the only one that is truly free. If you believe that you're a victim of ID theft, order all three of your reports and examine them carefully, looking for signs of fraud. Continue to monitor your credit reports until any fraudulent activity has been cleared up and there are no new signs of identity theft.

What's not in your credit report? Synthetic ID theft is a variation of ID theft in which identities are completely or partially fabricated. The most common form of synthetic ID theft involves combining a real SSN with a name or birth date other than the one associated with the number. This form of ID theft is difficult to track or detect because it may not show up on your credit report because the activity is being reported under a different name, date of birth, etc. According to the Identity Theft Resource Center, although the fraudulent activity may not be reported on your credit report, the information can still negatively impact an individual's ability to obtain credit, and may create various other identity and credibility issues for the victim. With just your SSN, thieves can create a brand

new identity, one that may not be stopped by a fraud alert, freeze or credit monitoring service, but these identities will likely show up in national databases. For example, in the section on criminal ID theft, it was mentioned that most individuals learn they are a victim of ID theft when stopped for minor traffic violation or when turned down for or fired from a job as a result of a background check.

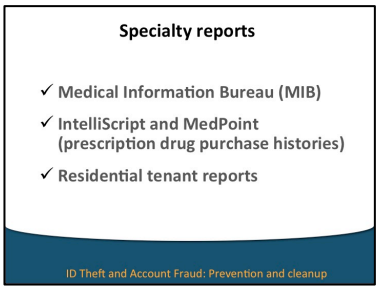
Specialty consumer reports: Consumer reports include not only those that track your bill payment (credit) history, but also those that compile information about things like your rental history, insurance claims history, prescription history, etc. and are provided to employers, insurance companies, banks and landlords. It is these national databases that can hold the key for early detection of possible identity theft. Scanning national databases such as LexisNexis, C.L.U.E, MIB, ChexSystems, etc. can reveal misuse of your SSN. Under the Fair Credit Reporting Act, you are entitled to a free report every 12 months from all nationwide specialty reporting agencies (those that compile reports for targeted users). The CFPB has created a list of specialty consumer reporting agencies: http://files.consumerfinance.gov/f/201207_cfpb_list_consumer-reporting-agencies.pdf.

→SLIDE #14

Key points about medical and prescription reports and residential tenant reports:

- Specialty reports don't exist for everyone, but it's likely there is at least one report on most people.
- The Medical Information Bureau (MIB) compiles reports that insurance companies use to determine someone's health risk level. Not everyone has an MIB file.
- IntelliScript and MedPoint report drug purchase histories.
- There are at least four major tenant history report companies (see slide notes for details).
- ID thieves can gain access to your personal information for the sole purpose of using it to rent an apartment or house. If you are looking to rent, consider ordering your tenant report(s) before you apply so that you can correct any inaccuracies or be prepared to explain any negative information.

Go over slide notes.



Slide notes:
Specialty consumer reports: There is no centralized source for obtaining free specialty reports. Requests must be made directly to each specialty reporting agency. FTC regulations do not require specialty consumer reporting agencies to establish a website or allow mail-in requests. The only requirement is that they maintain a toll-free number.

Medical Information Bureau (MIB): The MIB provides background information to its insurance company members so they can determine who they will accept or reject for insurance. A medical history report lists medical conditions you've reported on insurance applications for individual (not group) coverage, test results from medical underwriting exams, smoking history, participation in risky activities (such as skydiving) and, sometimes, driving records. The report does not include the details of your medical records kept by your health care provider.

To obtain a free copy of your MIB file, call 866-692-6901 or visit www.mib.com/html/request_your_record.html. According to the site. MIB will not have a file on you if you have not applied for individually underwritten life, health or disability insurance during the preceding seven years. You'll need to provide some personal identification information for them to find your file, if one exists.

IntelliScript and MedPoint: These are databases that report drug purchase histories, including dosages, refills and doctor visits. To obtain a free copy of your consumer IntelliScript file, call 877-211-4816 or visit http://www.rxhistories.com/ContactUs/. To obtain a free copy of your MedPoint file, call 888-206-0335 or visit https://www.annualmedicalreport.com/order-your-medical-report-file-from-medpoint-by-ingenix-inc/.

Residential tenant reports: Whether you rent or own your home, you should check your rental history yearly. ID thieves can gain access to your personal information for the sole purpose of using it to rent an apartment or house. If you're looking to rent and likely to be subject to a tenant screening, order your tenant reports before shopping for your new home so that you have time to correct inaccuracies or to be prepared to explain any negative information to a prospective landlord. Numerous companies prepare reports for landlords on individuals who have applied to rent housing:

LexisNexis Resident History Report: Contains information related to your tenant history as well as other background info. Call 888-497-0011 or visit https://personalreports.lexisnexis.com/index.jsp.

CoreLogic SafeRent*:* Provides landlord-tenant court records specific to rental housing payments, criminal background screening, resident scoring and access to traditional credit reports. Criminal background screening can include information about felonies, misdemeanors and sex offenses. Call 800-815-8664 or visit http://corelogic.com/downloadable-docs/saferent-consumer-disclosure.pdf.

RentBureau (owned by Experian): Receives rental payment data from its national network of multifamily property management companies. This data is accessed by resident screening companies for use during the rental application process. Call 877-704-4519 or visit www.experian.com/rentbureau/rental-payment.html.

Tenant Data: Provides information not only on rental payment history but also on personal suitability as a potential resident. (*Tenant Data does not cover the entire U.S.—primarily only properties located in Nebraska, Iowa and Arkansas.)* Call 800-228-1837 or visit http://tenantdata.com/for-consumers/your_personal_report.html.

→SLIDE #15

Key points about check-writing history reports:

- ChexSystems provides information used by banks and credit unions when you try to open an account. They can also use the information to try to collect on unpaid overdrafts and fees.
- Certegy (formerly SCAN) and TeleCheck both track instances of returned checks and checking account fraud for use by retailers and other businesses that accept checks.

Go over slide notes.

Slide notes: There are three major nationwide specialty consumer reporting agencies that compile checking account history reports: ChexSystems, Certegy (formerly SCAN) and TeleCheck.

ChexSystems collects and maintains information from banks and credit unions regarding account holders. For example, if a bank closes your checking account because of mismanagement, it will report the closure and reason to ChexSystems. When you apply for a new account at another financial institution, that bank or credit union can learn how you managed your previous accounts. If you have had checks stolen or bank accounts opened fraudulently as a result of identity theft, ask the bank to report the incidents to ChexSystems. If your personal information was used to set up fraudulent bank accounts, you can request that ChexSystems place a security alert on your file. Obtain a free copy of your ChexSystems report by calling 800-428-9623 or visiting www.consumerdebit.com/consumerinfo/us/en/chexsystems/report/index.htm.

Certegy (formerly SCAN) maintains a database of returned checks and instances of checking account fraud. It provides check authorization and verification services to member retailers. To contact Certegy for a free copy of your consumer file, call 866-543-6315 or visit https://www.askcertegy.com/FACT.jsp for information about ordering your report by mail.

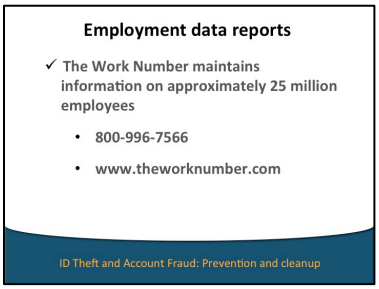
TeleCheck, like Certegy, maintains a database of returned checks and instances of checking account fraud and provides check authorization and verification services to member retailers. For a free copy of your report, call 800-835-3243 or visit https://www.firstdata.com/content/dam/FirstData/telecheck/telecheck-file-report.html.

→SLIDE #16

Key points about employment data reports:

- Employment data reports are not the same as employment background check reports.
- The Work Number tracks employment and income history as well as employer-sponsored medical and dental benefits and unemployment claims.
- The Work Number will also help child support workers locate non-custodial parents by providing information on most recent employment. Social service agencies may also use The Work Number to verify eligibility for benefits.

Go over slide notes.



Slide notes: ID thieves may use your Social Security number to get a job or to apply for government benefits, such as unemployment or welfare.

The Work Number is an employment and income verification database operated by Equifax, one of the three major credit bureaus. Your report contains things like paystub data and HR-related information (for example, whether you've ever filed an unemployment claim or if you have employer-sponsored medical/dental insurance).

Lenders, apartment managers and pre-employment screening services are among the users of The Work Number's employment verification services. Social services agencies may also use The Work Number to verify eligibility for benefits. In child support cases, the recent employment information in a Work Number report can be used by child support workers to locate non-custodial parents.

To obtain your employment data report, visit https://www.theworknumber.com/employees/employment-data-report/ and follow the instructions for one of the request options. If you have questions, call 800-996-7566. (Note: If your employer has not subscribed to the service, there will be no information about you in the database. If your employer is supplying information to The Work Number, you are entitled to one free report every 12 months.)

→SLIDE #17

Key points about insurance claims history reports:

- ID thieves can use your stolen identity to obtain insurance policies or make false insurance claims.
- There are separate reports for auto claims and personal property (homeowners/renters) claims.

Go over slide notes.

Slide notes: Identity theft crosses the line into insurance fraud when thieves use your stolen identity to obtain insurance policies or make false insurance claims. For example, an ID thief could apply for a vehicle insurance policy using your stolen driver's license and Social Security numbers. Upon receiving the insurance coverage, the identity thief almost immediately would have a questionable accident or report the vehicle as stolen and submit a false insurance claim in an effort to collect money from the insurer for the supposed loss or damage.

The C.L.U.E. and ISO Personal Property reports provide a seven-year history of personal property insurance claims; the C.L.U.E. and ISO Auto reports provide a seven-year history of automobile insurance claims The data reported for each loss includes date of loss, loss type and amount paid, along with general information such as policy number, claim number and insurance company name.

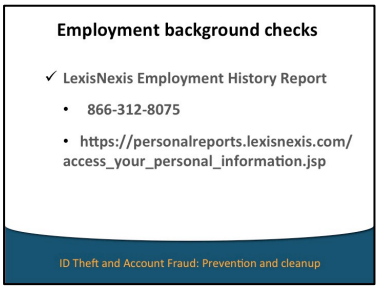
→SLIDE #18

Key points about employment background check reports:

- An employer must ask your permission before requesting a credit or background report on you; however, your job application might be rejected if you say no.
- If the employer decides not to hire or promote you or fires or reassigns you because of information in your report, you must be given a copy of the report.
- You might not be able to get a free annual copy of your report because some screeners evaluate you but do not maintain a file.

- More decision-makers (employers, lenders, etc.) are running social media background checks or doing their own social media checks on applicants—something you should consider as you decide what to share on social media.

Go over slide notes.



Slide notes: A background check can include everything from marital status to criminal records and credit reports—some even include character references and interviews with your neighbors. Many companies run background checks on applicants.

Notice and authorization: An employer cannot get a report about you for employment purposes without getting your permission first (usually written). Of course, if you don't give your permission, your application for employment might not get a second look. Before an employer can obtain reports about you, it must tell you that it might use the information to make a decision. (If an employer notifies you that a background check will be conducted, you can ask for the name of the screening company. However, you can only get a free disclosure if the company *maintains* a file on you. Some screeners evaluate you but do not maintain a file.)

Pre-adverse action procedures: Before taking an adverse employment action (such as rejecting your job application or a promotion, or terminating your employment or reassigning you), the employer must give you a notice that includes a copy of the consumer report the employer used to make the decision and a copy of *A Summary of Your Rights Under the Fair Credit Reporting Act*. The report is free if you ask for it within 60 days of learning of the adverse action.
To request your LexisNexis report, call 866-312-8075 or visit https://personalreports.lexisnexis.com/access_your_full_file_disclosure.jsp

Social Intelligence Corp. (https://www.socialintel.com/) runs social media background checks on prospective employees. It searches through Facebook photos, videos and groups as well as Twitter, YouTube and other social media platforms. Learn more at https://www.socialmediatoday.com/content/social-intelligence-corporation-can-keep-your-social-trail-7-years. According to a Wall Street Journal article (https://www.wsj.com/articles/borrowers-hit-socialmedia-hurdles-1389224469), "more lending companies are mining Facebook, Twitter and other social-media data to help determine a borrower's creditworthiness or identity."

→SLIDE #19

Key points about utility reports:

- Consumers' telephone and utility account histories are used by service providers to determine whether to require a deposit on new accounts and in what amount, and to collect past-due amounts on old accounts.
- If an identity thief has opened and/or abandoned an account in your name, it could appear here.

Go over slide notes.

Slide notes: The National Consumer Telecom & Utilities Exchange (NCTUE) is a member-owned database housed and managed by Equifax, one of the three major credit reporting agencies. Membership is available to telecommunications and utility companies.

NCTUE's stated objectives are:

- Early indication of higher-risk accounts for new residential service applicants
- Locating former customers whose service was terminated with an unpaid balance
- Identification and implementation of additional uses of the data to benefit members

Although the NCTUE shares account information among its members (in part to aid the collections process and to help members assess service deposits and identify higher-risk consumer applications), the company emphasizes that the decision to require a service deposit, and the amount of that deposit, is left up to each individual member.
You can find out if the NCTUE maintains information about you at https://www.nctue.com/consumers.

→SLIDE #20

Key points about internet safety:

- The internet is a valuable tool, but not everybody on the internet is your friend or has your best interests at heart.
- There are many threats on the internet, some of which can result in the theft of your identity.
- There are many precautions you can take and tools you can use to protect your information on the internet.
- Employers *and* ID thieves check social media for information, so it's a good idea to be careful about what you share; in other words, don't reveal too much.
- By law, parents have some control over the online collection of their children's personal information.

Go over slide notes.

Slide notes:
What are some of the risks that internet users face?
The main risks internet users face include:

- Inappropriate or unwanted contact (cyberbullying and spam, for example)
- Inappropriate or inaccurate content (pornography and hate sites, for example)
- Deceptive or fraudulent commerce (counterfeit and malicious sites, for example)

How do crooks and con artists find their victims online?

Phishing: An attempt to "hook" you into revealing your personal and confidential information by sending emails that appear to come from a legitimate business

Spam: Unwelcome email and instant messages, which may offer goods of little or no value or a promise of financial rewards if you give the sender money

Malware: Malicious software (spyware, Trojans, viruses and worms) that can be remotely installed on your computer, making it possible for the person who controls the malicious software to steal, damage or delete your files and other data

Malicious websites: Harmful sites that lure users by promising content on popular breaking news stories, offers from retailers or other desired information. Links to such sites can be included among online search results, sent to you via email or appear on social media (such as Facebook, Twitter, etc.).

Transactions that are not secure: Sites that don't have secure payment forms, or companies that store debit and credit card information without proper safeguards (possibly giving crooks the opportunity to intercept your personal information)

Social networking: Sites and platforms that enable you to reveal too much personal information, or the sites compromise your personal data

The revised **Children's Online Privacy Protection rule** went into effect in 2013. The new rule gives parents greater control over online collection of their children's personal information. The rule widens the definition of children's personal information to include persistent identifiers, such as cookies that track a child's activity online, geolocation information, photos (depending on your settings, your smartphone may be using its built-in GPS capability to embed your exact location into the photos you take using the device's built-in camera), videos and audio recordings. For more information on the Children's Online Privacy Protection Rule, see the FTC's announcement at www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.

For more about protecting your privacy and security on the internet, see Consumer Action's *Questions & Answers about Internet Safety:* www.consumer-action.org/modules/articles/questions_answers_about_internet_safety_trainers_manual.

→SLIDE #21

Key points about placing an active duty alert:

- An active duty alert is a special form of protection for members of the military who are away from their regular duty station.
- The alert requires creditors to verify your identity before granting credit in your name.

Go over slide notes.

Slide notes:
Under the Fair Credit Reporting Act, military personnel are allowed to place an "active duty" alert in their credit reports while on deployment (i.e., away from their usual duty station). The alert requires creditors to verify the identity of the servicemember before granting credit in his or her name. The business may try to contact the servicemember directly, but if the servicemember is on deployment, that could be impossible. As a result, the law allows the

servicemember to use a personal representative to place or remove the alert.

Active duty alerts are effective for one year, but servicemembers can have the alert removed sooner. Servicemembers on deployment longer than a year may place a second alert on their credit reports.

To place an "active duty" alert or to have it removed, contact one of the three national consumer reporting companies (Equifax, Experian or TransUnion), and that company will notify the other two.

When a servicemember places a fraud alert in his or her credit reports, his/her name will be removed from the national consumer reporting companies' marketing lists for prescreened offers of credit and insurance for two years unless the servicemember specifically requests that their name remain on the lists.

ID Theft Prevention Checklist

Ask participants to remove the ID Theft Prevention Checklist (page 32) from their packets and have them check off the things on the list they have already done. Encourage them to use the list after class as a guide for next steps.

ACTIVITY: Test Your Knowledge About ID Theft and Account Fraud quiz (20 min)

Ask participants to take the *Test Your Knowledge About ID Theft and Account Fraud* quiz from their folders.

You can have participants work on the exercise alone or have them break into small groups and work together to answer the questions. (If you are running short on time, you can split the room into two groups and have each group work on one of the two pages, or break it into three groups and assign five questions to each group.) Ask for volunteers to answer questions (if done individually) or rotate among groups for responses, allowing the spokesperson from each group to provide the correct answer along with their reasoning.

BREAK (10 min)

Announce a 10-minute break. Make yourself available for a few minutes to direct people to the restroom or a place to get drinks and snacks.

ID THEFT CLEANUP (25 min)

Learning objective: Understand what steps to take if you become a victim of identity theft.

Key points (slides 22-27):

- Being aware of the signs of identity theft will enable you to stop it sooner rather than later.
- Inmates can be at greater risk, so before leaving prison, they should take steps to find out if their identities were used while they were incarcerated.

Questions to generate discussion:

- Frequently, victims of ID theft are unaware that their identity has been stolen. How could that be?

- How do you think you could find out if your identity has been stolen? What are some signs that would indicate you might be a victim of identity theft? *(See slide notes for examples.)*
- What are some of the steps you think a victim would need to take to undo the damage done by an identity thief? Whom do you think you should notify?

→SLIDE #22

Slide notes: Are you already a victim of ID theft? What are the signs?

- Suspicious accounts or incorrect information appearing in your credit file
- Bills or collection calls that are not yours
- Denied credit applications despite your good credit
- Bills or account statements missing from your mail
- Bills and credit offers addressed to your child or your deceased loved one
- Notice from the IRS or a tax professional that you have already filed a return (i.e., someone has filed a return using your information); you have an unexpected balance due or a refund offset; collection action is being taken against you for a year you didn't't file; or you received wages from an employer you have not worked for

Consumers who believe their identity may have been used for tax purposes should contact the IRS immediately. If you could be at higher risk due to a lost/stolen purse or wallet or suspicious account activity, contact the IRS Identity Protection Specialized Unit (800-908-4490) so steps can be taken to secure your account.

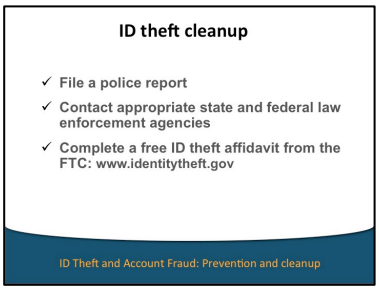
People leaving prison: Inmates can be at greater risk of identity theft and fraud—often at the hands of their own relatives (see article at www.creditcards.com/credit-card-news/how-to-prepare-inmate-financially-jail-prison-1265.php). The Reentry Survival Manual (https://www.paep.uscourts.gov/sites/paep/files/Reentry_Survival_Manual.pdf), published by Rutgers University, suggests that before leaving prison, individuals should conduct a background and credit check on themselves to find out if their identities were used while they were incarcerated. (See slide 18 for information about requesting your LexisNexis background report.)

→SLIDE #23

Key points about ID theft cleanup:

- It's important to file a police report—it will help you deal with creditors, collectors, etc.
- Close the accounts that you know have been tampered with or opened fraudulently.
- By law, companies must give you a copy of the application or other records relating to your identity theft if you submit your request in writing, accompanied by a police report. *(Refer participants to their packets for the "Letter to existing creditors.")*

Go over slide notes.



Slide notes: File a police report and get a copy, which should include the case number. If you can't get the local police to take a report, try a county or state law enforcement agency. Check with your state's attorney general to find out your rights as a victim of ID theft.

The FTC ID Theft Affidavit is a useful tool to assist victims of identity theft restore their good names. The ID Theft Affidavit can be used to report information to many companies, simplifying the process of alerting businesses where a new account was opened in your name.

You may also want to notify the Social Security Administration and the IRS, in case a thief used your SSN to get a job, apply for benefits or file a tax return. If you believe that your driver's license has been counterfeited, you should notify the fraud department of your state DMV and request a fraud alert or learn the options available to you.

If your ATM and/or debit card has been stolen or compromised, report it immediately. Contact your bank and fill out a fraud affidavit. Get a new card and account number, and change your password. ATM and debit card transactions are subject to the Electronic Fund Transfer Act. Even if you're a victim of ID theft, your liability for charges can increase the longer the crime goes unreported (check your account activity often to catch problems sooner). If you have had checks stolen or bank accounts set up fraudulently, ask your bank to report it to ChexSystems, and request that a security alert be placed on your file.

If you believe that phone service was established in your name, learn what to do in Consumer Reports' article *A New Threat to Your Finances: Cell-Phone Account Fraud* (https://www.consumerreports.org/scams-fraud/cell-phone-account-fraud/).

You should dispute and close all affected accounts and notify your existing creditors in writing that you are a victim of ID theft. Be sure to include a copy of the ID Theft Affidavit.

→SLIDE #24

Key points about placing a fraud alert:

- A fraud alert can help protect you from identity theft.
- The 90-day initial alert entitles you to one additional free credit report annually; an extended (seven-year) alert allows you to get two additional reports within 12 months.
- You only have to contact one of the three credit reporting agencies; your alert will automatically be sent to the other two.
- It will take longer to open a new credit account if you have a fraud alert on your report, so allow for extra time.
- There is no charge to place a fraud alert on your file.

Go over slide notes.

Slide notes:
Fraud alert: A fraud alert is a notation that's placed on your credit file to alert creditors that you may be a victim of identify theft and let them know that you should be contacted before credit is opened in your name. Under the Fair Credit Reporting Act, there are two types of fraud alert: an initial alert and an extended alert.

An initial fraud alert stays on your credit report for one year. This is appropriate if your wallet has been stolen or if you've been taken in by a "phishing" scam, or a company that you do business with notifies you that your personal information, such as your Social Security number, was compromised due to a security breach. With an initial fraud alert, potential creditors must use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. Once you place the fraud alert, each of the credit reporting agencies will mail you a notice of your rights as an identity theft victim. An initial alert on your credit report entitles you to one additional free credit report within 12 months from each of the three nationwide consumer reporting companies.

An extended fraud alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an ID theft affidavit, police report or similar documentation. With an extended fraud alert, potential creditors must actually contact you or meet with you in person before they issue you credit. When you place an extended alert on your credit report, you're entitled to two additional free credit reports within 12 months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for prescreened credit offers for five years unless you ask them to put your name back on the lists before then.

If you suspect your child's identity has been stolen, you should place a fraud alert with any credit reporting agency that has a file on your minor child. When adding a fraud alert to the report, be sure to ask for the free credit report that you are entitled to. (The one-year initial alert entitles you to one additional free credit report annually.)

Note:

• It may take longer to open a new credit account if you have a fraud alert on your report, so allow for extra time.

• You only have to contact one of the three credit reporting agencies; your alert request will automatically be sent to the other two.

• There is no charge to place a fraud alert on your file.

To understand the difference between a fraud alert and a credit freeze, read Consumer Action's explanation: www.consumer-action.org/helpdesk/articles/fraud_reports_security_freeze.

→SLIDE #25

Key points about freezing your credit:

- A security freeze makes your credit file off-limits. This usually means a credit request will be denied. It will also lock out insurance companies, landlords, employers who need to do a background check, cell phone companies, utilities, and others.

- You can lift the freeze before someone needs to access your credit report, or you can provide the PIN or password that the credit reporting agency gives you.
- A security freeze will not keep out anyone with whom you already have an account or other business relationship, and it will not prevent fraud involving your existing financial or credit accounts.

Go over slide notes.

Slide notes:
Credit freeze: A credit freeze will prevent ID thieves from opening up new accounts using your personal information because credit issuers will not be able to access your credit file. As of Sept. 21, 2018, freezing and unfreezing your reports is free in all states (there used to be a fee), and you can also get a free credit freeze for children under age 16 in all states. You must contact each of the three credit reporting agencies directly to place a credit freeze.

If you place a credit freeze, you will continue to have access to your free annual credit reports and you'll also be able to buy your credit reports and credit scores. Companies that you already do business with—for example, your mortgage, credit card or cell phone companies–-will still have access to your credit reports, as would collection agencies working for any of those companies. Companies will also still be able to send you prescreened credit offers (unsolicited credit offers you receive in the mail). And, according to the FTC, in some states, potential employers, insurance companies, landlords and other non-creditors can still access your credit report with a credit freeze in place.

If you're married, both you and your spouse must freeze your separate credit files to fully protect yourselves.

After processing your request, each agency will mail you a confirmation letter and a PIN or password that you will use whenever you temporarily lift the freeze and if you permanently remove it. In many states, you can choose to lift the freeze for a specific period of time or for a particular creditor or other credit report user. If you temporarily lift the freeze for a particular third party, you will provide a unique access code or a PIN to that person or business so that they can access your credit report.

For additional information about placing and lifting or removing a credit freeze, see Consumer Action's "Security Freeze" FAQs at www.consumer-action.org/modules/articles/security_freeze_training_manual_questions_and_answers.

→SLIDE #26

Key points about identity theft services:

- In most cases, a credit report monitoring service that charges a monthly or annual fee is not necessary.

Go over slide notes.

Slide notes: Identity theft protection services are a hot topic. But do these services work? Should consumers use them? The Consumer Federation of America (CFA) offers a list of nine questions consumers should ask before enrolling in one of these services:

1. Do the claims on the ID theft service's website or in advertisements make you think that the service will completely protect you against ID theft?

2. Does the service use scare tactics to try to get you to enroll?

3. Does the service make basic information about the company easy to find on its website?

4. If the service offers to monitor your personal information and alert you if someone may be fraudulently using it, is it clear what it monitors?

5. Does the service make clear how monitoring or other features of its program actually help you?

6. If the service offers to help ID theft victims, is it clear exactly what help it provides and who is eligible for it?

7. Is the cost of the service provided before you are asked for your payment info?

8. Does the service have a clear, transparent privacy policy?

9. If the service offers insurance or a guarantee, is it clear what it covers and who is eligible?

Find CFA's *Shopping for Identity Theft Services,* as well as tips on how you can protect your personal information and detect fraud, at https://idtheftinfo.org/shopping-for-id-theft-services.

Learn more about how to reduce the chances of becoming a victim and how to resolve ID theft problems from the FTC (https://www.consumer.ftc.gov/topics/identity-theft) and from Privacy Rights Clearinghouse (https://privacyrights.org/consumer-guides/identity-theft-what-do-if-it-happens-you).

→SLIDE #27

Key points about dealing with collection agencies:

- Never agree to pay for a debt that is the result of identity theft. Tell the collector you are a victim of ID theft and are not responsible for the account.
- Take detailed notes of all conversations with collectors and creditors, keep all letters you receive regarding the identity theft, and send letters by certified mail, return receipt requested.
- It is important to repair your credit report if there are unauthorized charges or accounts opened in your name.

Note: Contrary to what you might think, a new Social Security number may not be the answer to your problem. It may actually make things worse because you may not have any credit history at all. The Social Security Administration only assigns new numbers in limited cases.

Go over slide notes.

Slide notes:

Fix your credit reports: Since identity theft tends to start as a financial crime in most cases, the most important part of cleaning up the damage is fixing credit report errors or unauthorized charges and accounts opened in your name. The Fair and Accurate Credit Transactions Act entitles consumers to receive one free credit report per year from each of the three credit reporting agencies. Order a copy of your credit reports and look at both your personal and credit information for errors. (It has been reported that about 75 percent of credit reports contain at least one error, and that is without the work of an identity thief.) Once you've made a list of the errors, follow these steps for each one:

- **Write a letter of dispute**. Report each fraudulent account and each piece of erroneous information in writing to both the credit reporting agency (follow the dispute instructions provided with the credit report) and the credit issuer. Include a copy of your credit report, police report and FTC affidavit along with copies of supporting documents (keep the originals). Send your letter by certified mail, which gives you a tracking number (victims cleaning up after ID theft need to track everything).
- **Get organized.** Keep copies of all correspondence and notes about dates and content of conversations regarding the errors, and keep all information together.
- **Block errors**. The agencies are required to block disputed errors from future reports. Consumers should also instruct the credit reporting agencies to remove all inquiries that were generated due to the identity theft and notify those who received a copy of their report in the last six months of the disputed erroneous information.

Dealing with collection agencies: ID theft is often called the silent crime because most victims are not aware of the theft until contacted by a creditor or collection agency. If debt collectors try to get you to pay the bills on fraudulent accounts, ask for the name, address and telephone number of the collection agency, and the name of the person contacting you. Tell the collector you are a victim of ID theft and are not responsible for the account. Follow up with a letter to the collector via certified mail. Ask the agency for copies of documentation, such as credit applications, transaction receipts and statements associated with the fraudulent accounts. Amendments to the FCRA require that a debt collector who learns you may be the victim of identity theft must notify the original creditor about the fraud or identity theft and give you information about the debt. Amendments to the FCRA prevent businesses from reporting fraudulent accounts to the credit bureaus. Creditors will likely request that you complete a fraud affidavit (https://www.identitytheft.gov/). Learn more here: https://www.idtheftcenter.org/knowledge-base/collection-agencies-and-identity-theft-how-to-effectively-clear-identity-theft-accounts-from-collection-agency-records/.

Complaints: A consumer can file a complaint with the Consumer Financial Protection Bureau (CFPB) at 855-411-CFPB (TTY/TDD: 855-729-CFPB) or www.consumerfinance.gov/complaint if he or she has issues with: (1) incorrect information on a credit report; (2) a consumer reporting agency's investigation; (3) the improper use of a credit report; (4) being unable to get a copy of a credit score or file; and (5) credit monitoring or identity protection services. Consumer Action has created a booklet on "How to Complain" (https://www.consumer-action.org/english/articles/how_to_complain).

***ACTIVITY:* Savvy Consumer quiz *(*10 min)**

Ask participants to take the *Savvy Consumer* quiz from their folders.

Participants can break into small groups and work together to answer the questions, or can work individually. (If you are running short on time, you can assign just one question to each of five groups.) Ask for volunteers to answer the questions or rotate among the groups for responses, allowing the spokesperson from each group to provide the correct answer along with what the subject did right and wrong and what s/he should do next.

OPTIONAL ACTIVITY: Identity Theft Quiz (15 min)

The Identity Theft Quiz is an educational tool that can be used to complement and reinforce the ideas and concepts discussed in the ID Theft and Account Fraud training module. To use the game, download a PDF containing the instructions and rules, and a PowerPoint presentation containing the game slides, at www.consumer-action.org/outreach/articles/id_theft_quiz/.

IDENTITY THEFT RESOURCES (5 min)

Learning objective: Be aware of the various resources available for learning more about identity theft and account fraud.

Note: If you can project your computer screen, visit the sites and show participants where they can go to find valuable information.

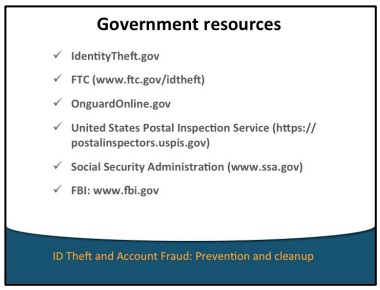
Key point (slides 28-29):

- There are many resources that provide free information about the potential liability and property risks and insurance options for sharing economy participants.

Questions to generate discussion:

- What websites do you visit for general consumer information? Why?

→SLIDE 28



Go over the list of resources.

→SLIDE 29

Go over the list of resources.

QUESTIONS AND ANSWERS (10 min)

Preparation: Review the brochure/guide and the backgrounder (Q&A). Open the floor to questions.

WRAP-UP AND EVALUATION (5 min)

→SLIDE #30

Thank participants for attending. Ask them to take a few minutes to fill out the evaluation form (page 47 of this lesson plan) that is in their folders and leave it in a large envelope you provide or face down on a table at the front or back of the room. If you will be conducting other trainings at a future time, announce that now.

ID Theft Prevention Checklist

Put a checkmark in the boxes next to the actions you have already taken to safeguard yourself from identity theft. Use the list as a guide for next steps to protect yourself from fraud, checking off each item as you complete it.

Review credit reports

☐ Ordered my credit reports (*www.annualcreditreport.com / 877-322-8228)*

☐ Reviewed my credit reports

☐ Disputed all questionable and inaccurate information with the credit reporting agency(ies)

☐ Placed an active duty alert in my credit files (servicemembers only)

Password all accounts

☐ Placed strong passwords on credit card, financial (checking/savings) and phone accounts

☐ Asked companies I do business with to not use my mother's maiden name as an identifier

Social Security number

☐ Memorized my Social Security number

☐ Ordered a new driver's license and/or checks without my Social Security number on them (if necessary)

Computer safety

☐ Bookmarked favorite sites (to avoid spoof sites)

☐ Password-protected my smartphone and set it to lock during inactivity

Miscellaneous

☐ Switched to a locking mailbox (or requested that landlord install one)

☐ Read privacy policies of the companies I do business with; changed my privacy settings/options where necessary

☐ Opted out of prescreened credit offers

If you are an identity theft victim:

☐ Filed a report with the police department and received a case number

☐ Filed reports with other appropriate agencies, such as the U.S. Postal Inspection Service, the Federal Trade Commission, the DMV, the Social Security Administration and my state's attorney general

☐ Downloaded and completed a free FTC ID Theft Affidavit (www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf)

☐ Put a fraud alert or security freeze on my credit report:

Equifax Security Freeze: 800-685-1111 / https://www.equifax.com/personal/credit-report-services/

Experian Security Freeze: 888-397-3742 / https://www.experian.com/freeze/center.html

TransUnion Security Freeze: 888-909-8872 / https://www.transunion.com/credit-freeze

Test Your Knowledge About ID Theft and Account Fraud

Take this quiz to see how much you know about identity theft and account fraud prevention and cleanup. Check "True" or "False" to answer the following statements.

1. You may not find out that you are a victim of identity theft until you review your credit or specialty consumer reports or a credit card statement and notice charges you didn't make.

○ True ○ False

2. Identity theft and identity fraud occur when an impostor uses your personal identification information to commit fraud or uses your credit card number to make unauthorized charges.

○ True ○ False

3. The National Consumer Telecom & Utilities Exchange determines if you are required to pay a deposit for telecommunication services and the amount of that deposit.

○ True ○ False

4. Fraudsters who use your identity to obtain medical care or services can introduce changes to your medical record that could pose a risk to you.

○ True ○ False

5 Typically, consumers are not held liable for fraudulent debts.

○ True ○ False

6. Under the FCRA and FACTA, you have a right to free reports from all nationwide credit and specialty agencies every 12 months.

○ True ○ False

7. You are entitled to a free copy of the credit report that was used in the decision to deny your credit application.

○ True ○ False

8. ChexSystems is a specialty consumer reporting agency that maintains a database of returned checks and instances of checking account fraud. It provides check authorization and verification to member retailers.

○ True ○ False

9. An employer must get your permission to conduct a background check on you, but if you are denied employment because of it, the employer is not required to show you the report or tell you how to get a copy of it.

○ True ○ False

10. Phishing is an attempt to “hook” you into revealing your personal and confidential information by sending emails that seem to come from a legitimate business.

○ True ○ False

11. To place an "active duty" alert, or to have it removed, servicemembers must call the fraud department of one of the three nationwide consumer reporting companies.

○ True ○ False

12. Suspicious accounts or incorrect information appearing in your credit file, calls from collection agencies, bills or account statements not arriving in the mail, and the inexplicable denial of credit applications are all signs that you may be a victim of identity theft.

○ True ○ False

13. An initial fraud alert is appropriate if your wallet has been stolen or you've been taken in by a "phishing" scam, or if a company that you do business with notifies you that your personal information was compromised due to a security breach.

○ True ○ False

14. An extended fraud alert stays on your credit report for five years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an identity theft affidavit.

○ True ○ False

15. A credit freeze will prevent ID thieves from opening up new accounts using your personal information because credit issuers will not be able to access your credit file.

○ True ○ False

Answer Key for the
Test Your Knowledge About
***ID Theft and Account Fraud* Quiz**

1. You may not find out that you are a victim of identity theft until you review your credit or specialty consumer reports or a credit card statement and notice charges you didn't make.

TRUE: Unfortunately, many consumers learn that their identity has been stolen only after some damage has been done—for example, when collection agencies contact them for overdue debts they never incurred; when they apply for a mortgage or car loan and learn that problems with their credit history are holding up the financing; or when they get something in the mail about an apartment they never rented, a house they never bought or a job they never held.

According to the FTC, the best way to find out sooner rather than later if you are a victim of identity theft is to monitor your accounts and bank statements each month and check your credit reports on a regular basis.

(See https://www.consumer.ftc.gov/topics/identity-theft.)

2. Identity theft and identity fraud occur when an impostor uses your personal identification information to commit fraud or uses your credit card number to make unauthorized charges.

TRUE: ID theft refers to the theft of another individual's personal information, such as name, Social Security number, birth date, mother's maiden name or other identifying information. Identity fraud is using that information for financial gain or some other purpose. Account fraud occurs when someone uses stolen information to make unauthorized charges or withdrawals on current accounts or open new accounts in the victim's name.

According to the FTC, identity theft is inherent in numerous types of fraud, including mortgage fraud and schemes directed at obtaining government benefits, including disaster relief funds. The IRS's Criminal Investigation Division, for example, has seen an increase in the use of stolen SSNs to file tax returns. In some cases, the thief files a fraudulent return seeking a refund before the taxpayer files. When the real taxpayer files, the IRS may not accept his/her return because it is considered a duplicate return. Even if the taxpayer ultimately is made whole, the government suffers the loss resulting from paying multiple refunds.

3. The National Consumer Telecom & Utilities Exchange determines if you are required to pay a deposit for telecommunication services and the amount of that deposit.

FALSE: According to information on the National Consumer Telecom & Utilities Exchange (NCTUE) website (www.nctue.com), the Exchange is a member-owned database housed and managed by Equifax, one of the three major credit reporting agencies. Membership is available to the nation's leading telecommunication and utility companies.

NCTUE's stated objectives are:

- Early identification of higher-risk accounts for new residential service applicants
- Locating former customers whose service was terminated with an unpaid balance

- Identification and implementation of additional uses of the data to benefit members

Although the NCTUE shares information on new connects and defaulted and/or fraudulent accounts among its members, the company emphasizes that the decision to assess a deposit, and the amount of that deposit, is left up to each individual member.

4. Fraudsters who use your identity to obtain medical care or services can introduce changes to your medical record that could pose a risk to you.

TRUE: The FTC warns that every time a thief uses your identity to get medical care, a record is created with the impostor's medical information that could be mistaken for *your* medical information—say, a different blood type, an inaccurate history of drug or alcohol abuse, test results that aren't yours, or a diagnosis of an illness, allergy or condition you don't have. Any of these could lead to improper treatment, which, in turn, could lead to injury, illness or worse. Victims of medical identity theft not only may have their health endangered by inaccurate entries in their medical records, they may also have their insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs. Victims may not even be aware that the fraud has occurred because medical identity theft can be difficult to discover, as few consumers regularly review their medical records. They might only find out when they receive collection notices or they attempt to seek medical care themselves and discover that they have reached their medical insurance coverage limits.

(See www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt10.shtm and www.idtheft.gov/reports/StrategicPlan.pdf.)

5. Typically, consumers are not held liable for fraudulent debts.

TRUE: Under various laws, your liability for fraudulent debts caused by identity theft is limited. The FTC offers the following summary:

- **Fraudulent credit card charges:** You cannot be held liable for more than $50 for fraudulent purchases made with your credit card, as long as you let the credit card company know within 60 days of when the credit card statement with the fraudulent charges was sent to you. Some credit card issuers say cardholders who are victims of fraudulent transactions on their accounts have no liability for them at all (referred to as a "zero liability" policy).
- **Lost or stolen ATM/debit card:** If your ATM or debit card is lost or stolen, you won't be held liable for more than $50 as long as you notify the bank or credit union within two business days of realizing the card is missing. If the card *isn't* missing, you've got 60 days to report fraudulent use of your account number. If you do not report the loss of your card promptly, your liability increases to $500 (up to 60 days), or unlimited (it takes you more than 60 days to report it).
- **Fraudulent electronic withdrawals:** If fraudulent electronic withdrawals are made from your bank or credit union account, and your ATM or debit card has not been lost or stolen, you are not liable as long as you notify the bank or credit union in writing of the error within 60 days of the date the bank or credit union account statement with the fraudulent withdrawals was sent to you.
- **Fraudulent checks:** Under most state laws, you are liable for just a limited amount for fraudulent checks issued on your bank or credit union account, as long as you notify the bank or credit union promptly. Contact your state banking or consumer protection agency for more information.

- **Fraudulent new accounts**: Under most state laws, you are not liable for any debt incurred on fraudulent accounts opened in your name and without your permission. Contact your state attorney general's office (www.naag.org/current-attorneys-general.php) for more information.

In cases where a thief commits a more serious crime, such as driving under the influence while using your identity, you may be detained by police and spend time and effort trying to clear up the situation. While, ultimately, you probably will not be held responsible for the crime, the cost in time and money to clear your name can be considerable. For instance, you could be turned down for a job or anything else that requires a background check while false information remains on your record.

(See https://www.idtheftcenter.org/knowledge-base/clearing-criminal-identity-theft/.)

6. Under the FCRA and FACTA, you have a right to free reports from all nationwide credit and specialty agencies every 12 months.

TRUE: Under the FCRA and FACTA, nationwide credit and specialty consumer reporting agencies—those companies that compile reports on consumers for targeted uses, other than credit—must provide a free report to consumers every 12 months, upon the consumer's request.

The types of reports that specialty consumer reporting agencies compile include:

- Medical conditions (for example, the Medical Information Bureau (MIB))
- Residential or tenant history and evictions (for example, the RentBureau)
- Check writing history (for example, ChexSystems)
- Employment background checks (for example, LexisNexis Screening Solutions)
- Homeowner and auto insurance claims (for example, CLUE reports)

(See https://www.consumer-action.org/news/articles/specialty_credit_report_issue_fall_2014.)

7. You are entitled to a free copy of the credit report that was used in the decision to deny your credit application.

TRUE: The law entitles you to a free report if a company takes adverse action against you, such as denying your application for credit, insurance or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address and phone number of the credit reporting company. You're also entitled to an additional free report per year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft. Otherwise, a consumer reporting company may charge you a nominal fee for another copy of your report (beyond your one free annual report) within a 12-month period.

(See www.ftc.gov/bcp/edu/pubs/consumer/credit/cre34.shtm.)

8. ChexSystems is a specialty consumer reporting agency that maintains a database of returned checks and instances of checking account fraud. It provides check authorization and verification to member retailers.

FALSE: There are three major specialty reporting companies that report on checking account activity/history: ChexSystems, Shared Check Authorization Network (SCAN) and TeleCheck. If a bank closes your checking account because of insufficient funds, it will make a report to ChexSystems that other banks will check when you apply for new accounts. It is Shared Check Authorization Network (SCAN) and TeleCheck that maintain a database of returned checks and instances of fraud. These two also provide check authorization and verification to member retailers.

(See https://www.consumer-action.org/news/articles/specialty_credit_report_issue_fall_2014.)

9. An employer must get your permission to conduct a background check on you, but if you are denied employment because of it, the employer is not required to show you the report or tell you how to get a copy of it.

FALSE: The Federal Credit Reporting Act (FCRA) provides that an employer must give you notice that a background screening may be conducted, and the employer must get your permission to conduct the screening. Notice and permission must be given on a separate document, not buried in an application or other form.

The national standard, set by the FCRA, does not require an employer to tell you the name of the screening company or tell you how to get a copy of your report. But the employer must give you a copy of the report if he or she decides not to hire you or denies you a promotion based on it.

(See https://www.privacyrights.org/consumer-guides/employment-background-checks-jobseekers-guide.)

10. Phishing is an attempt to "hook" you into revealing your personal and confidential information by sending emails that seem to come from a legitimate business.

TRUE: The FTC explains that **"**phishers" send an email or pop-up message that claims to be from a business or organization that you may deal with—for example, an internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to "update," "validate" or "confirm" your account information. Some phishing emails threaten a dire consequence if you don't respond. The messages direct you to a website that looks just like a legitimate organization's site, but it isn't. It's a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The FTC suggests these tips to help you avoid getting hooked by a phishing scam:

- **If you get an email or pop-up message that asks for personal or financial information, do not reply.** And don't click on the link in the message, either. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new internet browser session and type in the company's correct web address yourself. In any case, don't cut and paste the link from the message into your internet browser—phishers can make links look like they go to one place, but actually send you to a different site.

- **Area codes can mislead.** Some scammers send an email that appears to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." Because they use Voice over Internet Protocol (VoIP) technology, the area code you call does not reflect where the scammers really are. If you need to reach an organization you do business with, call the number on the statements they send you, on the back of your credit card, etc. In any case, delete random emails that ask you to confirm or divulge your financial information.
- **Use antispyware and antivirus software, as well as a firewall, and update them regularly.** Some phishing emails contain software that can harm your computer or track your activities on the internet without your knowledge. Antivirus software and a firewall can protect you from inadvertently accepting such unwanted files. Antivirus software scans incoming communications for troublesome files. Look for antivirus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically. A firewall helps make you invisible on the internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Firefox) also may offer free software "patches" to close holes in the system that hackers or phishers could exploit.
- **Don't email personal or financial information.** Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a padlock icon in the browser's status bar or a URL that begins with "https:" instead of just "http:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- **Review credit card and bank account statements as soon as you receive them** to check for unauthorized charges**.** If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- **Be cautious about opening any attachment or downloading any files from emails** you receive regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.
- **Forward spam that is phishing for information** to spam@uce.gov and to the company, bank or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

If you believe you've been scammed, file a complaint with the FTC at https://www.ftccomplaintassistant.gov.

(See www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm.)

11. To place an "active duty" alert, or to have it removed, servicemembers must call the fraud department of one of the three nationwide consumer reporting companies.

TRUE: If you are a member of the military and away from your usual duty station, you may place an "active duty" alert on your credit report to help minimize the risk of identity theft while you are deployed. When a business sees the alert on your credit report, it must verify your identity before issuing credit in your name. The business may try to contact you directly, but if you're on deployment, that may be impossible. As a result, the law allows you to use a personal representative to place or remove an alert. Active duty alerts on your report are effective for one

year, unless you request that the alert be removed sooner. If your deployment lasts longer, you may place another alert on your report.

To place an active duty alert, or to have it removed, call the toll-free fraud number of one of the three nationwide consumer reporting companies: Equifax, Experian or TransUnion. The company will require you to provide proof of your identity, which may include your Social Security number, your name, address and other personal information.

- Equifax: 800-685-1111; https://www.equifax.com/personal/credit-report-services/
- Experian: 888-EXPERIAN (397-3742); https://www.experian.com/help/
- TransUnion: 888-909-8872; https://www.transunion.com/credit-help

Contact only one of the three companies to place an alert—the company you call is required to contact the other two, which will place an alert on their versions of your report, as well. If your contact information changes before your alert expires, remember to update it.

Beginning in late 2019, credit reporting agencies must offer free electronic credit monitoring to all active duty servicemembers.

When you place an active duty alert, your name will be removed from the nationwide consumer reporting companies' marketing lists for prescreened offers of credit and insurance for two years, unless you ask that your name be placed back on the lists before then. Prescreened offers—sometimes called "preapproved" offers—are based on information in your credit report that indicates you meet certain criteria.

(See www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt147.shtm.)

12. Suspicious accounts or incorrect information appearing in your credit file, calls from collection agencies, bills or account statements not arriving in the mail, and the inexplicable denial of credit applications are all signs that you may be a victim of identity theft.

TRUE: Identity theft can go undetected for many months—but there typically are signs of the fraud. Some of these signs include:

- Missing credit card and loan statements, which may indicate that a thief has stolen them from your mailbox or changed your mailing address with your creditors
- Unauthorized purchases on your credit cards
- Cards and bills for accounts you didn't open, or rejection letters for credit you didn't apply for
- Calls or letters from collectors about bills you don't recognize
- Being denied such things as credit, a job, insurance or a home rental for no obvious reason

Read your account statements promptly and carefully and check your credit report every year—some experts recommend twice a year—even if you haven't seen anything to indicate you are a victim of identity theft. Look for any suspicious activity, such as accounts, loans and inquiries you don't recognize.

13. An initial fraud alert is appropriate if your wallet has been stolen or you've been taken in by a "phishing" scam, or if a company that you do business with notifies you that your

personal information was compromised due to a security breach.

TRUE: A fraud alert is a notation on your credit report that requires the three major credit-reporting agencies (Equifax, Experian and TransUnion) to alert you when someone applies for credit in your name. These alerts also are intended to prompt creditors to verify your identity before issuing credit in your name, although they are not compelled by law to do so.

Any consumer can request an "initial" fraud alert, which stays on your report for one year. This might be appropriate if you have reason to believe you might become a victim of identity theft. For example, you might want to place a fraud alert if you lost your wallet or inadvertently gave information to someone you believe may be a scam artist. You can renew the alert after the year is up.

(See https://www.nolo.com/legal-updates/new-law-extends-initial-fraud-alerts-to-one-year.html.)

14. An extended fraud alert stays on your credit report for five years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an identity theft affidavit.

FALSE: An extended fraud alert stays on your credit report for seven years (not five). You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an Identity Theft Report. An Identity Theft Affidavit, available at the FTC's IdentityTheft.gov (https://www.identitytheft.gov/) website should be sufficient to obtain an extended fraud alert. With an extended fraud alert, potential creditors must actually contact you or meet with you in person before they issue credit in your name. When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for prescreened credit offers for five years unless you ask them to put your name back on the list before then.

To place an extended alert on your credit report, or to have it removed, you will be required to provide appropriate proof of your identity, which may include your Social Security number, name, address and other personal information requested by the consumer reporting company.

15. A credit freeze will prevent ID thieves from opening up new accounts using your personal information because credit issuers will not be able to access your credit file.

TRUE: A credit security freeze is a much more stringent measure of protection than a fraud alert. Rather than simply alerting you when someone applies for credit in your name, a freeze actually prevents anyone from accessing your credit file until you take steps to give permission by "lifting" the freeze. Companies that can't check your credit report usually won't approve an application for credit, phone service, insurance, housing or employment until you authorize the credit bureau to release your information.

(See Consumer Action's "Freeze Your Credit File" [https://www.consumer-action.org/modules/articles/freeze_your_credit_file] and "Security Freeze Backgrounder" [www.consumer-action.org/modules/articles/security_freeze_training_manual_questions_and_answers].)

Savvy Consumer Quiz

Decide whether the consumer in each scenario is savvy (well informed) or not. Be prepared to answer these questions in a class discussion:

- *What did the consumer do right?*
- *What did the consumer do wrong?*
- *What should the consumer do next?*

1. Erica's bank calls. They would like to send her a new credit card and they need to verify some information. Since she was thinking about opening up a new credit card anyway, Erica gives them her Social Security number and birth date.

Erica is: ☐ savvy ☐ not savvy

2. Jason can't find his wallet, which contains nine credit cards, an ATM card and his Social Security card. He contacts the store where he made his last purchase, but it does not have his wallet. He contacts the card companies and his bank to report the loss.

Jason is: ☐ savvy ☐ not savvy

3. Peter and Linda have a joint credit card account. Peter wants to avoid additional interest and late fees by paying the balance in full each month. He notices that the balance is more than usual, but he pays the full amount without questioning the charges because he assumes Linda made them.

Peter is: ☐ savvy ☐ not savvy

4. Laura has excellent credit. She has two bank credit cards and always pays her bills on time. She applies for instant credit at a major department store to get an additional discount on her purchase, but the clerk tells her that her application was denied. She requests her free annual credit reports at www.annualcreditreport.com to see if she is a victim of identity theft.

Laura is: ☐ savvy ☐ not savvy

5. Andrew is in the military and must obtain a security clearance. Andrew's security clearance is denied because of bad credit—he is advised to check his credit report. When he gets his report, he notices four overdue credit card accounts that he did not open. He calls the credit card companies that issued the accounts and asks to have them closed. He also puts a fraud alert on his account and contacts his superior officer to inform her that he is a victim of fraud.

Andrew is: ☐ savvy ☐ not savvy

Savvy Consumer Quiz Answer Key

1. Erica is **not savvy**. She should never give her personal information over the phone to someone who calls her. Instead, Erica could ask for the caller's number and then hang up and call her financial institution at the phone number on her account statement or on the back of her credit or debit card. If they confirm that the call was not legitimate, Erica should report the number and the suspicious call to the bank's fraud department.

2. Jason is **not savvy**. He should never carry his Social Security card in his wallet. And he should put only the credit cards he needs in his wallet—not all nine of his cards at once.

3. Peter is **not savvy**. He should always go over the credit card statement with Linda to make sure the charges are valid. Otherwise he might pay for unauthorized charges, which he could easily have removed. If he waits more than 60 days from the statement date to dispute unauthorized charges, he may have to pay the whole amount.

4. Laura **is savvy**. Obtaining a credit report is a good way to check if someone else is opening up accounts using her personal information.

5. Andrew **is savvy in some ways**—he checked his credit report and added a fraud alert to stop further damages. He also contacted the credit card companies immediately to close the fraudulent accounts. But he might have been able to stop the fraud—and the credit damage—sooner if he had obtained his free credit reports regularly. And, if he's on active duty, he should consider placing an "active duty alert" (rather than a standard one), which would allow him to name a personal representative to manage the alert and would entitle him (as of late 2019) to free electronic credit monitoring.

Notification of death (to credit reporting agencies)

Equifax	Experian	TransUnion
P.O. Box 105139	PO Box 4500	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016

Date: _____

To: _____

I am writing to request that the credit file for _____ be flagged as "deceased."

His/her most recent address was: _____.
His/her Social Security number is _____ and birthdate is___/___/___.

Enclosed please find one copy of the decedent's death certificate. Also enclosed is a copy of a document confirming my authority as the decedent's executor/surviving spouse.

If you have any questions, you may contact me by telephone at _____or by email at _____.

Thank you.
[Your signature]
[Your name printed]

Instructions:
Fill in blanks with your information. Send by certified mail, return receipt requested, to each of the three credit bureaus. Along with this letter, include the required documentation (for example: a copy of the death certificate, a copy of the decedent's identification, a copy of your driver's license or other government-issued photo identification, and proof of executorship or marriage). Visit each credit bureau online to find out exact requirements.

To ensure the death is reported promptly to the Social Security Administration, a family member can call the SSA at 800-772-1213 (TTY: 800-325-0778) Mon-Fri from 7:00 a.m. to 7:00 p.m.

Letter notifying existing creditors of identity theft

Date: _____

[Your name]
[Your address]
[City, State, ZIP]

[Your account number]

[Name of creditor]
Attn: Billing Inquiries
[Creditor address]
[City, State, ZIP]

Dear Sir or Madam:

I am writing to dispute a fraudulent transaction on my account in the amount of $_____ on [date] _____. I am a victim of identity theft, and I did not make this transaction. I am requesting that the [charge be removed/the debit refunded], that any finance or other charges that have been assessed as a result of the fraudulent transaction be credited back to my account, and that I receive an updated statement.

Enclosed is a copy of my ID Theft Affidavit explaining the circumstances of the crime.
Please investigate this matter and update my account as soon as possible. You may send any correspondence to the address above.

Thank you.
[Your signature]
[Your name printed]

Instructions:
Fill in blanks with your information. Send by certified mail, return receipt requested, to each creditor where a fraudulent transaction has been processed on your account. Along with this letter, include a copy of your ID Theft Affidavit and police report. If no fraudulent transactions appear on the account, you can modify the letter to serve as simply a notification to the creditor that you are an ID theft victim and that your account may be at risk. The creditor will advise what next steps to take.

Letter requesting records related to fraudulent transaction

Date: _____

[Your name]
[Your address]
[City, State, ZIP]

[Account number or name]

[Name of creditor]
Attn: Billing Inquiries
[Creditor address]
[City, State, ZIP]

Dear Sir or Madam:

As we discussed on the phone on [date] _____, I am a victim of identity theft. The thief made a fraudulent transaction or opened a fraudulent account with your company using my identity. Pursuant to federal law, I am requesting that you provide me, at no charge, copies of applications and other records in your control relating to the fraudulent transaction.

Pursuant to the law, I am providing you with the following documentation, so that you can verify my identity: a copy of my government-issued identification; a copy of the police report; and a copy of my ID Theft Affidavit (form provided by the FTC).

Please provide all information relating to the fraudulent transaction, including: applications, statements, transaction slips, mailing addresses and phone numbers of applicant, investigator's summary, and any other documentation related to the account.

Please send the information to me at the above address and to the officer who is investigating my case: [insert officer's name, address and telephone number].

Thank you.
[Your signature]
[Your name printed]

Instructions:
Fill in blanks with your information. Send by certified mail, return receipt requested, to each company where an account was opened or a transaction was made using your identity. Along with this letter, include a copy of your ID Theft Affidavit and police report. Follow up in 10 days to confirm receipt of the letter and an estimate of when the documentation will be sent to you.

Training evaluation: ***ID Theft and Account Fraud: Prevention and cleanup***

Please help us improve future presentations by giving us your opinion of today's class. Circle the response that best reflects your feelings about each statement.

1. I have a better understanding of what ID theft and account fraud are.

Strongly Agree Agree Disagree Strongly Disagree

2. I know what steps I can take to avoid becoming an identity theft victim.

Strongly Agree Agree Disagree Strongly Disagree

3. I feel confident that I could recognize and avoid a scam.

Strongly Agree Agree Disagree Strongly Disagree

4. I have a better understanding of what I should do if I become an identity theft victim.

Strongly Agree Agree Disagree Strongly Disagree

5. I know where to go for more information and assistance on this subject.

Strongly agree Agree Disagree Strongly disagree

6. The instructor was well informed.

Strongly Agree Agree Disagree Strongly Disagree

7. The materials I received are easy to read and understand.

Strongly Agree Agree Disagree Strongly Disagree

8. I would like to attend another class like this.

Strongly Agree Agree Disagree Strongly Disagree

On a scale of 1 to 10 (10 being the highest), how would you rate the seminar? _____

Please let us know how we could improve future trainings (use back, if necessary):

_____

_____

_____

_____

Thank you for attending!