

Participant Guide



FDIC Financial Education Curriculum



Table of Contents

Pre-Test.....	4
Federal Consumer Protection Laws and Regulations	6
Activity 1: Deposit Accounts Laws and Regulations	7
Additional Deposit Insurance Information.....	8
Non-Deposit Investment Products.....	10
Privacy Notices	10
Identity Theft.....	11
Activity 2: Identity Theft Self-Check	13
Elder Financial Abuse	16
Insurance–Managing Risks to Your Financial Security.....	18
Planning For Unexpected Life Events–Death and Disability.....	19
How to Be Financially Prepared for Disasters	20
Activity 3: How Financially Prepared Are You?	21
Post-Test.....	22
Glossary	24
What Do You Know? – Keep It Safe.....	26
Evaluation Form	27

Checking In

Welcome

Welcome to *Keep It Safe*! There are many consumer protection laws that protect your rights as a consumer, and knowing your legal rights can help you protect your money.

The *Keep It Safe* module will give you general information on the laws and regulations that protect your rights as a consumer, and will help you guard against identity theft and elder financial abuse. It will also help you know how to be financially prepared when a disaster strikes.

Objectives

After completing this module, you will be able to:

- Recognize how federal deposit insurance protects deposits
- Recognize how to guard against identity theft
- Recognize how to prevent elder financial abuse
- Recognize how the various types of insurance will help you manage risks
- Recognize the need to plan for unexpected death or disability
- Describe the ways you need to be financially prepared for disasters

Student Materials

This *Keep It Safe* Participant Guide contains:

- Information and activities to help you learn the material
- Tools and instructions to complete the activities
- Checklists and tip sheets
- A glossary of the terms used in this module

Pre-Test

Test your knowledge about protecting your finances before you go through the course.

1. **The Federal Deposit Insurance Corporation (FDIC) protects and insures which types of accounts? Select all that apply.**
 - a. Checking and savings
 - b. Money market deposit accounts, Certificates of Deposit (CDs), and certain retirement deposits
 - c. Stock and bond investments
 - d. Mutual funds

2. **Where can you find information on how a financial institution handles and shares your personal information?**
 - a. It is listed in the Truth in Lending Act
 - b. In the Terms & Conditions listed on your account statement
 - c. In a Privacy Notice sent to you by the financial institution
 - d. On the back of your checks

3. **Which of the following are ways to prevent identity theft?**
 - a. Protect your numbers (Social Security Number (SSN), credit card, etc.)
 - b. Protect your mail
 - c. Sign up for direct deposit
 - d. All of the above

4. **Which of the following are ways to protect your credit report against identity theft? Select all that apply.**
 - a. Place a fraud alert on your credit file
 - b. Never apply for credit
 - c. Remove your credit report from the credit reporting agencies' databases
 - d. Place a security freeze on your credit file

5. **Elder financial abuse can include:**
 - a. Taking an older person's money or property
 - b. Forging an older person's signature
 - c. Scamming or deceiving an older person
 - d. All of the above

6. **Insurance is important because:**
 - a. It is required by law
 - b. It protects for you from certain financial losses
 - c. It helps you save money on taxes
 - d. It helps you get a job

7. Which of the following are reasons why you should plan for unexpected death and disability?

- a. Planning gives you control
- b. Planning allows you time to make the right choices for your situation
- c. Planning helps you avoid financial disasters or setbacks
- d. b and c
- e. All of the above

8. What should you do to be financially prepared for disasters? Select all that apply.

- a. Pack an emergency evacuation bag with extra clothes and personal/first aid items
- b. Have important documents readily available in a secure location
- c. Arrange for direct deposit and automatic bill payments
- d. Review your insurance plans to ensure the coverage is adequate

Federal Consumer Protection Laws and Regulations

There are many federal consumer protection laws. In fact, there are too many to cover in this module. However, you should know that financial institutions must follow certain laws and regulations that protect your rights as a consumer.



Truth in Savings Act

The *Truth in Savings Act (TISA)* requires financial institutions to disclose the terms and conditions of bank accounts clearly and in writing. Some of the required information that a bank must give to consumers includes:

- Interest rate information
- Balance requirements
- Fee information

Because of this law, the bank must send you statements for your accounts periodically and provide account information to you any time you ask for it. This allows you to shop for the best account and make informed decisions before opening a deposit account.

Electronic Fund Transfer Act

The *Electronic Fund Transfer Act (EFTA)* establishes rights, liabilities, and responsibilities of:

- Customers who use electronic fund transfer services
- Banks that offer these services, which include the use of:
 - Automated teller machines (ATMs)
 - Debit cards
 - Telephone or computer transactions

Expedited Funds Availability Act

The *Expedited Funds Availability Act (EFAA)* limits the amount of time a bank can hold a check deposited into your checking account.

FDIC Deposit Insurance Regulations

The *Federal Deposit Insurance Corporation (FDIC) deposit insurance regulations* protect your money if the bank fails. However, FDIC does not insure non-deposit investment products (e.g., stocks, bonds, mutual funds, and annuities).

If you have any questions or problems with your deposit account, write a letter to your financial institution. If you do not receive a response, contact your bank's regulatory agency.

Activity 1: Deposit Accounts Laws and Regulations

Read each scenario. Determine whether a federal consumer protection law protects each account holder, and if so, which one. You can refer to the laws and regulations listed on the previous page.

Example 1

Mary is considering opening a bank account, and she asks for written information about the account. Does a federal law guarantee Mary's right to receive written information? If so, which one?

Example 2

The bank charges Chris an overdraft fee when he writes a check without sufficient funds in his account. This fee was listed on the fee schedule when he opened his account. Chris believes that by law, the bank cannot require him to pay this amount. Is Chris correct? Why?

Example 3

John deposits his paycheck into his checking account. He then tries to make a withdrawal from the ATM, only to discover that the money he just deposited is not available. John calls the bank and learns that his check is being held for one day. Does a federal law regulate the time in which banks can hold a check deposited into your checking account? If so, which one?

Example 4

Theresa has been using her debit card to pay for groceries. One day while shopping, she could not find her debit card. Theresa immediately called her bank. Is there a consumer protection law that protects Theresa from the unauthorized use of her card? If so, which one?

Additional Deposit Insurance Information



FDIC insures funds in deposit accounts at FDIC-insured institutions including:

- Checking
- Savings
- Money Market Deposit Accounts (MMDAs)
- Certificates of Deposit (CDs)

FDIC insurance does not, however, cover other financial products and services that insured banks may offer, (e.g., stocks, bonds, mutual fund shares, life insurance policies, annuities or municipal securities).

By law, federal deposit insurance is backed by the full faith and credit of the Federal Government. If a bank fails, the FDIC will pay all insured deposits up to the insurance limit, including principal and any accrued interest through the date of the bank closing. Federal law requires that all insured deposits be paid as soon as possible.

Insurance Coverage and Ownership Categories

Deposit insurance coverage is based on a depositor's ability to meet the specific requirements for an ownership category. The most common account ownership categories for individual and family deposits are single accounts, joint accounts, revocable trust accounts, and certain retirement accounts.

Each ownership category has different requirements, and the potential amount of insurance coverage for each category is based on the Standard Maximum Deposit Insurance Amount (SMDIA), which is \$250,000. For additional details on the coverage limits, requirements, and in-depth information on all account ownership categories and other types of deposit accounts visit www.myfdicinsurance.gov, call toll-free **1-877-ASK-FDIC**, or talk to your bank representative.

Single Accounts

A *single account* is a deposit account owned by one person and titled in that person's name only, with no beneficiaries. All of your single accounts at the same insured bank are added together, and the total is insured up to the SMDIA of \$250,000 per person. Note that retirement accounts and eligible trust accounts are not included in this ownership category.

Joint Accounts

A *joint account* is a deposit account owned by two or more people and titled jointly in the co-owners' names only, with no beneficiaries. If all co-owners have equal rights to withdraw money from a joint account, a co-owner's shares of all joint accounts at the same insured bank are added together and the total is insured up to the SMDIA of \$250,000 per person. A fiduciary or agent acting on behalf of another person is not to be considered an owner of the deposit for the purpose of creating a joint account. Note that jointly owned revocable trust accounts are not included in this ownership category.

Certain Retirement Accounts

Certain retirement accounts are deposit accounts owned by one person and titled in the name of that person's retirement plan. Only the following types of retirement plans are insured in this ownership category:

- Individual Retirement Accounts (IRAs), including: traditional IRAs, Roth IRAs, Simplified Employee Pension (SEP) IRAs, and Savings Incentive Match Plans for Employees (SIMPLE) IRAs
- Section 457 deferred compensation plan accounts (whether self-directed or not)
- Self-directed defined contribution plan accounts
- Self-directed Keogh plan (or HR 10 plan) accounts

All deposits that an individual has in any of the types of retirement plans listed above, and at the same insured bank, are added together and the total is insured up to the SMDIA (\$250,000 per person).

Revocable Trust Accounts

A *revocable trust account* is a deposit account held as a payable on death (POD) or in trust for (ITF) account, or one that is established in the name of a formal revocable trust (also known as a living or family trust account).

- POD and ITF accounts (also known as testamentary or Totten Trust accounts) are created when the account owner signs an agreement stating that deposits will be payable to one or more beneficiaries upon the owner's death.
- Living or family trusts are formal revocable trusts created for estate planning purposes.

If a revocable trust account has more than one owner, each owner's coverage is calculated separately:

- **Revocable Trust Deposits with Five or Fewer Beneficiaries:** Each owner's share of revocable trust deposits is insured up to \$250,000 for each beneficiary (i.e., \$250,000 times the number of different beneficiaries), regardless of the actual interest provided to beneficiaries.
- **Revocable Trust Deposits with Six or More Beneficiaries:** Each owner's share of revocable trust deposits is insured for the greater of either (1) coverage based on each beneficiary's actual interest in the revocable trust deposits, with no beneficiary's interest to be insured for more than \$250,000, or (2) up to \$1,250,000.

Determining coverage for living trust accounts that have six or more beneficiaries and provide different interests for the trust beneficiaries can be complicated. Contact the FDIC at **1-877-275-3342** if you need assistance in determining the insurance coverage of your revocable trust.

Non-Deposit Investment Products

The FDIC does not insure non-deposit investment products (e.g., bonds, mutual funds, and annuities). It only insures funds held in deposit accounts at FDIC-insured banks. When deposits are placed at an insured bank, the FDIC will provide up to at least the maximum amount allowed by law.

Here are some important tips you should keep in mind when considering buying investment products:

- Have enough emergency money in a savings or other readily accessible account to support you and your family for at least six months before investing in non-deposit products.
- Do your homework. Never invest in a product you do not understand.
- Attend classes, seminars, or check the business reference section of the public library to become better informed.
- Understand the risks before investing. Investments always have some degree of risk.
- Be sure your sales representative knows your financial objectives and risk tolerance.
- Take your time when making investment choices. Be careful of “act now” or “before it’s too late” statements.
- Retain and maintain account statements and confirmations you receive about your investment transaction.
- Document all conversations with brokers.
- Take immediate action if you detect a problem. Time is critical so do not be afraid to complain.
- Make checks payable to a company or financial institution, never an individual.
- Invest wisely online and offline. Be wary of investment scams.

Find out about the broker’s background via the **Financial Industry Regulatory Authority (FINRA) BrokerCheck** at www.finra.org, or by calling the **FINRA BrokerCheck Hotline** at **1-800 289-9999**. You may also contact the state securities office and Better Business Bureau.

Privacy Notices

Opting Out

If you prefer to limit the promotions you receive or do not want marketers and others to have your personal financial information, you must take steps to “opt out.” Federal privacy laws give you the right to stop or opt out of some sharing of your personal financial information. You can opt out of most, but not all, information sharing with other companies.

Information about your relationship with a company may also be shared with companies that are jointly owned or similarly affiliated with that company. If you opt out, you limit the extent to which the company can provide your personal financial information to non-affiliates. If you do not opt out within a reasonable period of time (generally about 30 days after the company mails the notice), the company is free to share certain personal financial information.

- If you did not opt out the first time you received a privacy notice from a financial company, it is not too late. You can always change your mind and opt out of certain information sharing. Contact your financial company and ask for instructions on how to opt out.
- Remember, your right to opt-out does not apply to personal financial information shared before you opted out.

In addition, you can call a toll-free number to opt out of receiving most preapproved offers of credit or insurance. To opt out, call **1-888-5-OPTOUT (567-8688)** or visit www.optoutprescreen.com.

Identity Theft

Identity theft occurs when thieves steal your personal information (e.g., your Social Security number (SSN), birth date, or credit card numbers). With sufficient information, another person can become you and use your identity to commit fraud or other crimes.



How to Avoid Identity Theft

1. **Protect your SSN, credit card and debit card numbers, personal identification numbers (PINs), passwords, and other personal information.**

Never provide this information in response to an unwanted phone call, fax, letter, or email, no matter how friendly or official the circumstances may appear. Be mindful of those who may be shoulder surfing (or trying to look over your shoulder) while you use the ATM, and seeking to steal your PIN. In case your wallet is lost or stolen, carry only the identification you really need: checks, credit cards, or debit cards. Keep the rest, including your Social Security card, in a safe place. Do not preprint your SSN, phone number, or driver's license number on your checks. You have the right to refuse requests for your SSN from merchants. Ask the merchant to use another form of identification that does not include your SSN (e.g., a passport) and have your driver's license number changed.

2. **Protect your incoming and outgoing mail.**

For incoming mail: Try to use a locked mailbox or other secure location (e.g., a post office box). If your mailbox is not locked or in a secure location, try to promptly remove mail that has been delivered or move the mailbox to a safer place. When ordering new checks, ask about having the checks delivered to your bank branch instead of having them mailed to your home where you run the risk of a thief finding them outside your front door.

For outgoing mail containing a check or personal information: Try to deposit it in a United States (U.S.) Postal Service blue 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. A mailbox that holds your outgoing bills is a prime target for thieves who cruise neighborhoods looking for account information. Avoid putting up the flag on a mailbox to indicate that outgoing mail is waiting.

3. **Sign up for direct deposit.**

Sign up for direct deposit of your paycheck or state or federal benefits, (e.g., Social Security). Direct deposit prevents someone from stealing a check out of your mailbox and forging your signature to access your money. It is also beneficial in the event of a natural disaster.

4. **Keep your financial trash “clean.”**

Thieves known as dumpster divers pick through garbage looking for pieces of paper containing SSNs, bank account information, and other details they can use to commit fraud. What is your best protection against dumpster divers? Before tossing out these items, destroy them, preferably using a crosscut shredder that turns paper into confetti that cannot be easily reconstructed.

5. **Keep a close watch on your bank account statements and credit card bills.**

Monitor these statements each month and contact your financial institution immediately if there is a discrepancy in your records or if you notice something suspicious (e.g., a missing payment or an unauthorized withdrawal).

Contact your institution if a bank statement or credit card bill does not arrive on time. Missing financially related mail could be a sign someone has stolen your mail and/or account information, and may have changed your mailing address to run up big bills in your name from another location.

6. Avoid identity theft on the Internet.

Never provide bank account or other personal information in response to an unsolicited email, or when visiting a website that does not explain how personal information will be protected. Legitimate organizations would not ask you for these details because they already have the necessary information, or can obtain it in other ways. If you believe the email is fraudulent, consider bringing it to the attention of the Federal Trade Commission (FTC). If you do open and respond to a phony email, contact your financial institution immediately. For more about avoiding phishing scams, or to obtain a brochure with tips on avoiding identity theft, visit www.fdic.gov.

Take precautions with your personal computer (PC). For example, install a free or low-cost firewall to stop intruders from gaining remote access to your PC. Download and frequently update security patches offered by your operating system and software vendors to correct weaknesses that a hacker might exploit. Use passwords that will be hard for hackers to guess. For example, use a mix of numbers, symbols, and letters instead of easily guessed words. Also, shut down your PC when you are not using it. For practical tips to help you guard against Internet fraud, secure your computer, and protect your personal information visit www.OnGuardOnline.gov.

7. Review your credit record annually and report fraudulent activity.

Review your credit report carefully for warning signs of actual or potential identity theft (e.g., items that include mention of a credit card, loan, or lease you never signed up for, and requests for a copy of your credit record from someone you do not recognize), which could be a sign that a con artist is snooping around for personal information. Learn more by visiting the FTC at www.ftc.gov/credit.

8. Get more information.

Visit the FTC at www.ftc.gov/idtheft or call **1-877-IDTHEFT (438-4338)**.

Activity 2: Identity Theft Self-Check

Review each response on the list and indicate whether you perform this action always, sometimes, or never. Then, tally your score and see how well you are taking measures to avoid identity theft.

	Always (2 points)	Sometimes (1 point)	Never (0 points)
1. Cover or block the Point of Service (POS)/ATM keypad when I enter my PIN			
2. Carry only the identification, checks, credit cards, or debit cards I really need			
3. Use direct deposit for paychecks, tax refunds, etc.			
4. Shred documents with personal/financial information before disposing of/recycling them			
5. Use complex passwords with a mix of numbers, symbols, and letters instead of easily guessed words			
6. Review financial statements/bills monthly and identify/correct errors			
7. Review my credit report annually and identify/correct errors			
8. Use secure mailboxes for incoming/outgoing mail			
9. Avoid providing/sharing personal information (e.g., SSN) whenever possible			
Total each column			
Grand Total			

Scores:

0–6: You are not taking many actions to minimize your risk of identity theft. Consider what you have learned today, and consider how you can implement steps to protect your identity.

7–13: You have developed some good practices to avoid identity theft; however, you have room for improvement. Consider what actions you need to take or apply more regularly to better protect your identity.

14–20: You are doing a great job at minimizing your risk of identity theft. Continue to apply these actions regularly and determine what additional steps you can take to protect your identity.

What to Do If You Suspect You Are a Victim of Identity Theft

If you believe you are a victim of identity theft, the FTC recommends that you immediately take the following actions:

- File a report with your local police. Get a copy of the police report, so you have proof of the crime.
- Contact your creditors about any accounts that have been changed or opened fraudulently. Ask to speak with someone in the security or fraud department.
- Follow up in writing, and include copies of supporting documents.
- Keep records of your conversations and all correspondence.
- Use the Identity Theft Affidavit at www.ftc.gov/idtheft to support your written statement.
- File a complaint with the FTC using the online complaint form (www.ftccomplaintassistant.gov) or call the FTC Identity Theft Hotline.
- Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
- Call the FTC's Identity Theft Hotline at **1-877-IDTHEFT (438-4338)** or visit www.ftc.gov/idtheft.

Fraud Alerts

If you suspect you have been a victim of identity theft, or think you are about to be, (e.g., if your wallet is stolen):

- Contact the fraud department of any of the three major credit reporting agencies. The agency you call is required to notify the other two credit agencies. Tell them you are an identity theft victim (or potential victim).
- You have the right to place an *initial fraud alert* in your credit file. You can do this by calling, writing, or visiting any of the three credit agencies online. This initial fraud alert will last for 90 days.

If you know you are a victim of identity theft, you may have an extended fraud alert placed in your credit file.

- The *extended fraud alert* requires a lender to contact you and get your approval before authorizing any new account in your name.
- The alert is effective for seven years.
- To place an extended alert in your credit file, submit your request in writing and include a copy of an identity theft report filed with a law enforcement agency (i.e., the police) or with the U.S. Postal Inspector.

You can get a free copy of your credit report if you ask when you place a fraud alert on your file. Active-duty military personnel have the right to place an alert in their credit files so that lenders acting on loan applications can guard against possible identity theft.

Security Freeze

- Many states have laws that allow you to place a security freeze on your credit file. A *security freeze* restricts potential creditors and third parties from accessing your credit report unless you authorize the release of the security freeze.
- Be aware that using a security freeze to restrict access to your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application for credit.
- State laws vary, and there may be a charge to freeze and unfreeze a credit file. The cost of placing, temporarily lifting, and removing a credit freeze also varies. Many states make credit freezes free for identity theft victims; while in other states consumers pay a fee, typically \$10. For more information please visit: www.ftc.gov.

What to Do If Your Wallet or Purse is Lost or Stolen

What would you do if your wallet or purse were lost or stolen?

If your wallet or purse is lost or stolen, the FTC suggests you:

- File a report with the police as soon as possible. Keep a copy of the report in case your bank or insurance company needs proof of the crime.
- Cancel your credit cards immediately. Get new cards with different numbers.
- Place a fraud alert on your credit report by calling any of the major credit reporting agencies:
 - **Equifax: 1-800-525-6285**
 - **TransUnion: 1-800-680-7289**
 - **Experian: 1-888-397-3742**
- Report the loss to your bank. You might want to open new checking and savings accounts and stop payment on any lost checks.
- Contact the major check verification companies to request that they notify the stores that use their databases to not accept your lost checks. You can also ask your bank to notify the check verification service with which it does business. Two of the check verification companies that accept reports of check fraud directly from consumers are:
 - **TeleCheck: 1-800-366-2425**
 - **Certegy: 1-800-437-5120**
- Request a new ATM card with a new number and password.



Elder Financial Abuse

Elder financial abuse is occurring at an alarming rate. It involves using an older person's money or assets contrary to his or her wishes, needs, or best interests for the abuser's personal gain.



Elder financial abuse covers a wide range of activities, including:

- Taking money or property
- Forging an older person's signature
- Getting an older person to sign a deed, will, or power of attorney through deception, coercion, or undue influence
- Using the older person's property or possessions without permission
- Promising lifelong care in exchange for money or property and not following through on the promise
- Committing fraud against older people through the use of deception, trickery, false pretence, dishonest acts, or statements for financial gain
- Using telemarketing to commit scams against older people

Potential perpetrators of elder financial abuse may include family members who:

- Have substance abuse, gambling, or financial problems
- Stand to inherit and feel justified in taking what they believe is almost or rightfully theirs
- Fear that their older family member will get sick and use up his or her savings, depriving the abuser of an inheritance
- Have had a negative relationship with the older person and feel a sense of entitlement
- Have negative feelings toward siblings or other family members whom they want to prevent from acquiring or inheriting the older person's assets

Telemarketers may also seek out elderly people who are more trusting of investment or charity schemes.

Who is at Risk?

The following conditions or factors may increase an older person's risk of being victimized: isolation, loneliness, recent losses, physical or mental disabilities, lack of familiarity with financial matters, and family members who are unemployed and/or have substance abuse problems.

For more information, contact your state's Adult Protective Services department. You may also contact the U.S. Department of Health and Human Services' Elder Care Locator at www.eldercare.gov or **1-800-677-1116** for a referral to services in your community.

How Can Elders Be Made Less of a Target?

Here are some lifestyle factors to help you assess whether an elder is at risk for financial abuse:

- Does the elder live alone?
- Does the elder still drive? If so, he or she may be prone to accidents, or to being victimized by driving-related scams.
- Does the elder spend a lot of time on foot in public places? If so, he or she may be targeted by exploiters who search for elderly victims at places, including: banks, stores, parks, malls, and libraries.
- How many local friends does the elder have?
- Does the elder have information about housing options, care choices, and support groups?
- Have the elder's outside activities decreased over the past few years?
- Does the elder have family members and friend in the area? Do they maintain weekly contact?
- Who regularly checks the status of the elder's bank accounts, charge or credit accounts, or investments?
- Where and from whom is the elder getting financial and medical advice?
- Who oversees the elder's power of attorney?
- Does the elder seek advice of fortunetellers or psychic advisors?
- Does the elder know when and how to call the police for emergencies and non-emergencies (e.g., suspicious persons)?

How Can I Be More Careful in Employing Elderly Caregivers?

Ensure:

- The caregiver is hired from a reputable agency and is insured, bonded and, if required in your community, licensed.
- The caregiver's references have been checked.
- A criminal background check has been completed on the caregiver.
- The elder's checks, credit cards, etc., are locked up and secure.
- There is a written service agreement, signed by the caregiver and elder, specifying duties and pay.
- There is a log of workers, hours, and salary payments.
- There is a weekly review of caregiver expenses.

For more information, contact your state's Adult Protective Services department. You may also contact the U.S. Department of Health and Human Services' Elder Care Locator at www.eldercare.gov or **1-800-677-1116** for a referral to services in your community.

Insurance—Managing Risks to Your Financial Security

Insurance is protection for you (and your family) from financial loss if the unexpected happens. Some of the most common types of insurance coverage that may help you avoid a financial setback include:

- Life insurance, which provides money for your loved ones if you die
- Health insurance to help pay for medical and recovery costs if you get sick
- Auto insurance for repair or replacement of your car and liability coverage to protect you if you are in an accident and held responsible for someone else's property damage or bodily injuries
- Homeowner's or renter's insurance for repair or replacement of your home and contents, and liability coverage to protect you if you are held responsible for someone else's loss
- Disability insurance, which provides you with income if you become too ill to work

Determining how much and what type of insurance you need will depend on your circumstances. If you cannot afford or do not want to afford the consequences of the risk, then you should consider getting insurance.

Insurance Coverage Tips

Check with organizations (e.g., your state's department of insurance, the Better Business Bureau, and the FTC) for free tips and online tools and information prior to purchasing insurance. Additional resources include:

- www.mymoney.gov
- www.naic.org
- www.insureuonline.org

In addition:

- Shop around for products and services; not every company charges the same rate or offers the same features.
- Ask about discounts for good driving records, good health, good grades, and special education or training.
- Consider the cost and benefits of opting for higher deductibles.
- Read your insurance policy carefully and ask questions if you do not understand any terms.
- Review your insurance coverage at least once a year.

Remember to help manage risk:

- Plan ahead for unexpected life events to minimize the risk of a financial loss.
- Maintain and review files for insurance policies.
- Evaluate your situation; needs change with life stages.
- Risk management strategies can be combined with savings and investments to achieve financial goals.

Insurance Issues for Military Service Members and Their Families

As a service member, you have certain rights and protections under federal law with respect to health and life insurance. Additional information regarding insurance issues for military service members and their families can be found at:

- www.naic.org/consumer_military_insurance.htm
- www.bbb.org/us/Military
- www.insurance.va.gov

Planning For Unexpected Life Events—Death and Disability

Planning ahead:

- Gives you control; you make choices for your situation
- Relieves stress of decision making from caretakers/family members
- Saves money and helps you avoid financial disaster or setback
- Allows time for gathering information, comparing options, and determining which options help achieve what is most important

Long-Term Care

A majority of people who need long-term care are older. However, the need for long-term care can come at any age due to disabling diseases, car accidents, Acquired Immune Deficiency Syndrome (AIDS), brain injuries, strokes, and other disabling events. For instance, it is estimated that 43 percent of the approximately 12 million people in the U.S. who say they need assistance with activities of daily living are working-age adults or children.

Families and individuals who do plan ahead for long-term care will be in a better position to understand long-term care changes, weigh options, and make sound long-term care decisions. Consider taking these steps before you or a family member becomes ill or disabled:

- **Prepare a plan.** Start with reviewing your income and expenses.
- **Make sure trusted family members know where to find personal and financial documents in an emergency.**
- **Think about the direct deposit of pay and benefit checks into bank accounts.**
- **Consider automatic payment of important, recurring bills.**
- **Make sure you are properly insured.** Speak with a financial planner or an insurance agent you trust. Review your policy often as life changes.
- **Maintain a healthy lifestyle.**
- **Consider a durable power of attorney.** This is a legal document giving one or more people the authority to handle finances or other personal matters if the individual becomes mentally or physically incapacitated.
- **Suggest a living will or other instructions about future medical care.** Most people should have a living will specifying the type of medical care they want or do not want if they become terminally ill and are unable to communicate their wishes.

Experts also recommend a health care power of attorney or health care proxy designating a family member or other trusted person to make decisions about medical treatment. Living wills and health care proxies are intended to ensure that someone's wishes regarding medical care are honored, but they also can prevent unnecessary and costly procedures.

How to Be Financially Prepared for Disasters

Natural or man-made disasters strike without warning and can happen to anyone. These include floods, fires, earthquakes, tornadoes, hurricanes or similar events that can force people to evacuate their homes. Even minor disasters can damage or destroy property or other belongings. They can also seriously impair your ability to conduct essential financial transactions. In addition to planning for your family's safety and basic needs (e.g., shelter, food, and water) you should be ready to deal with financial challenges, including how to pay for supplies or temporary housing if necessary.

What to Have Ready

Consider keeping the following documents, bank products, and other items in a secure place and readily available in an emergency:

- **Forms of identification:** These primarily include driver's licenses (or state identification cards for nondrivers), insurance cards, Social Security cards, passports, and birth certificates.
- **Your checkbook with enough blank checks and deposit slips to last at least a month**
- **ATM cards, debit cards (for use at ATMs and merchants), and credit cards:** Do not assume that merchants and ATMs in areas affected by a disaster will immediately be functioning as usual. Have other options available for getting cash and making payments.
- **Cash**
- **Phone numbers for your financial services providers:** These include local and toll-free numbers for your bank, credit card companies, brokerage firms (for stocks, bonds, or mutual fund investments) and insurance companies.
- **Important account numbers:** These include bank and brokerage account numbers, credit card numbers, and homeowner's or renter's insurance policy numbers. You may want to copy the front and back of your credit cards (and keep them in a safe place).
- **The key to your safe deposit box**

What to Keep and Where to Keep It

After you have gathered your most important financial items and documents, protect them as well as you can while also ensuring you have access to them in an emergency. Here is a reasonable strategy for many people:

- Make backup copies of important documents.
- Make an electronic image of your documents so you can more easily store the information.
- Give a copy of your documents to loved ones or let them know where to find the documents in an emergency.
- Store your backups some distance from your home in case the disaster impacts your entire community.



1. **Determine what to keep at home and what to store in a safe deposit box at your bank.** A safe deposit box is best for protecting certain papers that could be difficult or impossible to replace, but not anything you might need to access quickly. What should you put in a safe deposit box? Examples include a birth certificate and originals of important contracts. What is better left safely at home, preferably in a durable, fireproof safe? Your passport and medical care directives because you might need these on short notice. Consult your attorney before putting an original will in a safe deposit box. Some states do not permit immediate access to a safe deposit box after a person dies, so there may be complications accessing a will stored in a safe deposit box.

2. **Seal important documents in airtight and waterproof plastic bags or containers to prevent water damage.**
3. **Prepare one or more emergency evacuation bags.** Pack essential financial items and documents (e.g., cash, checks, copies of your credit cards and identification cards, a key to your safe deposit box, and contact information for your financial services providers). Make sure each evacuation bag is waterproof and easy to carry and kept in a secure place in your home. Periodically update the contents of the bag. It will not do you any good if the checks in your bag are for a closed account.

What Else to Consider

1. **Sign up for direct deposit.** Having your paycheck and other payments transmitted directly into your account will give you better access to those funds by check or ATM, and you will not have to deliver the deposit to the bank or rely on mail service, which could be delayed. **Note:** There could be delays in the processing of direct deposits in a disaster situation, but the problem is usually fixed within a reasonable timeframe.
2. **Arrange for automatic bill payments from your bank account.** This service enables you to make scheduled payments, (e.g., for your phone bill, insurance premiums and loan payments, and avoids late charges or service interruptions).
3. **Sign up for Internet banking services.** This also makes it possible to conduct your banking business without writing checks.
4. **Review your insurance coverage.** Make sure you have enough insurance, including: flood, earthquake, and personal property coverage, as applicable, to cover the cost to replace or repair your home, car and other valuable property.

To find out more about being financially prepared for disasters visit www.fdic.gov/consumers/consumer/news/index.html and type in *disaster preparedness* in the search box.

Activity 3: How Financially Prepared Are You?

Think about what you have learned today. What steps can you take after this class to ensure you are financially prepared for a disaster?

Post-Test

Now that you have gone through the course, see what you have learned.

1. **Which of the following is required information that a bank must provide to consumers under the Truth in Savings Act (TISA)? Select all that apply**
 - a. Interest rate and fee information
 - b. Periodic account statements
 - c. Balance requirements
 - d. Average monthly charges for the past year

2. **Is your money insured by the FDIC if you invest in a stock-based individual retirement account and the bank fails?**
 - a. Yes
 - b. No

3. **The federal privacy law permits a financial company to share certain information about you without giving you the right to opt out in which of the following situations? Select all that apply.**
 - a. When sharing your information with other companies looking to market their own products and services
 - b. When receiving a profit for your personal data
 - c. When a courts orders it to do so
 - d. When sharing your payment history on loans with credit bureaus

4. **How can you protect yourself from identity theft? Select all that apply.**
 - a. Keep a copy of your PIN in your wallet or purse should you forget the number
 - b. Sign up for direct deposit
 - c. Carry all of your credit cards and identification with you at all times
 - d. Review your financial account statements and credit report regularly

5. **You should plan for unexpected life events, (e.g., death and disability) so you can:**
 - a. Save money
 - b. Avoid a financial setback
 - c. Reduce stress of decision making during an emergency
 - d. Make choices that are right for you and your family
 - e. All of the above

-
- 6. Which of the conditions or factors below increase an older person's chance of becoming a victim of elder financial abuse? Select all that apply.**
- a. Person has close network of family and friends
 - b. Person has suffered recent losses and is lonely
 - c. Person has physical or mental disabilities
 - d. Person's finances are handled by a responsible person
- 7. What can you do to prepare financially for a disaster?**
- a. Set up automatic bill payments
 - b. Know where to find important documentation in an emergency
 - c. Review insurance information regularly to ensure you have adequate coverage
 - d. All of the above
- 8. Which of the following statements are true about insurance?**
- a. It protects you in the event of an accident or property damage
 - b. You are required to have insurance on your home, contents, and personal property
 - c. It is an important part of managing your money
 - d. Once you purchase insurance, there is no need to review or change your policy

Glossary

Certain Retirement Accounts: Deposit accounts owned by one person and titled in the name of that person's retirement plan.

Elder Financial Abuse: Act of using an elder's money or assets contrary to his or her wishes, needs, or best interests for the abuser's personal gain.

Electronic Fund Transfer Act (EFTA): An act that establishes rights, liabilities, and responsibilities of customers who use electronic fund transfer services and the banks offering these services.

Electronic Fund Transfer Services: Services including the use of automated teller machines (ATMs), debit cards, and telephone or computer transactions.

Expedited Funds Availability Act (EFAA): An act that limits the amount of time a bank can hold a deposit in your checking account.

Federal Deposit Insurance Corporation (FDIC) Deposit Insurance Regulations: Regulations that protect your money if the bank fails. However, FDIC does not insure non-deposit investment products, including: stocks, bonds, mutual funds, and annuities.

Identity Theft: When a person uses your personally identifying information without your permission to commit fraud or other crimes.

Insurance: Protection for you and your family against loss, for which you pay a certain sum periodically (known as an insurance premium) in exchange for a guarantee from the insurance company that they will cover or compensate you for certain losses (e.g., fire, accident, death, etc.).

Joint Account: A deposit account owned by two or more people and titled jointly in the co-owners' names only, with no beneficiaries.

Long-Term Care: Care or help with daily activities for those with a chronic illness or disability.

Non-Deposit Investment Products: Products including stocks, bonds, mutual funds, and annuities. The FDIC does not insure these products.

Pharming: When criminals seek to obtain personal or private information by making fake websites appear legitimate.

Phishing: When criminals send out unsolicited emails that appear to be from a legitimate source in an attempt to trick you into divulging personal information.

Privacy Notices: These notices explain how the company handles and shares your personal financial information. You will usually receive a privacy notice when you open an account or become a customer of a financial company, once a year after opening an account, and any time the financial company changes its privacy policy.

Revocable Trust Account: A deposit account held as a payable on death (POD) or in trust for (ITF) account, or one that is established in the name of a formal revocable trust (also known as a living or family trust account).

Single Account: A deposit account owned by one person and titled in that person's name only, with no beneficiaries.

Skimming: When criminals steal credit/debit card numbers by using a special storage device when processing your card.

Truth in Savings Act (TISA): An act that requires financial institutions to tell you the terms of consumer deposit accounts (e.g., checking or savings accounts). It also requires the bank to periodically send you statements for your accounts.

For Further Information

Federal Deposit Insurance Corporation (FDIC)

www.fdic.gov/consumer

Division of Supervision & Consumer Protection

2345 Grand Boulevard, Suite 1200

Kansas City, Missouri 64108

1-877-ASK-FDIC (275-3342)

Email: consumeralerts@fdic.gov

Visit the FDIC's website for additional information and resources on consumer issues. For example, every issue of the quarterly *FDIC Consumer News* provides practical hints and guidance on how to become a smarter, safer user of financial services. Also, the FDIC's Consumer Response Center is responsible for:

- Investigating all types of consumer complaints about FDIC-supervised institutions
- Responding to consumer inquiries about consumer laws and regulations and banking practices

U.S. Financial Literacy and Education Commission

www.mymoney.gov

1-888-My-Money (696-6639)

MyMoney.gov is the U.S. Government's website dedicated to teaching all Americans about financial education.

Whether you are planning to buy a home, balance your checkbook, or invest in your 401k, the resources on MyMoney.gov can help you. Throughout the site, you will find important information from federal agencies.

Federal Trade Commission

www.ftc.gov/credit

1-877-FTC-HELP (382-4357)

The Federal Trade Commission (FTC) website offers practical information on a variety of consumer topics, including credit and identity theft. The FTC also provides guidance and information on how to select a credit counselor.

What Do You Know? – Keep It Safe

Instructor: _____ Date: _____

This form will allow you and the instructors to see what you know about protecting your finances both before and after the training. Read each statement below. Please circle the number that shows how much you agree with each statement.

	Before the Training				After the Training			
	Strongly Disagree	Disagree	Agree	Strongly Agree	Strongly Disagree	Disagree	Agree	Strongly Agree
I can:								
1. Recognize how federal deposit insurance protects deposits	1	2	3	4	1	2	3	4
2. Recognize how to guard against identity theft	1	2	3	4	1	2	3	4
3. Recognize how to prevent elder financial abuse	1	2	3	4	1	2	3	4
4. Recognize how the various types of insurance will help me manage risks	1	2	3	4	1	2	3	4
5. Recognize the need to plan for unexpected death or disability	1	2	3	4	1	2	3	4
6. Describe ways to be financially prepared for disasters	1	2	3	4	1	2	3	4

Evaluation Form

This evaluation will enable you to assess your observations of the *Keep It Safe* module. Please indicate the degree to which you agree with each statement by circling the appropriate number.

<p>1. Overall, I felt the module was:</p> <p><input type="checkbox"/> Excellent</p> <p><input type="checkbox"/> Very Good</p> <p><input type="checkbox"/> Good</p> <p><input type="checkbox"/> Fair</p> <p><input type="checkbox"/> Poor</p>	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
2. I achieved the training objectives.	1	2	3	4	5
3. The instructions were clear and easy to follow.	1	2	3	4	5
4. The overheads were clear.	1	2	3	4	5
5. The overheads enhanced my learning.	1	2	3	4	5
6. The time allocation was correct for this module.	1	2	3	4	5
7. The module included sufficient examples and exercises so that I will be able to apply these new skills.	1	2	3	4	5
8. The instructor was knowledgeable and well-prepared.	1	2	3	4	5
9. The worksheets are valuable.	1	2	3	4	5
10. I will use the worksheets again.	1	2	3	4	5
11. The participants had ample opportunity to exchange experiences and ideas.	1	2	3	4	5
	None		Advanced		
12. My knowledge/skill level of the subject matter before taking the module.	1	2	3	4	5
13. My knowledge/skill level of the subject matter upon completion of the module.	1	2	3	4	5
14. Name of Instructor:	Response Scale: 5 Excellent 4 Very Good 3 Good 2 Fair 1 Poor				
Instructor Rating:					
Please use the response scale and circle the appropriate number.					
Objectives were clear & attainable	1	2	3	4	5
Made the subject understandable	1	2	3	4	5
Encouraged questions	1	2	3	4	5
Had technical knowledge	1	2	3	4	5

What was the most useful part of the training?

What was the least useful part of the training and how could it be improved?
