MONEY SMART

MONEY SMART FOR YOUNG ADULTS

MODULE 9

Protecting Your Money and Your Identity

Instructor Guide

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

FDIC-026-2022

The Federal Deposit Insurance Corporation is an independent agency created by Congress to maintain stability and public confidence in the nation's financial system. One way we do that is by providing free, nonbiased financial education materials, including this instructor guide. For more information about our family of Money Smart products, visit **fdic.gov/moneysmart**.

Contents

Welcome

Welcome to the FDIC's Money Smart for Young Adults!

This is the instructor guide for **Module 9: Protecting Your Money and Your Identity**.

Module Purpose

This module helps participants protect their money and prevent identify theft. Participants will be able to:

- Identify risks to assets
- Identify ways to reduce risks to assets
- List warning signs of identity theft and financial fraud
- Use strategies to prevent identity theft and financial fraud
- Report identity theft and get help
- Explain how insurance works
- Identify types of insurance and when they are needed
- Explain the role of recordkeeping for making sure insurance covers risks

Module at a Glance

We estimate that you will need 2 hours to cover the entire module, not including breaks. You can train on all sections or select sections based on the time you have available and the needs of participants.

SECTION	SUBSECTIONS AND ACTIVITIES	ESTIMATED TIME (MINUTES)
Module Opening	■ Welcome Participants as They Arrive ■ Pre-Training Survey (optional) ■ Parking Lot and Participant Guide	**10**
Section 1: Risks to Your Assets	■ Assets and Risks ■ Try It: Spotting Risks to Assets ■ Reducing Risks to Your Assets ■ Apply It: Risks to My Assets	**20**
Section 2: Identify Theft and Fraud	■ Identity Theft Basics ■ Warning Signs of Identity Theft ■ Try It: Spotting Warning Signs of Identity Theft ■ Steps to Minimize Identity Theft ■ Apply It: My Action Plan to Reduce Risks of Identity Theft ■ Reporting Identity Theft and Getting Help	**70**
Section 3: Insurance and Recordkeeping	■ How Insurance Works ■ Types of Insurance ■ Getting Insurance ■ Apply It: Insurance—Do I Have It? Do I Need It? ■ Keeping Accurate Records	**20**
Module Closing	■ Remember the Key Takeaways ■ Take Action ■ Post-Training Survey (optional)	**10**

The FDIC created Real-Life Money Situations for Young Adults to strengthen the financial knowledge, skills, and self-efficacy of young adults ages 16 to 24. The five scenarios can be used with the Money Smart for Young Adults financial education curriculum, with other financial education curricula, or as stand-alone activities. Each scenario features a young adult facing realistic financial decisions. Young adults reflect on the scenarios and consider how they might respond in similar situations. The scenario titled Reggie Takes a Trip with Friends features financial decisions that relate to the content of this module. Search fdic.gov for Real-Life Money Situations for Young Adults.

Module Opening

Time estimate for this section: 10 minutes

Welcome Participants as They Arrive

SHOW SLIDE 1

DO

- As participants arrive for the training, use this time to:
  - Welcome them and introduce yourself
  - Ask them to sign in for the training if you are using a sign-in sheet
  - Ensure that any requested reasonable accommodations are in place and make any necessary adjustments

Pre-Training Survey (Optional)

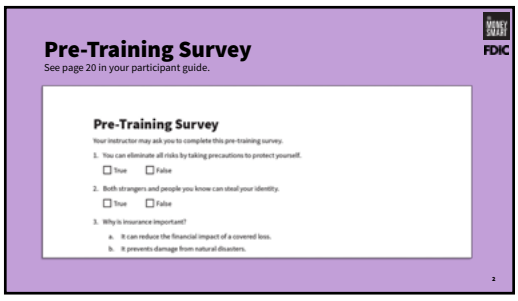
See page 20 in the participant guide.

Note to Instructor: Before training starts, you can ask participants to complete the pre-training survey in the back of the participant guide. Give participants copies of the survey so they do not have to tear pages out of their guides. The questions are repeated in the post-training survey.

The answer key is at the end of this instructor guide, but do not share the answers now.

Using the pre- and post-training surveys allow you to estimate knowledge gains and get other feedback on the training. You may decide to compare pre-training surveys to post-training surveys to estimate knowledge gains of the entire group or for individual participants. To estimate by participant, ask them to write their name or some other unique identifier on both their pre- and their post-training surveys.

SHOW SLIDE 2



SAY

- Thank you for coming to this Money Smart training on "Protecting Your Money and Your Identity."
- Please complete the pre-training survey on page 20 of your participant guide.
- It should take less than five minutes to complete.

DO

- Collect the completed surveys.

Parking Lot and Participant Guide

SAY

- I will use a parking lot to capture questions, ideas, and other thoughts. We can add items anytime during the training. Time permitting, I will address them during breaks or at the end of training.
- You have a participant guide. You can write in it. It is yours to keep.

Section 1: Risks to Your Assets

Time estimate for this section: 20 minutes

See page 2 in the participant guide.

Participants will be able to:

- Identify risks to assets
- Identify ways to reduce risks to assets

SHOW SLIDE 3

SAY

- We will discuss how to identify risks to your assets and ways you can reduce those risks.

SHOW SLIDE 4

SAY

- The key takeaway for this section is: Being aware of risks to your assets prepares you to take steps to reduce those risks.

Assets and Risks

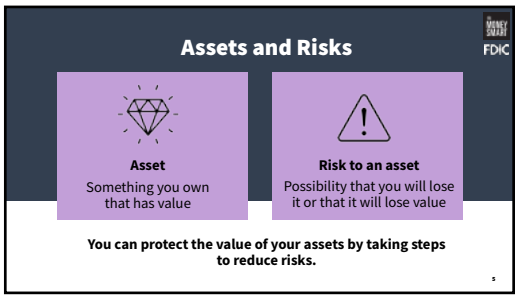
Lead discussion (7 minutes)

See page 2 in the participant guide.

SHOW SLIDE 5

SAY

- Something you have that has value is called an asset.
  - Examples are a lawn mower and a gift card
- Risk to an asset is the possibility that you will lose it or that it will lose value.
  - A lawn mower could break down.
  - A gift card could get lost or stolen.
- You can protect the value of your assets by taking steps to reduce risks.
  - You could properly maintain a lawn mower to keep it working longer.
  - You could find a place for a gift card where it will unlikely be lost or stolen.



Try It: Spotting Risks to Assets

Lead activity (10 minutes)—Brainstorm

See page 3 in the participant guide.

SHOW SLIDE 6

DO

- Break the participants into groups.
- Assign each group one of four topics. If you have more than four groups, assign the same topic to more than one group. The topics are:
  - Cash
  - Home
  - Car
  - Job

SAY

- Turn to "Try It: Spotting Risks to Assets" on page 3 in your participant guide.
- Let's look at some common types of assets and risks to those assets.
- Take three minutes to brainstorm risks associated with the asset I assigned to your group: What could happen that would make the value of these assets go down, or cause a loss?
- For example: Cash can be stolen.

DO

- After three minutes, ask each group to share the results of their brainstorming.
- Write responses on a flip chart or whiteboard.
- Add the following possibilities if not contributed:
  - Cash
    - » Loss.
    - » Theft
    - » Destroyed in a fire.
  - Home
    - » Damage from a water leak.
    - » Damage from a natural disaster.
    - » Downturn in the housing market.

- Car
  - » Mechanical breakdown requiring costly repairs.
  - » Damage from an accident.
  - » Theft.
  - » Repossession, if the loan becomes delinquent.
- Job
  - » Unable to work because of an injury or illness.
  - » Laid off or hours reduced.
  - » Fired.
  - » Shutdown from a disaster.

Reducing Risks to Your Assets

Present information (2 minutes)

See page 2 in the participant guide.

SHOW SLIDE 7

SAY

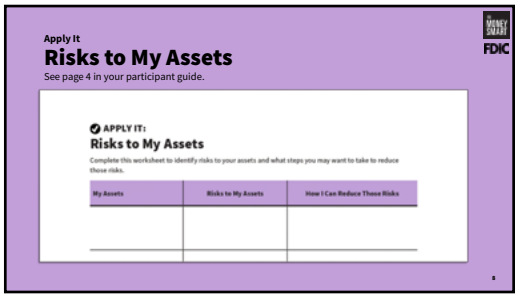
- You cannot eliminate all risks, but you can reduce many.
- **Make informed choices that anticipate risks.** If you are aware of risks, you can anticipate them. For example, if you are aware of the risk of cash getting lost or stolen, you might choose to deposit some or all of the money at a federally insured financial institution.
- **Be careful with personal information.** Being careful how and where you store and share your personal and financial information can reduce the risks of identity theft, potential loss of assets, and possible damage to your credit history.
- **Know your rights and responsibilities.** Understand how and when laws protect consumers and know what to do if rights are violated.
- **Get insurance.** Insurance can reduce the financial impact of a covered loss. For example, car insurance can help pay for repairs to your car due to an accident.

Apply It: Risks to My Assets

Present information (1 minute)

See page 4 in the participant guide.

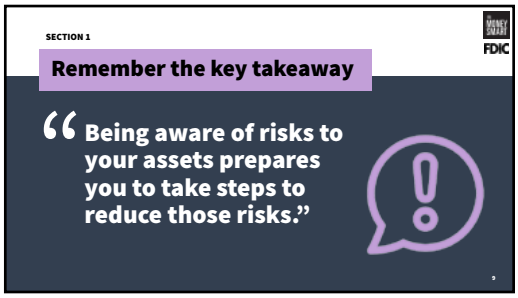
SHOW SLIDE 8



SAY

- You can complete this table after today's training to identify risks to your assets and how to reduce those risks.

SHOW SLIDE 9



SAY

- Remember the key takeaway: Being aware of risks to your assets prepares you to take steps to reduce those risks.

Section 2: Identity Theft and Fraud

Time estimate for this section: 70 minutes

See page 5 in the participant guide.

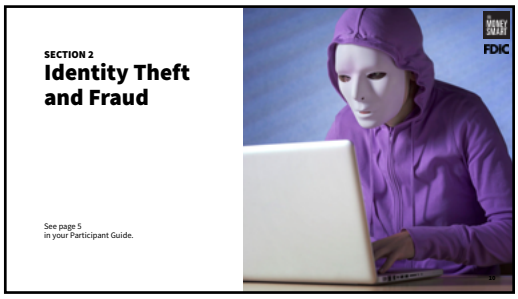
Participants will be able to:

- Recognize warning signs of identity theft and financial fraud
- Use strategies to prevent identity theft and financial fraud
- Report identity theft and get help

SHOW SLIDE 10

SAY

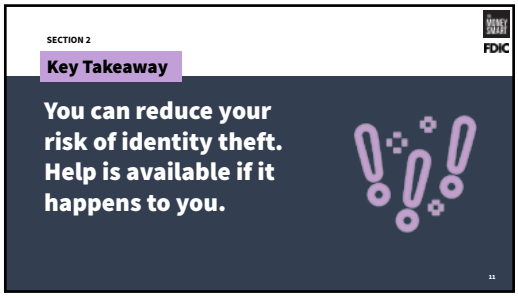
- We will discuss identity theft and fraud, steps you can take to reduce the risks of identity theft and fraud, and what to do if it happens to you.



SHOW SLIDE 11

SAY

- The key takeaway for this section is: You can reduce your risk of identity theft. Help is available if it happens to you.



Identity Theft Basics

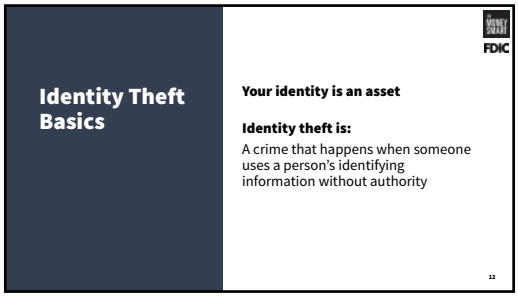
Lead discussion (15 minutes)

See page 5 in the participant guide.

SHOW SLIDE 12

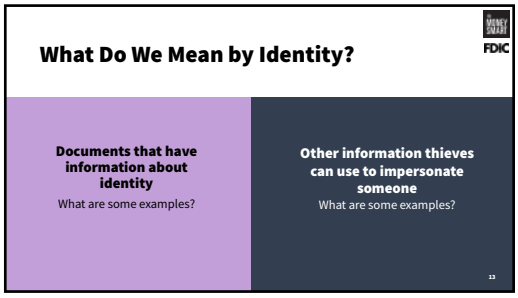
SAY

- Your identity, personal information about who you are, is an asset. For example, your name, Social Security number, and personal financial information can help you get a job, be approved for a loan, rent an apartment, and open a bank account.
- There are risks to your identity, and a major one is identity theft.



- Identity theft is a crime that happens when someone uses a person's identifying information without authority.
- For example, someone might open credit cards in your name.
- Your identity can be stolen by family, friends, or strangers.

SHOW SLIDE 13



SAY

- What do we mean by "identity" when we talk about identity theft?
- Many different pieces of information make up your identity.
- Your identity includes information in documents that can verify who you are.
- You can take notes on page 6 in your participant guide as we go over some examples of where information about your identity is found.

ASK

- What are examples of documents with information about identity?

DO

- Write participant responses on a flip chart or whiteboard.
- Add the following if not contributed:
  - Social Security card or number
  - Student ID
  - Medicare or other health identification card
  - Birth certificate
  - Driver's license card or number
  - State ID card
  - Passport
  - Individual Taxpayer Identification Number (ITIN)
  - Native American Tribal document
  - Consular Identification Card, such as the Matrícula Consular de Alta Seguridad (MCAS)
    - » A Consular Identification Card is an ID issued by a foreign government through an office called a consulate that is located in the United States

SAY

- There are also other pieces of information that can be used by thieves to impersonate you.

ASK

- What other pieces of information can thieves use to impersonate someone?

DO

- Write participant responses on a flip chart or whiteboard.
- Add the following if not contributed:
  - Financial account numbers, such as credit card numbers and bank account numbers
  - Insurance policy information
  - Information from prior tax returns
  - History of where you have lived and when
  - Utility account numbers
  - Usernames and passwords for online accounts
  - Answers to common security "challenge questions" used to control access to accounts, such as your mother's maiden name, the name of the street you grew up on, or the name of a school you attended
  - Your medical information, such as your doctor's name, or a medical record number
  - Bills
  - Bank statements
  - Checks
  - Credit card offers, even those that come in the mail that you did not apply for

ASK

- How could you be harmed if someone got that information?

DO

- Write participant responses on a flip chart or whiteboard.
- Add the following if not contributed:
- The person committing identity theft could:
  - Open up accounts in your name at financial institutions, including credit accounts. The person committing identity theft could then borrow money or buy things and leave you with the debt.
  - Access your financial accounts and steal your money or leave you with debt.
  - File a false tax return in your name, stealing your refund and reporting inaccurate information you will need to clear up.
  - Use your identity to obtain prescriptions or medical treatments. This may result in medical providers billing you for services you did not receive.
- Your health plan rejecting your legitimate medical claim because the records show you have reached your benefits limit.
- Other issues with your insurance coverage because your medical records show a condition you do not have.
- Medical mistakes if someone else's medical information is connected to your name or identity.

SHOW SLIDE 14

SAY

- Criminals continue to become more skilled with identity theft. For example:
  - **Phishing** is when criminals attempt to trick you into giving them personal information, often through email.
    - » A criminal sends a fake email that appears to be from a legitimate source, such as your bank, utility company, well-known merchant, your internet service provider, or even a trusted government agency (for example, the FDIC).
    - » These emails often look very legitimate, but they are not.
    - » They ask you to provide sensitive personal information the criminal can use to steal your identity.
    - » Phishing through the phone is called vishing (voice phishing).
    - » Phishing through text messages is called smishing (SMS text phishing).
  - **Spear phishing** is a targeted form of phishing in which criminals try to trick groups of people with something in common.
    - » For example, a spear phishing scheme might target people who work at the same company, have accounts at the same financial institution, attend the same school, or shop online at the same website.
    - » The spear phishing emails look like they were sent from organizations that people are familiar with and trust. In reality, they are from criminals who are trying to get personal information.
  - **Pharming** is when criminals seek to obtain personal or private information by making fake websites appear legitimate.
  - **Skimming** is when criminals steal your credit or debit card number by using a special storage device they hide in automated teller machines (ATMs) and point of service machines (where you swipe your card at places of business, such as gas stations). You swipe your card, they get your number, and they use it to buy things.
  - **Social media scamming** is when criminals trick people into giving them personal information on social media sites, chat rooms, bulletin boards, mobile apps, photo sharing sites, and similar places. These scams sometimes start with a sales pitch about an investment from a person you do not know.
- These are just a few of the ways a criminal can access your information.

Warning Signs of Identity Theft

Present information (5 minutes)

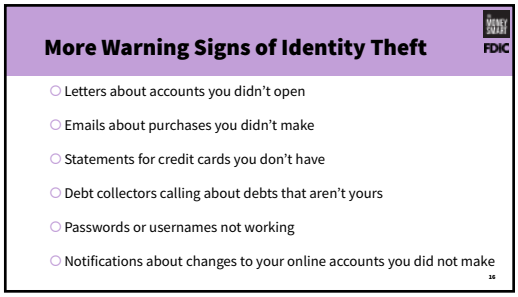
See page 6 in the participant guide.

SHOW SLIDE 15

SAY

- Watch out for early warning signs that your identity has been or may have been stolen.
  - You see withdrawals from your bank account you did not make.
  - You do not receive your bills, account statements, or other mail when expected.
  - Merchants refuse your checks.
  - Your credit card transactions do not go through.

SHOW SLIDE 16



SAY

- Also watch out for these warning signs:
  - You receive letters thanking you for opening an account you did not open.
  - You receive emails about purchases you did not make.
  - You receive credit card statements for credit cards you do not have.
  - Debt collectors call you about debts that are not yours.
  - Suddenly your passwords or usernames or IDs do not work on your online accounts.
  - You receive notifications that your passwords have changed or other changes have been made to your online accounts.

SHOW SLIDE 17

SAY

- Also watch out for these warning signs:
  - You find unfamiliar accounts on your credit reports.
  - You receive medical bills for services you did not receive.
  - Healthcare providers have records of conditions you do not have.
  - The Internal Revenue Service (IRS) notifies you that more than one tax return was filed in your name, or that you have income from somewhere you never worked.
  - You are notified that your information was compromised by a data breach at a company where you do business or have an account.

Try It: Spotting Warning Signs of Identity Theft

Lead activity (15 minutes)—Exercise

See page 7 in the participant guide.

SHOW SLIDE 18

DO

- Ask participants to turn to "Try It: Spotting Warning Signs of Identity Theft" on page 7 in the participant guide.
- Read the scenario to participants or ask for a volunteer to do so.

Scenario: Ella Spots Warning Signs of Identity Theft

Ella is training to become a physical therapy assistant and also works. Ella receives a lot of communications, including paper mail, email, text messages, and direct messages and posts in social media. One day in spring she receives:

- An email from her place of worship
- An envelope from a dentist's office
- A direct message on a social media site for professionals
- An email from her career training program
- An envelope from her bank
- A thick envelope with coupons
- An envelope from the county government

DO

- Take five minutes to work in small groups. For each piece of mail, answer the question, "Are there warning signs of identity theft?" Be prepared to explain your answers.
- After five minutes, review each piece of mail using the answer key below. Time permitting, give participants opportunities to share and explain their answers.
- Conclude by reminding participants that mail is just one way you can be exposed to identity theft.

Try It: Spotting Warning Signs of Identity Theft – Answer Key

Communication	Are There Warning Signs of Identity Theft?
An email from her place of worship. The subject line is "Contribute to the Renovation Fund this month and we will match your donation!"	**Likely No** This is low risk, especially if Ella is familiar with the renovation project. She can double-check that all of the details in the mailing look legitimate, such as the address that is preprinted on the return envelope.
An envelope from a dentist's office. It looks like a bill, but Ella does not remember going to the dentist recently.	**Yes** Receiving medical bills for services you did not receive is a warning sign of identity theft. Ella should investigate immediately. She should report any identity theft and get help. (More information on how to report and get help is provided later in the training.)
A direct message on a social media site for professionals. The sender, whom she does not know, is looking for professionals in the field of physical therapy. Her short message encourages Ella to contact her to explore career opportunities.	**Likely No** This is low risk. She can do research on the sender's company to make sure it looks legitimate. Information from sources other than the company itself may be especially helpful. If Ella responds to the sender, she should ask a lot of questions and avoid sharing personal information that could be used for identity theft or fraud.
An email from her career training program. It is an automatically generated notice that her username and password for the school's billing and tuition management system have been changed. Ella has not logged into the system in the past week.	**Yes** This notification indicates that another person may be accessing her account. Ella should investigate immediately. She should report any identity theft and get help. (More information on how to report and get help is provided later in the training.)
An envelope from her bank. It is marked, "Make the most of your new EasyCard Express!" Ella does not remember applying for anything new.	**Yes** Receiving letters thanking you for opening an account you did not open is a warning sign of identity theft. Ella should read the contents of this piece of mail and then contact her financial institution to find out if someone has opened an account or accessed a bank product in her name.

Communication	Are There Warning Signs of Identity Theft?
A thick envelope with coupons. It is addressed to "Resident."	**Likely No** This is low risk, assuming the contents are coupons that contain no personal information about Ella.
An envelope from the county government. It is marked "citation notice." It looks similar to a speeding ticket she got two years ago.	**Likely No** This is low risk, especially if Ella recognizes the car, place, and date that are the subject of the citation.

Steps to Minimize Identity Theft

Present information (15 minutes)

See page 8 in the participant guide.

SHOW SLIDE 19

DO

- Share this list of steps participants can take to minimize identity theft. Time permitting, ask participants to offer ideas for each step on the list, and additional steps not listed.

SAY

You can never eliminate the risk of identity theft, but you can try to minimize it.

- Guard your personal information closely.
  - Be extremely careful about sharing your Social Security number, credit card and debit card numbers, personal identification numbers (PINs), passwords, and other personal information. If someone requests this information, ask:
    - » Why they need it.
    - » How it will be used.
    - » How they will protect it.
    - » What happens if you do not share it.
  - If automated teller machines (ATMs) do not work well for you because of mobility or dexterity considerations, try to get cash other than sharing your PIN with a personal attendant, friend, or family member. Visit a bank branch to get cash from a teller or ask for cash back at a trusted establishment where you do business.
  - Be suspicious of email or phone requests to update or verify your personal information. A legitimate organization will not solicit updates in an unsecured manner for information it already has.
  - Often standard forms contain blanks for filling in your Social Security number even if it is not needed. Do not assume you must provide it. Ask if you need to provide the number and why.

- Both online and paper forms sometimes have privacy statements that state how your information will and will not be used. Review these privacy statements so you can make an informed decision about whether you want to provide your information. If there is no privacy statement, reconsider whether you want to complete the form.
- Cover the keypad when typing in your PIN in public, including when you use financial institution websites in public places.
- Check ATMs, checkout registers at stores, and other machines for devices designed to steal your information when you swipe your card or type on the keypad. Before inserting your card, look at the card reader for signs it has been altered. Scan for hidden cameras. Beware of equipment like keypads or faceplates that look fake, look like they are the wrong size, or look out of place.
- Choose PINs and passwords that would be difficult to guess. For example, use a mix of numbers, symbols, and letters instead of easily guessed words. Avoid using easily identifiable information such as your name, your mother's maiden name, birth dates, the last four digits of your Social Security number, or phone numbers.
- Do not use the same PIN or password for multiple purposes.
- Change your passwords frequently and always change them if a company you do business with has a breach of its database.

■ Avoid letting others use your smartphone.

- Letting others use your phone gives them opportunities to access your personal information. Personal information can be used to commit identity theft or fraud.
- If you use your smartphone for mobile banking, a person borrowing your phone may transfer funds from your accounts.

■ Activate security features on your devices.

- Lock screens and other features prevent others from using them without your knowledge.
- If you lose your phone or leave it unattended, the security features will help prevent others from using it.

■ Do not respond to unsolicited requests.

- Never provide personal information in response to an unsolicited contact by email or phone. Even if the caller or emailer states they are with a financial institution or other organization you have a relationship with, do not give them the information requested. Instead contact the financial institution or organization directly using the contact information on its website or your account statement.
- Do not take the caller's word that they are who they say they are.

■ Protect your mail.

- Your mail is often an easy target for an identity thief because you likely receive and send personal information in the mail.
- Consider using a locked mailbox or other secure location to receive mail.
- If you are sending mail with personal information, deposit it in a United States Postal Service (USPS) collection box, hand it to a mail carrier, or take it to the post office instead of leaving it in your doorway or home mailbox.

- Pay attention to billing cycles and account statements and contact your financial institution if you do not receive a monthly bill or statement. Identity thieves often divert account documentation.
- Going paperless is a great way to protect your mail. Sign up for alerts at the company's or financial institution's website so you know when your bills and statements are ready to view online.
- Some people who are blind or visually impaired may ask others to read their print mail to them. People reading the mail have access to personal information. If you get help of this type, consider instead getting a scanner or mobile app that can read print materials to you. You can also opt to receive your financial information electronically instead of in the mail. If you have to use human readers, be sure they have been vetted by you or a trusted source.

- Sign up for direct deposit.
  - Signing up for direct deposit gives thieves less access to your banking information because payments of salary, pensions and annuities, and public benefits do not arrive by mail.
- Shred all personal and financial information.
  - Destroy all pieces of paper containing your personal information before recycling them. The best way to do this is using a crosscut shredder that cuts paper into tiny pieces of confetti that cannot be reconstructed.
  - Many financial institutions sponsor "shredding days" where you can bring your sensitive documents and shred them for free. Your library or other community organization may also offer such an event.
- Review your financial accounts regularly and carefully.
  - Contact your financial institution immediately if you notice something suspicious. For example, look out for a missing payment, a withdrawal you do not recognize, or a record of a purchase you did not make.
  - Most financial institutions offer several types of alerts and you can choose which ones you want. For example, you may be able to sign up for alerts so you are notified if someone uses your account overseas or without the physical card being present. Another common alert sends you an email or text if there has been a transaction over a certain dollar amount that you specify.
  - While federal and state laws may limit your losses if you are a victim of fraud or theft, to fully protect yourself, you need to report the problem quickly.

SHOW SLIDE 20

SAY

- Beware of identity theft on the internet.
  - Never provide bank account, credit or debit card, or other personal information when visiting a website that does not explain how your personal information will be protected. Look for "https://" in front of website addresses when placing an order and providing your credit or debit card information online.

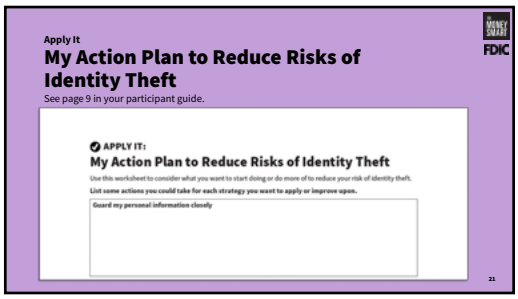
- Protect your devices, such as computers, phones, and tablets.
  - Ensure your access points are safe, including by setting a strong password for your Wi-Fi network at home, and being very cautious when using public or free Wi-Fi.
  - Download and frequently update security patches and software updates offered by your operating system and software vendors to correct weaknesses a hacker might exploit.
  - Find more information about staying safe online at **onguardonline.gov**, a Federal Trade Commission (FTC) resource.
- Review your credit reports at least once every 12 months for warning signs of identity theft.
  - You are entitled by law to receive free annual credit reports from each of the three nationwide credit reporting agencies. **Annualcreditreport.com** is the only website authorized to fill orders for these free credit reports.
  - You can get three credit reports per year for free. Visit **annualcreditreport.com** to learn more.
  - Ordering your own credit reports does not affect your credit scores. That is a common misunderstanding.
- Keep your important documents secure.
  - Consider storing critical paper records in a fire-resistant, waterproof, locked box in your house or in a safe-deposit box.
  - For digital records, ensure your storage location is encrypted and uses a strong password. Read the privacy policy for the document storage company to ensure you are comfortable with how your information is handled.
- Beware of disaster-related scams.
  - Con artists take advantage of people after disasters by claiming to be from legitimate charitable organizations when they are attempting to steal money or valuable personal information.
- Read scam alerts.
  - The Federal Trade Commission (FTC) maintains a running list of scams at **consumer.ftc.gov/features/scam-alerts**. You can report scams on the FTC site, too.

Apply It: My Action Plan to Reduce Risks of Identity Theft

Lead activity (5 minutes)

See page 9 in the participant guide.

SHOW SLIDE 21



SAY

- Turn to "Apply It: My Action Plan to Reduce Risks of Identity Theft" on page 9 in your participant guide.
- Take three minutes to list specific things from our discussion that you may want to do more often or start doing. It is okay if you do not finish this right now.

DO

- Give participants three minutes to work on the exercise.
- After three minutes, invite a few participants to share what they want to do more often or start doing.

Note to Instructor: For your reference, the Apply It from the participant guide is provided. The boxes for answers are larger in the participant guide.

APPLY IT

My Action Plan to Reduce Risks of Identity Theft

Use this worksheet to consider what you want to start doing or do more of to reduce your risk of identity theft.

List some actions you could take for each strategy you want to apply or improve upon.

Guard my personal information closely

Avoid letting others use my smartphone

Activate security features on your devices

Do not respond to unsolicited requests

Protect my mail

My Action Plan to Reduce Risks of Identity Theft *continued*

Sign up for direct deposit

Shred all personal and financial information

Review my financial accounts regularly and carefully

Beware of identity theft when I use the internet

Protect my devices, such as computers, phones, and tablets

My Action Plan to Reduce Risks of Identity Theft *continued*

Review my credit reports at least once every 12 months

Keep my important documents secure

Beware of disaster-related scams

Read scam alerts

Can you think of anything else?

Reporting Identity Theft and Getting Help

Present information (15 minutes)

See page 12 in the participant guide.

SHOW SLIDE 22

SAY

- The Federal Trade Commission (FTC) is a great source of information on identity theft and fraud. Its site at **identitytheft.gov** lets you know how to take action if your identity has been stolen.
- The FTC advises you to create an identity theft report if your identity has been stolen. Your identity theft report proves to businesses that someone stole your identity, and makes it easier to correct problems caused by identity theft. You can create an identity theft report by filing a report with the FTC at **identitytheft.gov**.
- There is a copy of an identity theft report in your participant guide on page 12.

SHOW SLIDE 23

SAY

- If your identity has been stolen, the FTC advises you to work with credit reporting agencies to respond to the identity theft. Credit reporting agencies, also called credit bureaus, consumer reporting companies, or credit reporting companies, provide credit reports.
- You can work with credit reporting agencies to place a fraud alert on your credit reports. This alert means potential creditors must verify your identity before they issue credit in your name.
  - Placing a fraud alert on your credit reports is free.
  - To place this alert, contact one of the three nationwide credit reporting agencies: Equifax, TransUnion, or Experian. Contact information is in your participant guide. Whichever credit reporting agency you contact to place the fraud alert must contact the other two.
  - You can place a one-year initial fraud alert. You can do this if your identity has been stolen or if you think it might be stolen. An identity theft report is not required. When it expires, you can place another one.
  - You can also place a seven-year extended fraud alert. You must first file an identity theft report.
- You can work with credit reporting agencies to dispute inaccurate information on your credit reports. Do so with each of the credit reporting agencies that included the inaccurate information.

- Finally, you can work with credit reporting agencies to place credit freezes on your credit reports.
  - Getting a credit freeze is free.
  - A credit freeze lets you restrict access to your credit reports, making it less likely an identity thief can access them without your permission.
  - A credit freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether.

SHOW SLIDE 24

SAY

- If your identity has been stolen, the FTC also advises you to communicate with your creditors and debt collectors to:
  - Alert them about fraudulent accounts. After you give them a copy of a valid identity theft report, they are not allowed to report on fraudulent accounts to the credit reporting agencies.
  - Get copies of documents related to the theft of your identity, like transaction records or applications for new accounts. Write to the company with the documents, and include a copy of your identity theft report.
  - Ask them to stop contacting you about fraudulent accounts. Debt collectors generally must stop contacting you after you send them a letter telling them to stop because the accounts are fraudulent.
  - Get written information about fraudulent accounts, including the name of the creditor and the amount you supposedly owe. If a debt collector contacts you about a debt, request this information in writing.

SHOW SLIDE 25

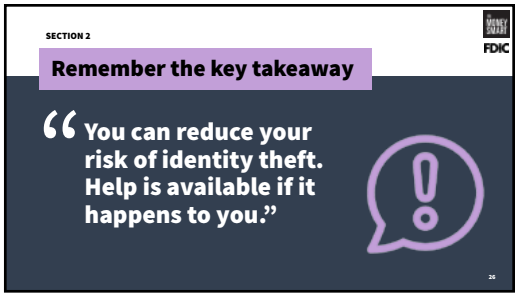
SAY

- You have other federal rights related to identity theft. See **identitytheft.gov** for more details. For example, you generally have limited liability for fraudulent debts caused by identity theft. Your liability depends on what type of financial product was used by the thief and also how soon you reported the issue after learning of the theft.
- In many states, businesses or organizations that lose or misplace certain types of personal information must tell you if that has happened. To learn more, go to **usa.gov** and search for "data breach" together with "[your state's name]." For example, if you live in Indiana, you will type "data breach Indiana."

SHOW SLIDE 26

SAY

- Remember the key takeaway: You can reduce your risk of identity theft. Help is available if it happens to you.



Section 3: Insurance and Recordkeeping

Time estimate for this section: 20 minutes

See page 14 in the participant guide.

Participants will be able to:

- Explain how insurance works
- Identify types of insurance and when they are needed
- Explain the role of recordkeeping for making sure insurance covers risks

SHOW SLIDE 27

SAY

- We will discuss how insurance can reduce the financial impact of a loss and the importance of keeping accurate records.

SHOW SLIDE 28

SAY

- The key takeaway for this section is: Insurance provides protection from financial loss. Keep accurate records of your assets and any damages to your property.

How Insurance Works

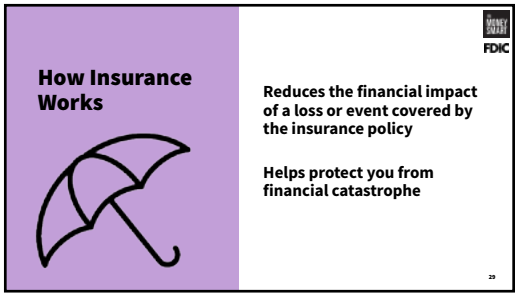
Present information (8 minutes)

See page 14 in the participant guide.

SHOW SLIDE 29

SAY

- Insurance can reduce the financial impact of a loss or event covered by the insurance policy. For example, insurance can cover part or all of your losses due to various events, such as car accidents, property theft, identity theft, natural disasters, medical expenses, disability, or death.

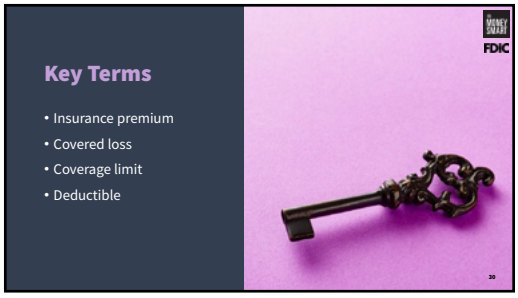


- Some people may think of insurance as a luxury or an unnecessary expense. But insurance is an important way to protect yourself from financial catastrophe.

- Sometimes, laws require you to have insurance. For example, most states require car owners to have some form of car insurance, although the details differ by state.

- If you do not have insurance and something happens that could have been covered by insurance, you will likely have to use your own money to recover from the loss, or go into debt by borrowing money.
- It is also important to shop around and compare prices for insurance from several sources.
- A key consideration about insurance is that you need to have the insurance before the event you are trying to cover happens. For example, you cannot get fire insurance when your house is burning.

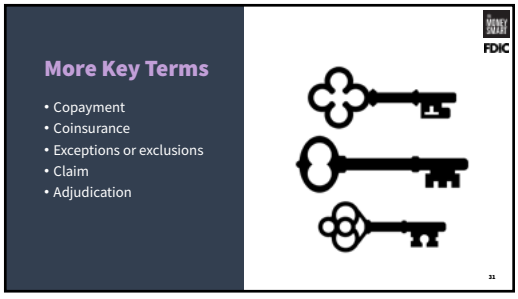
SHOW SLIDE 30



SAY

- There are some key insurance terms. The meaning of these terms depends on the type of insurance and the insurance policy. We'll talk about these in general. However, check your insurance policies for the exact meaning of these terms as they relate to your policies.
- When you purchase an insurance policy, you agree to pay money (known as an insurance premium) to the insurance company regularly.
- In exchange, the insurance company agrees to pay for losses or events covered under the policy, known as a covered loss, up to a maximum amount of money called the coverage limit.
- Some insurance policies include a deductible. You may have heard the phrase "I met my deductible."
  - If it is an annual deductible, which is common with health insurance, you agree to pay up to that amount each year before the insurance company will pay any claims.
  - If it is a per-claim deductible, which is common in vehicle insurance, you agree to pay up to this amount for each covered loss. If the loss is more than the deductible, the insurance company will pay the balance.
- For example, if you have vehicle insurance with a $200 per-claim deductible, that means you pay up to $200 for each covered loss.
  - » Let's say you get in a car accident. The insurance company estimates the covered loss is $850 to fix your car.
  - » You would pay $200 of the cost and the insurance company would pay the remaining $650.
  - » Let's say you had a very minor accident and repairs cost $190. With a $200 deductible, you would pay the full $190 because the loss was less than your deductible.

SHOW SLIDE 31



SAY

- Some insurance policies include a copayment or coinsurance.
  - A copayment is a dollar amount you have to pay each time you receive services or file a claim for a covered loss. It is similar to a per-claim deductible, but usually a smaller dollar amount.

- Coinsurance is a percentage of each claim you must pay before the insurance will pay. If you have 20% coinsurance, that means you pay 20% of the cost of a covered loss and the insurance pays 80%.

- Most insurance policies include exceptions or exclusions. These are limits on insurance coverage, or situations the insurance will not cover.
  - For example, homeowners insurance policies generally have an exception or exclusion for floods. That means damage from that type of natural disaster is not a covered loss. People can generally purchase separate coverage for the risk of floods.

- To be compensated, you usually need to file a claim with your insurance company. A claim notifies the insurance company you have incurred a loss that you believe your insurance policy covers.
  - The insurance company will adjudicate the claim. Adjudication is a process of reviewing the claim. It means the company will try to determine if the loss is covered by your insurance policy. If it determines it is covered, it will also determine what it will pay and what you may need to pay.
  - You have a right to submit claims for losses that you believe your insurance policy covers. However, insurance companies may consider multiple claims a sign that you are costly for them to insure, especially if the claims are close together in time.

Types of Insurance

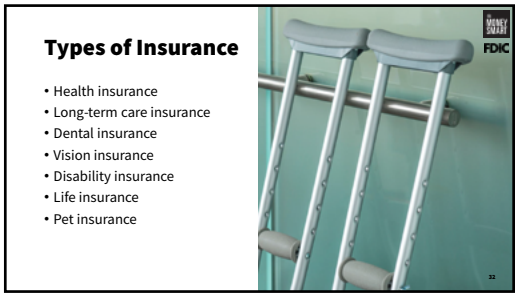
Present information (2 minutes)

See page 15 in the participant guide.

SHOW SLIDE 32

SAY

- These are types of insurance:
  - Health insurance.
  - Long-term care insurance.
  - Dental insurance.
  - Vision insurance.
  - Disability insurance.
  - Life insurance.
  - Pet insurance.



SHOW SLIDE 33

SAY

- Types of insurance also include:
  - Identity theft insurance.
  - Vehicle insurance.
  - Renter's insurance.
  - Homeowners insurance.
  - Flood insurance.

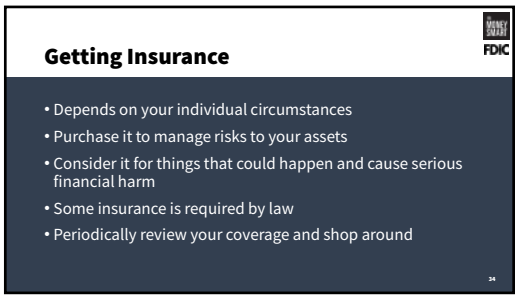
- For more information on types of insurance, you can visit the website of the National Association of Insurance Commissioners at **naic.org**.

Getting Insurance

Lead discussion (5 minutes)

See page 15 in the participant guide.

SHOW SLIDE 34



SAY

- The types and amounts of insurance you need depend on your individual situation.
- Purchasing insurance is about managing risks to your assets. Have the right insurance coverage.
- Consider getting insurance to protect against things that could happen and would cause you serious financial harm.
  - For example, having homeowners insurance is generally a good idea since your home is an expensive asset. Repairs needed because of a fire or other covered loss are generally costly. If you have a mortgage, the lender will require you to carry homeowners insurance.
  - However, for less expensive assets, like an inexpensive piece of jewelry, purchasing insurance to repair or replace it may be unnecessary. You may be able to afford to buy a new one or simply live without it for a while.
- Sometimes, insurance is required by law. For example, most states require car owners to have some form of car insurance, although the details differ by state.
- Periodically review all your insurance coverage and find out what is and is not covered by your policies. Shop around to find out if you can get a better deal considering both cost and coverage.
  - Before purchasing additional insurance, make sure that what you want to cover is not already covered by insurance you already have. For example, some homeowners insurance policies provide coverage for identity theft and fraud. If your homeowners insurance policy already includes that coverage, purchasing additional identity theft insurance may be unnecessary.

ASK

- What changes in your life may mean changes in the insurance you need?

DO

- Write participant responses on a flip chart or whiteboard.

- Add the following if not contributed:
  - Additions to your family mean more people are depending on you. You'll want to consider life insurance to reduce the financial impact on your dependents when you die.
  - If you have acquired expensive items, such as a television, mobility scooter, or power wheelchair, you'll want to make sure your renter's insurance or homeowners insurance policy covers those items.

SHOW SLIDE 35

SAY

- You can buy insurance directly from companies and organizations that offer it.
- In addition, you may be able to access health insurance, life insurance, and other types of insurance through your employer. Your premiums will be deducted from your pay.
- Shopping around may help you get a better deal on insurance.
- These tips can help you shop wisely:
  - Consider reviewing state-specific information on shopping for insurance from your state's department of insurance. To locate your state's department of insurance, go to the website of the National Association of Insurance Commissioners at **naic.org** and search for "state map."
  - Check out insurance companies.
    - » Research a company's complaint record at **content.naic.org/cis_consumer_information.htm**.
    - » Find out what others think about a company's customer service by reading online reviews.
  - Ask insurance agents about discounts. You may be able to get a lower premium for reasons such as safety features of your property or factors related to your lifestyle, such as how much you drive.
  - Compare quotes from several companies.
  - Consider the tradeoffs between a policy's deductible, coinsurance, coverage limit, and premium.
    - » An insurance policy with a higher deductible or coinsurance should have lower premiums than an identical policy with a lower deductible or coinsurance.
    - » An insurance policy with a higher coverage limit should have higher premiums than an identical policy with a lower coverage limit.

Apply It: Insurance—Do I Have It? Do I Need It?

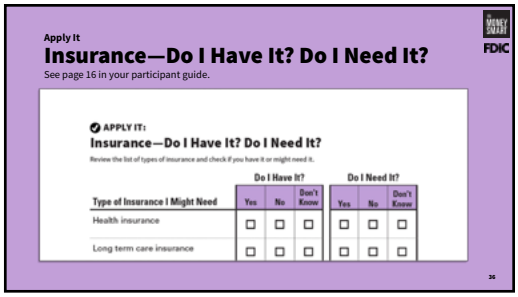
Lead activity (1 minute)

See page 16 in the participant guide.

SHOW SLIDE 36

SAY

- Turn to "Apply It: Insurance—Do I Have It? Do I Need It?" on page 17 in your participant guide.
- You can use this table after today's training to think about types of insurance you already have and what you might need.



Keeping Accurate Records

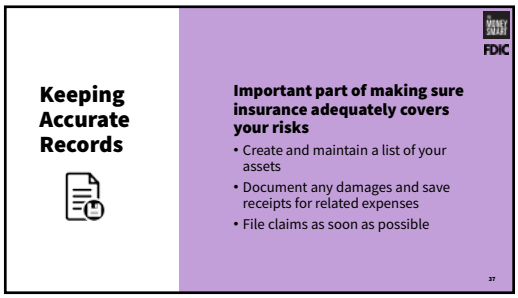
Present information (4 minutes)

See page 17 in the participant guide.

SHOW SLIDE 37

SAY

- Keeping accurate records is an important part of making sure insurance adequately covers your risks.
- It is important to keep a list or inventory of your assets, document damages to your assets if and when they occur, and file claims as soon as you discover the loss.



- Create and maintain a list of your assets.
  - Creating and maintaining a detailed inventory of the assets you are insuring will help if you need to file an insurance claim. This mainly applies to insurance that covers property.
  - Consider taking videos and/or pictures of your property. That could be quicker and more accurate than maintaining a written list. Keep your inventory in a safe place and update it as your property changes.
  - Your inventory will help you:
    - » Prove the value of what you own.
    - » Speed your claim processing.
    - » Keep records ,such as receipts, to support tax deductions you be able to claim for your losses.
  - An inventory can also help you determine how much insurance you need.

Note to Instructors: Time permitting, consider sharing copies of "Apply It: What Do I Need to Protect?" with participants as an example of a property inventory. That resource is found in Module 12: Living on Your Own in Section 5: Renter's Insurance.

- Document any damages and save receipts for related expenses.
  - Take pictures and videos to record damage to your home, personal property, or vehicle. Keep copies for your records and share them with your insurance company.

- Save receipts for any expenses you incur as a result of the damage or loss. If in doubt, save it. If possible, take pictures of your receipts. This could include receipts for:
  - » Construction or hardware supplies you purchase to repair something that was damaged.
  - » Hotel and restaurant expenses if you need to relocate temporarily.
  - » Written estimates for car repairs.

- File claims as soon as possible.
  - If you've incurred a loss that you believe is covered by your insurance policy, file a claim as soon as you discover the loss. Your policy might include a time limit for filing a claim and usually requires specific steps to file a claim.
  - If it is a physical asset that has been damaged, a representative of the company might come to see the damage.
    - » Cooperating with the representative and answering questions accurately can make the process go more smoothly.

SHOW SLIDE 38

SAY

- Remember the key takeaway: Insurance provides protection from financial loss. Keep accurate records of your assets and any damages to your property.

Module Closing

Time estimate for this section: 10 minutes

Remember the Key Takeaways

Note to Instructor: Only mention key takeaways for sections you included in the training.

SAY

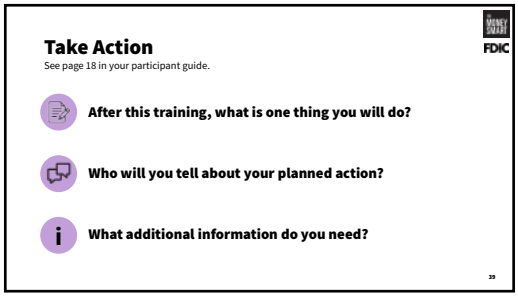
Remember the key takeaways. These are also listed on page 18 in your participant guide. Let me know if you have questions about any of them.

SECTION	KEY TAKEAWAY
1: Risks to Your Assets	Being aware of risks to your assets prepares you to take steps to reduce those risks.
2: Identity Theft and Fraud	You can reduce your risk of identity theft. Help is available if it happens to you.
3: Insurance and Recordkeeping	Insurance provides protection from financial loss. Keep accurate records of your assets and any damages to your property.

Take Action

See page 18 in the participant guide.

SHOW SLIDE 39



SAY

- You are more likely to take action if you commit to taking action now.
- Consider writing down what you intend to do based on today's training.
- Take a few minutes to answer the questions under "Take Action" on page 18 in your participant guide.

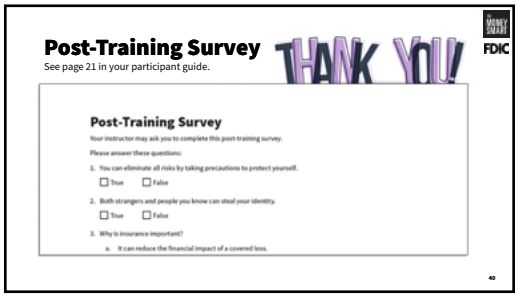
DO

- If time permits, ask a few participants to share what they wrote.
- Remind participants about the activities in their participant guide they can complete after today's training.
- Refer participants to "Where to Get More Information or Help" on page 19 in their participant guide for a list of online resources.
- If this is the end of your training, thank participants for attending and administer the post-training survey.

Post-Training Survey (Optional)

See page 21 in the participant guide.

SHOW SLIDE 40



SAY

- Thank you for coming to this Money Smart training.
- Please complete the post-training survey on page 21 of your participant guide.
- It should take less than five minutes to complete.

DO

- Collect the completed surveys.

Answer Key for the Pre- and Post-Training Survey

1. You can eliminate all risks by taking precautions to protect yourself.

   The answer is **false**.

2. Both strangers and people you know can steal your identity.

   The answer is **true**.

3. Why is insurance important?

   a. It can reduce the financial impact of a covered loss.
   b. It prevents damage from natural disasters.
   c. It has federally insured deposit protection.
   d. It allows you to digitally encrypt your information to keep it safe.

   The answer is **a. It can reduce the financial impact of a covered loss.**

4. Which of the following are ways to reduce the risk of identity theft?

   a. Protect your numbers (e.g., Social Security number, credit card numbers, bank account numbers)
   b. Protect your mail
   c. Sign up for direct deposit
   d. All of the above

   The answer is **d. all of the above**

Note to Instructor: There are no "right" or "wrong" answers to the remaining questions, which appear in the post-training survey and not in the pre-training survey.