Consumer Protection: How to Avoid the Latest Scams

EHC Lesson Guide

Dr. Laura Hendrix, Professor

Objectives:

- Participants will become familiar with common methods of consumer fraud, scams and identity theft.
- Participants will learn steps to protect their finances from fraud, scams, and identity theft.

Target Audience:

- EHC members
- Other adult audiences

Handout: Solve the Money Mystery. Common Cents: Protect Your Finances

Suggestions for Teaching:

- Review the lesson and handout.
- Obtain copies of the handouts and evaluation survey.
- If using the Power Point, practice your presentation using the Power Point.

Introduction

Fraud, scams, and identity theft are a danger to consumers. Identity theft is when someone uses your personal or financial information without your permission. They might steal your name and address, credit card or bank account numbers, Social Security number, or medical insurance account numbers. And they could use them to buy things with your credit cards, get new credit cards in your name, open a phone, electricity, or gas account in your name and steal your tax refund.

The Federal Trade Commission logged more than 1.1 million identity theft reports in 2024. The federal agency also received roughly 2.6 million cases of related fraud, with total losses of more than $12.7 billion.

Key findings include:

- Impostor scams, where criminals pose as trusted entities, made up the top-reported fraud category.
- Credit card abuse was the largest category of identity theft.
- More victims reported being contacted by email than any other method.

How it Happens

New schemes and scams are invited every day so it's impossible to give a list of every scam in existence at any given moment. Here is a list of some of the most common methods of identity theft. It's important for consumers to be on guard and protect their personal financial information.

- Cyberattacks – thieves hack systems, software, and servers in companies of all sizes. They may use the information to open accounts, make charges, or impersonate the business.
- Dumpster-diving – thieves can rummage through trash, looking for bills or other papers with your personal information on them.
- Identity theft – your name, Social Security number, bank account information, or credit card number used without your permission.
- Imposter scams – thieves try to convince you to send money by pretending to be someone you know or trust.
- Mail fraud – thieves may send letters asking you to send money or personal information.
- Phishing - a scammer tries to trick you into giving out your personal information, such as passwords, credit card numbers, or bank account information.
- Skimming – thieves can steal credit/debit card numbers by using a special storage device when processing your card.
- Spoofing - a caller disguises the information shown on your caller ID.
- Wire or money transfer fraud – thieves try to trick consumers into wiring or transferring money to them.

What can you do?

Fortunately, there are many steps we can take to protect ourselves from fraud, scams, and identity theft.

Don’t talk to strangers.

Don’t give out personal information unless you know who you are dealing with. Never click on links sent in unsolicited e-mails.

- Hang up the phone. Don’t respond to emails. If the call or email appears to be from your bank or other legitimate source, you can initiate the contact and find out if there is a true concern or need. For example – if you receive a call or email from someone who claims to be from your bank and wants your SS# or bank account numbers, don’t respond. Banks should already have this information. Call your bank and ask a representative if they called or emailed with the request.
- Never click links in suspicious emails or popups. Report them – some phones or email have a “report junk” or “report phishing” option that can be used to report suspect texts or email.
- National Do Not Call Registry - The National Do Not Call Registry is designed to stop unwanted sales calls from real companies that follow the law. It’s free to register your home or cell phone number. The Registry is a list that tells registered telemarketers what numbers not to call — but it doesn’t block calls. https://consumer.ftc.gov/national-do-not-call-registry-faqs
- Call Blocking - Some cell phones have a Call Blocking App. Check your app store and make sure you are using a legitimate app.

Protect your Social Security number. Don’t carry your Social Security card in your wallet or write the number on a check. Don’t give your Social Security number unless you know it is a legitimate request.

Use strong passwords. Get creative. Don’t use obvious passwords like your birth date, your mother’s maiden name or your Social Security number.

Verify with security questions. Use security questions to verify your account. Examples of security questions are: What was your maternal grandmother’s first name? What was the name of your first pet? What was the mascot of your high school?

Set up roadblocks online. Set up roadblocks online. Log out of accounts and close browsers. Use firewalls, spyware and anti-virus software. Update frequently.

Receive notifications. Allow notifications for log-in alerts. Set up notifications on bank accounts and credit cards. This can help you know if someone else is trying to access your account.

Shop reputable businesses. Shop at reputable businesses in-person or online. Comparison shop to make sure deals are really a good price. Keep records/receipts of your transactions.

When shopping online:

- read reviews
- check shipping rates and return policies
- Make sure websites use encryption (https)
- Monitor credit card or bank statements to be sure charges are accurate

Limit the cards you carry. Carry fewer cards in case your wallet or purse is stolen or swiped with a card reader. If a card-reading device looks as if it's been tampered with, don't swipe your card.

Protect Financial Information. Hide it. Keep personal information in a secure place at home, especially if you have roommates, employ outside help or are having work done in your house. This could include birth certificates, social security cards, marriage or divorce decrees, citizenship papers, adoption papers, death certificates, tax returns, vehicle titles, property deeds, etc.

Shred financial documents, paperwork, and mail with personal information before you discard them – shred anything that has personal/financial information, credit offers, credit card statements, ATM receipts, etc.

Some financial documents may need to be kept for a period of time for tax purposes.

Monitor accounts.

Monitor accounts and your credit report. View account information online and/or sign up for text alerts. Check your credit report at www.annualcreditreport.com. Contact the bank, credit union, creditor(s), and/or credit bureau(s) if you notice anything suspicious.

Contact the credit reporting bureau (Trans Union, Equifax, or Experian) if you see something incorrect on your credit report.

Credit Freeze and Fraud Alert are two types of protections consumers can put in place to help protect their credit.

Credit Freeze

- What it does: While a credit freeze is in place, nobody can open a new credit account in your name, including you. If you need to do things like apply for new credit or a job, rent an apartment, or buy insurance, you can temporarily lift the freeze and put it back when you're done.

- A credit freeze is always a good idea, but it's even more important if your Social Security number or other information is exposed in a data breach or if an identity thief has misused your information.
- Who can place one: Anyone can freeze their credit report, for any reason, even if their identity hasn't been stolen.
- How long it lasts: A credit freeze lasts until you lift it.
- Cost: Free
- How to place one: Contact all three of the credit bureaus — Equifax, Experian, and TransUnion.
- When to lift one: Contact the bureau(s) to request it be lifted when you need lenders to access your credit. It is a good idea to identify which bureau a lender will use to check your credit and just lift the freeze at that one bureau and then put the freeze back in place once the need for a credit check passes.

Fraud Alerts

Even if you already have a credit freeze in place, you can also place a fraud alert. Fraud alerts make lenders verify your identity before they grant new credit in your name. There are two types of alerts, and which is best depends on your situation and needs.

Initial fraud alert - An initial fraud alert tells businesses to check with you before opening a new credit account in your name. Usually, that means contacting you first to make sure the person trying to open a new account is really you. Unlike a credit freeze, a fraud alert doesn't prevent businesses from seeing your credit report.

- Who can place one: Anyone who is or suspects they may be affected by identity theft. When you place an initial fraud alert on your credit report, you can get a free copy of your credit report from each of the three credit bureaus.
- How long it lasts: An initial fraud alert lasts one year, but you can renew it.
- Cost: Free
- How to place one: Contact one of the three credit bureaus — Equifax, Experian, and TransUnion. You don't have to contact all three. The credit bureau you contact must tell the other two to place an initial fraud alert on your credit report.

Extended fraud alert - Like an initial fraud alert, an extended fraud alert tells businesses to check with you before opening a new credit account in your name and doesn't prevent businesses from seeing your credit report. An extended fraud alert also requires the credit bureaus to take you off their marketing lists for unsolicited credit and insurance offers for five years, unless you ask them not to. Only people who have experienced identity theft and have completed an FTC identity theft report at IdentityTheft.gov or filed a police report can file an extended fraud alert. It lasts for seven years.

Signs you may be a victim. How will you know if you have been a victim of a fraud, scams or identity theft? It's important to find our as soon as possible to give thieves less time to rack up charges or drain your accounts. Here are a few questions to ask yourself?

- Are there charges or bills from creditors or collection agencies demanding payment for items that you never bought or for accounts that you never opened?
- Is there information in your credit report about accounts that you never opened?
- Are there calls from creditors, or potential creditors, about suspicious new accounts, a large volume of credit card activity, wire transfers, etc.?
- Have there been unauthorized withdrawals from your bank accounts?
- Has your wallet, purse, laptop, iPad or cell phone been lost or stolen?
- Are your statements, bills, or other regular mail not arriving on time as regularly scheduled?
- (Your mail may have been diverted to another address or stolen from your mailbox.)
- Have you had a surprise credit score drop or denial of loan or credit applications?

What to do if you think you have been a victim of fraud, scams, or identity theft.

Contact your bank or credit card company if you notice anything suspicious.

Contact the credit reporting bureau (Trans Union, Equifax, or Experian) if you see something incorrect on your credit report.

Contact the lender or credit card company if there are charges you didn't make or accounts you didn't open.

File a police report if your wallet, purse, or electronic device are stolen.

To report identity theft, contact:

- The Federal Trade Commission (FTC) online at IdentityTheft.gov https://www.identitytheft.gov or call 1-877-438-4338
- The three major credit reporting agencies. Ask them to place fraud alerts and a credit freeze on your accounts.
- The fraud department at your credit card issuers, bank, and other places where you have accounts

- If you believe you have experienced tax-related identity theft but have not received a notification from the IRS about it, learn about filing Form 14039. Completing the Identity Theft Affidavit will invalidate a fraudulent return filed using your information.

Contact the Arkansas Attorney General's Office- The Consumer Protection Division assists Arkansas consumers when problems arise during consumer transactions. Attorney General staff may help by contacting a business and mediating a positive resolution. In other instances, attorneys pursue lawsuits against those who violate the Arkansas Deceptive Trade Practices Act. Antitrust laws are designed to promote healthy competition among businesses and thereby ensure consumer choice. When companies collude to set prices or affect a fair marketplace, consumers often pay the price. The Attorney General's office investigates and prosecutes alleged violations of the State and federal antitrust laws. Those laws are premised on two basic requirements: companies cannot agree to limit competition in ways that hurt consumers, and a single company cannot monopolize or try to monopolize an industry through unfair practices. Email consumer@ArkansasAG.gov or call 800-482-8982. File a consumer complaint online: https://arkansasag.gov/file-a-complaint

Closing

If you become a victim, you may spend a large amount of time closing compromised accounts, opening new accounts and fixing credit records. There can be out-of-pocket expenses related to clearing your name. You could even be denied loans because of identity theft. Take steps now to protect yourself from fraud, scams, and identity theft.

Please complete the evaluation.

References

- Federal Trade Commission Consumer Advice, https://consumer.ftc.gov/
- Consumer Financial Protection Bureau, Fraud and Scams, https://www.consumerfinance.gov/consumer-tools/fraud/
- USA.gov Fraud and Scams, https://www.usa.gov/scams-and-fraud