bankon Hampton Roads

Keep It Safe

Participant's Guide

Table of Contents

Welcome

Welcome to the *Keep It Safe* module! This lesson discusses fraud and identity theft, and ways to protect ourselves. The Crisis Mode module addressed our vulnerability when it comes to falling for quick fix schemes. This vulnerability doesn't just happen when we're in crisis, though. Anyone looking to improve their financial situation can fall victim to consumer fraud. As you'll see, fraud doesn't discriminate. This module also looks at insurance and different ways to guard against disaster, both natural and man-made.

.

Objectives

After completing this module, you will be able to:

– Recognize how to guard against identity theft

– Recognize how to prevent elder financial abuse

– Recognize how the various types of insurance will help them manage risks

– Recognize the need to plan for unexpected death or disability

– Describe ways to be financially prepared for disasters

Participant Materials

This *Keep It Safe* Participant Guide contains:

– Information to help you learn the material

– Tools and instructions to help you save

– Checklists and tip sheets

– A glossary of the terms used in this module

Pre-Test
Test your knowledge about protecting your finances

1. 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

2. 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

3. 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

4. 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

5. 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
    a. b and c
    a. All of the above

What is Identity Theft?

Identity theft always begins when the criminal obtains sensitive personal information that's used to assume another person's identity to make financial transactions or engage in other activities based on personal data, such as creating a resume to gain a job.

Six types of personal information are typically needed to steal an individual's identity:

- Name
- Address
- Social Security number
- Telephone number
- Mother's maiden name
- Employment

In addition, identity thieves may seek to collect information that can be used in social engineering, or personal contacts that help persuade the victim to trust the can artist, who then solicits more information to be used for fraudulent purposes. Information that can be effectively obtained through social engineering for the purposes of committing theft via identity fraud includes:

- past addresses
- financial account numbers
- children's names
- family background

Identity theft is a serious problem. Here is why:

- Despite the efforts of law enforcement, identity theft is becoming more sophisticated and the number of new victims is growing.
- If the crime is not detected early, you may face months or years cleaning up the damage to your reputation and credit rating. You may even lose out on loans, jobs, and other opportunities.

Did You Know...

- The number of U.S. identity fraud victims rose 12 percent to 11.1 million adults last year, the highest level since the survey began in 2003.[1]
- Nearly half of fraud victims now file police reports, resulting in double the reported arrests, triple the prosecutions and double the percentage of convictions in 2009.[1]
- Women were 26 percent more likely to be victims of identity fraud than men in 2008.[2]
- "Lost or stolen wallets, checkbooks and credit and debit cards" made up 43 percent of all ID theft incidents in which the "method of access" was known. [2]
- Credit and debit card fraud is the No.1 fear of Americans in the midst of the global financial crisis. Concern about fraud supersedes that of terrorism, computer and health viruses and personal safety.[3]

1 *Javelin Strategy & Research, "Identity Fraud Survey Report," February 2010.*

2 *Javelin Strategy & Research, February 2009 study.*

3 *Unisys Security Index: United States, March 2009.*

Common Forms of Identity Theft

Most identity theft occurs the "old fashioned way" and not electronically. Dumpster-diving, where thieves steal information out of the trash, is the most common way your information is obtained. But, technological advances, we are seeing more sophisticated attempts to commit fraud.

Phishing is when criminals send out unsolicited emails that appear to be from a legitimate source: perhaps from your financial institution, utility company, well-known merchants, your Internet service provider, or even a trusted government agency (e.g., the FDIC or NCUA). Their goal is to trick you into divulging personal information

Pharming is similar to email phishing in that criminals seek to obtain personal or private information by making fake websites appear legitimate. Your internet browser will even show that you are at the correct website which makes pharming more difficult to detect than phishing.

Also be careful of ***skimming***. This is when criminals steal credit/debit card numbers by using a special storage device when processing your card. This often occurs at places such a restaurants, gas stations and ATMs.

One of the newest scams involves text messages. The ***text scams*** occur when a criminal sends a text message to your cell phone under false pretenses to trick you into entering personal information with a bogus phone line or website so the criminal can use the information to raid your account. With cyber criminals shifting their focus to mobile devices, major telecommunications carriers such as AT&T, T-Mobile and Verizon are offering a new service for consumers who receive text spams that may involve scams. If you get a text you think is a scam, forward it to the number 7726. All three carriers use the same number in an attempt to establish a communications industry standard for dealing with spam.

You should also be mindful of unsecure online transactions. Many people use online seller-to-buyer sites like eBay and craigslist where you are giving your information directly to someone you don't know. This can put your information at risk. Remember, not all transactional websites are secure. Be sure to look for the padlock icon in the web address and for the "https" rather than "http."

Gold Mines

Identity thieves prize information that contains vital data or allows the holder to gain access to more data or additional privileges. The piece of information most highly sought by identity thieves is the Social Security number, which can then be used to obtain information about credit, financial accounts, medical records, and education records.

Forms of information that fall into the "gold mine" category include:

- Social Security cards
- birth certificates

• Passports

- permits to carry a concealed weapon
- medical cards, especially older versions that contain Social Security numbers
- student identification cards, especially versions containing Social Security numbers.

Victims Should Take Action *Immediately*

If you believe you are a victim of identity theft, the FTC recommends 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 at 1.877.IDTHEFT (438.4338).
- Ask for verification that the disputed account has been closed and the fraudulent debts discharged. If

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

- Report the loss to your bank or credit union. 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 all stores that use their databases to not accept your lost checks. You can also ask your financial institution 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) and Certegy (1.800.437.5120).
- Request a new Debit card with a new number and password.

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,* which is effective for seven years, requires a lender to contact you and get your approval before authorizing any new account in your name. To place an extended alert in your credit file, submit your request in writing to any of the three credit bureaus and include a copy of an identity theft report filed with a law enforcement agency (e.g., 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.

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. In Virginia, the fee for placing a security freeze on a credit report is $10. If you are a victim of identity theft and submit a valid investigative, incident or police report, the fee will be waived.

Protect Your Personal Information

Keep your important papers secure

- Lock them up. Lock your financial documents and records in a safe place at home, and lock your wallet or purse in a safe place at work. Keep your information secure from roommates or workers who come into your home.
- Limit what you carry. When you go out, take only the identification, credit, and debit cards you need. Leave your Social Security and Medicare cards at home or in a secure place.
- Pick up your new checks at the bank or credit union . When you order new checks, don't have them mailed to your home, unless you have a secure mailbox with a lock.
- Be careful with your mail. Take outgoing mail to post office collection boxes or the post office. Promptly remove mail that arrives in your mailbox. If you will be away from home for several days, request a vacation hold on your mail.
- Shred sensitive documents. Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents before you put them in your trash.
- Consider opting out of prescreened offers of credit and insurance by mail. You can opt out for five years or permanently. To opt out for 5 years, call 1.888.567.8688 or go to www.optoutprescreen.com. The three nationwide credit reporting companies operate the phone number and website.
- Protect your medical information. Destroy the labels on prescription bottles before you throw them out. Don't share your health plan information with anyone who offers free health services or products.
- Exercise your curiosity. Before you share information at your workplace, a business, your child's school, or a doctor's office, ask who will have access to your information, how it will be handled, and how it will be disposed of.

Secure your Social Security Number

- Protect it. Share your Social Security number, and your child's, only when necessary. Ask if you can use a different kind of identification.
- If someone asks you to share your Social Security number or your child's, ask why they need it, how it will be used, how they will protect it, what happens if you don't share the number. The decision to share is yours. A business may not provide you with a service or benefit if you don't provide your number.
- Sometimes you must share your number. Your employer and financial institutions need your Social Security number for wage and tax reporting purposes. A business may ask for your Social Security number so they can check your credit when you apply for a loan, rent an apartment, or sign up for utility service.

Protect Your Personal Information *con't*

Protect your computer and mobile device

- Use anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.

- Don't open files, click on links, or download programs sent by strangers. Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information you type.

Safely dispose of personal information.

- Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive.

- Before you dispose of a mobile device:

  – check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device.

  – Remove the memory or subscriber identity module (SIM) card from a mobile device.

  – Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer photos.

2010 Top FTC Fraud Complaints

Category	Complaints	% of Total Complaints
Identity Theft	278,078	21%
Third-party and creditor debt collection	119,549	9%
Internet services	83,067	6%
Shop-at-home and catalog sales	74,581	6%
Foreign money offers and counterfeit check scams	61,736	5%
Internet auctions	57,821	4%
Credit cards	45,203	3%
Prizes, sweepstake and lotteries	41 ,763	3%
Advance-fee loans and credit protection/repair	41,448	3%
Banks and lenders	32,443	2%
Credit bureaus, information furnishers and report users	31,629	2%
Television and electronic media	26,568	2%
Health care	25,414	2%
Business opportunities, employment agencies, work-at-home plans	22,896	2%
Computer equipment and software	22,621	2%

Protect Your Personal Information *con't*

Protect your data and personal information

- Encrypt your data. Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.

- Be wise about Wi-Fi. Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

- Keep passwords private. Use strong passwords with your laptop, credit, bank and other accounts. The longer the password, the harder it is to crack. Create passwords that mix letters, numbers, and special characters. Don't use the same password for many accounts. If it's stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts.

- Don't overshare on social networking sites. If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.

- Lock up your laptop. Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.

- Read privacy policies. Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

- Create PINs and passwords that are not easily determined and never use personal information such as birth dates, maiden names, your Social Security Number, pets names, etc.

Other Resources

Visit the Bank On Virginia Beach blog at bankonvb.blogspot.com for links to a variety of publications that will help you protect your identity as well as your children's. You'll also find the Office of the Attorney General's Identity Theft Passport.

Donotcall.gov: The National Do Not Call Registry gives you a choice about whether to receive telemarketing calls at home. Most telemarketers should not call your number once it has been on the registry for 31 days. If they do, you can file a complaint at this Website. You can register your home or mobile phone for free.

Optoutprescreen.com: a joint venture among Equifax, Experian and TransUnion, allowing customers to opt out of receiving credit card solicitations by mail

CreditKarma.com: continue to monitor changes in credit score monthly

Elder 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 acts that involve committing fraud against older people through the use of deception, trickery, false pretence, or dishonest acts or statements for financial gain. Particular examples include:

- 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
- Using telemarketing to commit scams against older people, including:

  – Perpetrators calling victims and using deception, scare tactics, or exaggerated claims to get them to send money.

  – Perpetrators making charges against victims' credit cards without authorization.

Potential perpetrators of elder financial abuse may include family members (e.g., children, grandchildren, or spouses) 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 increase an older person's risk of being victimized:

- Isolation: 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.
- Loneliness: How many local friends and family members does the elder have?
- Recent losses: Grief can cause us to do irrational things.
- Physical or mental disabilities: Have they become more forgetful?
- Lack of familiarity with financial matters: 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?
- Ties to family members who may have substance abuse problems

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 friends in the area? Do they maintain regular 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)?

For more information about elder financial abuse, contact your state's Adult Protective Services department. You may also contact Senior Services of Southeastern Virginia (SSSEVA). They offer a wide variety of services and programs for mature adults. They can be reached at 757.461.9481 or online at www.ssseva.org.

Insurance

Insurance is an important part of managing your money. It is protection for you (and your family) from financial loss if the unexpected happens. For example, you can get insurance to protect you if you become ill or disabled and are unable to work, to protect you in the event of an accident or property damage, or to provide for your loved ones in the event of your death.

If you do not plan ahead and protect yourself with insurance, you may have to use funds set aside for other financial goals or emergencies, or go further into debt by borrowing money.

Types of Insurance

There are many different types of insurance, too many to name for this class. 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
- Homeowner's or renter's insurance for repair or replacement of your home and contents if damaged, destroyed, or stolen, and liability coverage to protect you if you are held responsible for someone else's loss (e.g., if a friend trips and falls while visiting your home)
- Auto insurance for repair or replacement of your car if it is damaged, destroyed, or stolen, and liability coverage to protect you if you are in an accident and held responsible for someone else's property damage or bodily injuries
- Disability insurance, which provides you with income if you become too ill to work

There are also insurance products out there that may not be worth the investment, such as car repair insurance, some extended warranty insurance, etc. You'll need to evaluate the potential for loss and determine whether it is a good investment. Be sure to read carefully what is actually covered and what is excluded.

Savings is always the best form of insurance. Unlike an insurance contract, savings can be directed to any unexpected loss and there are no deductibles or co-pays. Savings may not be enough for larger costs like car accidents, but it can cover smaller needs.

Only one-third of Americans are covered by individual life insurance, the lowest level in 50 years.

LIMRA's 2011 Life Insurance Ownership Study

Determining Your Needs

Determining how much and what type of insurance you need will depend on your circumstances. One way to weigh whether you need a particular form of insurance is to consider the risk to your assets. For insurance purposes, assets can include both tangible assets, such as your home or car, and intangible assets, such as your health, your life, and your ability to earn a living.

Ask yourself the following questions to determine your risk:

- What are the risks to my assets? If you live atop a forest-covered mountain far from any streams or rivers, you're unlikely to be at risk from flood. Instead, protecting yourself from losses due to fire is likely to be more important.
- Can I afford to pay for the loss? If the asset is destroyed or damaged, can you do without it? If not, can you afford to repair or replace it? This applies to many types of assets, from your health to your home.
- What is the best method to handle this risk? Options include:

– Assuming losses yourself. For example, you may decide it's cheaper to pay-as-you-go for repairs to your television instead of purchasing a "maintenance contract," which is a form of repair insurance.

– Reducing the potential for loss. Purchasing a fire extinguisher to keep near your backyard fire pit is one way to reduce the potential for loss, for example.

– Buying insurance to protect the asset.

Rules for Better Insurance Decisions

When evaluating what type of insurance to buy and what to forgo, you should consider these rules.

- Determine your insurance needs. Always insure major risks first. Don't insure small losses that can be covered by your emergency fund.
- Select the type of insurance that meets your needs.
- Shop and compare prices.
- Make certain the premium quoted fits your budget. Otherwise, you won't be able to maintain the insurance and you'll be left with nothing.
- Never risk more than you can afford to lose.
- Ask specifically 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 (remember it is a legal document) and ask questions if you do not understand any terms.
- Review your insurance coverage at least once a year.
- Remember, your credit score impacts your insurance premiums. The lower your score, the higher the premium. This is just another example of how the work you're doing to build a better credit record will pay off for you.
- Also be careful of trading a higher deductible for a lower premium. If you get in an accident and can't afford the deductible, insurance won't pay.

Life Insurance Needs Calculation

To determine how much life insurance you need, consider the following:

- Mortgage Debt
  The first point worthy of consideration is whether your life insurance proceeds will be sufficient to help pay the remaining mortgage on your home. If you are carrying a large mortgage, you may need a sizable amount.
- College Expenses
  Many people want life insurance proceeds large enough to help cover their children's college expenses. The amount needed can be roughly calculated by matching the ages of your children against projected college costs adjusted for inflation.
- Continuing Income for Your Family
  The amount of income you will need to help provide for your surviving spouse and dependents will vary greatly according to your other assets, retirement plan benefits, Social Security benefits, age, health, and your spouse's earning power. Many surviving spouses may already be employed, or will find employment, but their income is based on education, training, and experience. Your spouse's income, alone, may be insufficient to cover the monthly expenses of your family's current lifestyle. Providing a supplemental income fund can help your family maintain its standard of living.
- Existing Resources
  If your current assets and retirement plan death benefits are sufficient to cover your financial needs and obligations, you may not need additional life insurance for these purposes. However, if they are inadequate, the difference between your total assets and your total needs may be funded with life insurance.

Who Needs Life Insurance?

Those with the highest need for life insurance include:

- Wage earners with dependents. Life insurance helps maintain the family's financial stability if the primary breadwinner dies. This is probably the most important single member of the family to insure.
- Homemakers with young children. A homemaker provides childcare. home maintenance. housekeeping. meal preparation. and other services. Replacing services provided by a homemaker can be costly.
- People who have debt. The only way to pass on the assets to your heirs may be to have life insurance to cover the unpaid balance.
- Keep in mind that the average cost for funerals and burials range from $8,000 to $10,000, and these expenses can be covered by a small life insurance policy. That being said, almost everyone can benefit from a life insurance policy.

When To Buy

Three factors typically drive life insurance availability and costs: age, need, and insurability, which include factors such as health and occupation. Typically, the best time to buy insurance is when you are young and healthy. Yet even middle-aged people should recognize that it's essential to purchase coverage if they want to protect their family-either the family they have now or the one they hope to building the future-from life's unexpected events.

Planning Ahead

Recognize the need to plan for unexpected life events (e.g., illnesses and disabilities that may require long-term care). Millions of people serve as financial caregivers for ill or elderly spouses, parents, children, or other loved ones. They perform services that include paying bills, handling deposits and investments, filing insurance claims, and preparing taxes. This role can be costly and physically and emotionally exhausting, especially for a caregiver who lives far away.

Planning ahead:

- Gives you control; you make choices for your situation.
- Relieves stress of decision making from caretakers/family members.
- Allows time for gathering information, comparing options, and determining which options help achieve what is most important.
- Saves money and helps you avoid financial disaster or setback. These are the situations that can ruin us financially if we are not prepared.

Disability Insurance

Disability insurance is designed to help people with ongoing expenses and loss of income when an illness or injury leaves them unable to work. The Health Insurance Association of America states that about 30 percent of Americans ages 35 to 65 will suffer a disability that lasts at least 90 days sometime during their career.

Disability policies are available from a variety of sources, including agencies, brokers, and employers. It's important to note, however, that even employees of companies that offer disability insurance may need a supplemental policy. Most workplace policies cover only 60 percent of the employee's base salary and are subject to income tax. To make up the difference, some workers choose to purchase supplemental disability policies.

A few questions to ask when purchasing disability insurance include:

- How long the policy will pay for your disability.
- How long must you be disabled before you are eligible for benefits? The period can vary from 30 days to one year.
- The length of time the disability benefits will be paid. This is usually a set number of years or until age 65.
- What type of disabilities are excluded under the policy? Some policies may cover illnesses but not accidents.
- Is the policy guaranteed renewable noncancelable?. The insurer can't cancel a guaranteed renewable policy, but the insurer can raise your premium for specific reasons.

Long-Term Care

Long-term care is something most people do not like to think about. But the chances that you, or someone in your family, will become ill or disabled probably are greater than you realize. It is estimated that 43% 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.

Consider taking these steps before you or a family member becomes ill or disabled:

- Prepare a plan. Start with reviewing your income and expenses. How would an illness or disability impact your finances? Do you need to reduce spending or increase your income? Studies show that short-term disabilities average from one to six months and long-term disabilities can average about two and a half years. Do you have that much saved in your emergency fund?
- Make sure trusted family members know where to find personal and financial documents in an emergency. These include bank, brokerage, and credit card statements; original wills; insurance policies; and Social Security, Medicare, and pension records.
- Think about the direct deposit of pay and benefit checks into bank accounts. Direct deposit is safer and more convenient than paper checks. There are no delays in getting funds deposited, and no checks are lost or stolen in the mail or forgotten at home.
- Consider automatic payment of important, recurring bills. You will have one less thing to worry about if you can arrange for utility bills and other regular commitments (e.g., insurance and the mortgage) to be paid electronically out of a checking account.
- Make sure you are properly insured. If you have doubts about your insurance coverage or ability to pay for long-term care, get a second opinion from a financial planner or an insurance agent you trust. Review your policy often as life changes.
- Maintain a healthy lifestyle. Getting regular checkups, not smoking, exercising, becoming safety minded, and taking care of your mental and emotional health may reduce your chances of becoming disabled. Back injury and arthritis are two of the leading causes of disability.
- 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 having 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.

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.

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. These documents will be crucial if you or your family should need to rebuild lost records or otherwise prove to a government agency, a bank, or other business that you are who you claim to be. It is best to have the originals, but have photocopies of these documents in case originals are misplaced or destroyed. Never keep the originals with the copies.

- **Your checkbook with enough blank checks and deposit slips to last at least a month**: Your need for checks will vary depending on how long you may be displaced or how often you write checks. Even if you rarely or never write checks, keep a copy of a check or your checking account number handy. This will enable you to authorize an important payment by providing the recipient (e.g., an insurance company) with your checking account number over the phone in an emergency.

- **ATMs, debit cards (for use at ATMs and merchants), and credit cards**: These cards give you access to cash and may help you pay outstanding bills. Make sure you know the PINs for your ATM and debit cards. Do not write your PINs on or near your cards in case they are lost or stolen. Do not assume that merchants and ATMs in areas affected by a disaster will immediately be functioning as usual—that is why it is smart to have other options available for getting cash and making payments.

- **Cash**: The amount you should have available will depend on several factors, including the number of people in your family and your ability to use ATMs and debit and credit cards to get more cash or to make purchases. Keep in mind that cash in your house or wallet can easily be lost or stolen.

- **Phone numbers for your financial services providers**: These include local and toll-free numbers for your banks and credit unions, credit card companies, brokerage firms (for stocks, bonds, or mutual fund investments), and insurance companies. Why have these numbers handy? You may need to defer a payment, replace lost cards or documents, open new accounts, or otherwise request assistance. If you have people you regularly deal with, have their phone numbers on your list too. Working with someone who knows you can speed things up and provide you with some additional peace of mind.

- **Important account numbers**: These include bank and credit union 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). Often, if you have a copy of your credit card and a valid ID, you can make a purchase without having your actual card. Additionally, the photocopies can help you keep track of your account numbers and company phone numbers.

- **The key to your safe deposit box**: You cannot access a safe deposit box without your key, no matter how many forms of identification you have. Also, while many places issue two keys when a box is rented, simply giving someone else a key does not allow that person access to a box in an emergency. He or she also must be designated in the financial institution's records as a joint renter or be appointed a deputy or agent who has access to your box. Contact your bank or credit union about the proper arrangements.

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 ensuring you have access to them in an emergency. Here is a strategy that works well for many people:

- Make backup copies of important documents.
- Consider making an electronic image of your documents using a computer scanner so you can easily store the information.
- Consider giving a copy of your documents to loved ones, or at least let them know where to find the documents in an emergency.
- Consider storing your backups some distance from your home, even in another state, in case the disaster impacts your entire community.

Also:

- Determine what to keep at home and what to store in a safe deposit box at your financial institution. 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. Examples include a birth certificate and originals of important contracts. Items that are better left safely at home, preferably in a durable, fireproof safe include 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. A few 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.
- Seal important documents in airtight and waterproof plastic bags or containers to prevent water damage.
- Prepare one or more emergency evacuation bags. Most of what you are likely to pack inside will be related to personal safety (e.g., first aid kits, prescription medications to last several days, flashlights, etc.). But your emergency kit also is the place to keep some essential financial items and documents, including 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 that it is kept in a secure place in your home. Review the contents of the bag periodically to make sure the contents are up to date. It will not do you any good, for example, if the checks in the bag are for a closed account.

Estate Planning

Financial planning for death is often called *estate planning*. For example, estate planning includes making a will to ensure that any money, property or assets you leave behind go directly to the recipients of your choice – not to the state or to other relatives who may suddenly decide to make a claim.

Here are some suggestions to help with estate planning.

- **Make or update your will**. A will allows you to determine what happens to your money and possessions when you die, and who becomes the guardian of your minor children. Otherwise, state laws and courts make those decisions for you. DO NOT make children beneficiaries of a will or insurance policy. They can't inherit the assets until they are of legal age. Two strategies: have the guardian manage the assets for the children or another trusted family member or place the assets in a trust for the benefit of the children.

- **Create durable powers of attorney**. These documents allow you to appoint someone to make decisions on your behalf if you become incapacitated. There are two types: one to deal with your personal, legal and financial affairs, and another to deal with health-care decisions. A financial power of attorney is used when you are living and not able to address your financial needs. Abuse of this power is also one of the strategies that generates elder abuse. These powers become vital if you are mentally or physically not able to care for your affairs; even your spouse cannot access accounts in your name alone without a power of attorney or a judges order.

- **Create a letter of instruction**. This document provides a list of instructions for your survivors to follow. For example, it can spell out funeral wishes, people to contact, and where your will and other key papers can be found. It also can provide information about your financial accounts and activities.
- **Create an Advance Health Care Directive (or Advance Medical Directive).** This allows you to state what you want for your own medical care if you are unable to make decisions for yourself. You can:

  – Direct that a specific procedure or treatment be provided, such as artificially administered hydration (fluids) or nutrition (feeding);

  – Direct that a specific procedure or treatment be withheld; or

  – Appoint a person to act as your agent in making health care decisions for you, if it is determined that you are unable to make health care decisions for yourself. This includes the decision to make anatomical gifts of a specific part or parts of your body via organ and tissue donation, or of all of your body.

  – A link to the 2012 Virginia Advance Directive Form—Simplified Basic can be found on the Bank On Virginia Beach blog at bankonvb.blogspot.com.

- **Create a list of financial accounts**. List account numbers and pertinent information about your investments, bank accounts, insurance policies (life, disability, homeowners, credit and life) and other financial matters.

Estate Planning *con't*

- **List the location of valuable documents**. Your list might include deeds, car titles, military records, birth and marriage certificates, divorce decrees and estate planning documents.

- **List your personal data**. This can include your Social Security number, driver's license number, VA claim number, your date of birth and the names and phone numbers of family members. Be sure to include the location of your tax records.

- **Make arrangements for access to your safe-deposit box**. In many states, safe-deposit boxes are closed upon death and are not opened until probate. Make sure copies of your will and other important documents are available outside of your safe-deposit box.

- **List loan payments**. This listing should include information about credit cards, mortgages, consumer loans, and auto and personal loans.

- **List other income sources and government benefits**. This includes pensions and Social Security. For information on military benefits, check with the Veteran's Administration or your nearest military installation's casualty assistance office.

- **Verify account ownership and beneficiary designations**. Check financial accounts and insurance policies to make sure these conform to your estate planning arrangements.

- **List all organizations in which you have membership**. They may provide special death benefits and should be noted for your survivors.

If you store any of this information on your computer, make a list of all passwords, indicate where any discs or thumbdrives are stored and where the information can be found.

Post-Test

1. 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

2. 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

3. 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

4. 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

5. 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
        a. Once you purchase insurance, there is no need to review or change your policy

Glossary

Deductible: the amount of expenses that must be paid by you before an insurer will pay any expenses.

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.

Extended Fraud Alert: The extended fraud alert requires a lender to contact you and get your approval before authorizing any new account in your name. This type of alert is only used when you know you are a victim of identity theft and is effective for seven years.

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

Initial Fraud Alert: A 90-day alert placed on your credit bureau file indicating you may have been a victim of fraud.

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., those by fire, accident, death, etc.).

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

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.

Security Freeze: restricts potential creditors and third parties from accessing your credit report unless you authorize the release of the security freeze.

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

Text Scams: When a criminal sends a text message to your cell phone under false pretenses to trick you into entering personal information with a bogus phone line or website so the criminal can use the information to raid your account.