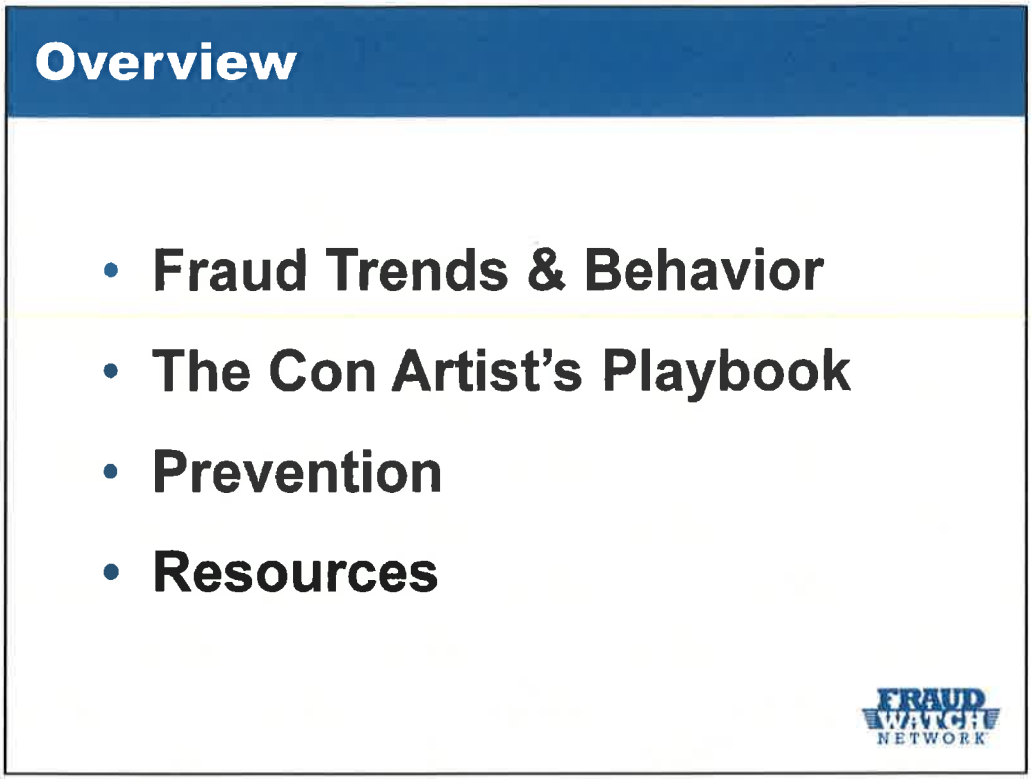
Identity theft, investment fraud and scams rob millions of Americans of their hard-earned money.

We are here as volunteers for AARP New Hampshire. AARP New Hampshire has an office in Concord and serves its 225,000 members and their families statewide. For more than 50 years, AARP has been serving our members. AARP's mission is to enhance the quality of life for all as we age, leading positive change and delivering value to people 50+ and to society through **advocacy**, **service** (Tax Aide, Driver Safety Program, Local Discounts), and **information** (consumer protection, Medicare, Social Security).

AARP is launching the Fraud Watch Network to give people the resources to spot and avoid ID theft and fraud so they can protect themselves and their families. Non-members and members alike can get watchdog alerts, stay up to date on the con artists latest tricks, or talk to a real live person for help. Anyone interested in this information can access it free of charge. We're also training volunteers just like you so you can coach people on how to avoid fraud.



To help you protect yourself and your loved ones, today we are going to look at:

- **Fraud Trends and Behavior** – Understanding how much fraud is out there and the behaviors that put you at risk.
- **The Con Artist's Play Book** – Understand the strategy and tactics used by con artists to defraud.
- **Prevention** – Know and practice the most effective prevention strategies to avoid becoming a victim, recognize the "red flags" & report.
- **Resources** – How to access and share up-to-date information about fraud identification and prevention and where to go if you or someone you love has been a victim.

Florida ranked number one in the nation for identity theft & fraud reports to the Federal Trade Commission. The top categories for frauds and scams reported to the FTC in 2012 here in **New Hampshire** fell into these **top 3 categories:**

- **Identity theft**: State laws typically define Identity Theft as the intent to use another's identity for any unlawful activity without the authorization, consent, or permission of the victim, and with the intent to defraud.
- **Debt collection:** Things like when a debt collector calls repeatedly or continuously, misleads you on the amount owed or current status of the debt, falsely threatens to sue, or uses profane language & threats.
- **Banks & Lenders:** Deceptive or predatory mortgage lending practices; problems with modification of mortgage terms; miscellaneous customer service and account issues with bank products, including fees and overdraft charges; etc.

Also, **phone & Internet scams** are also quite prevalent in NH. (ex: "Grandparent scam", "You've Won ... whatever.....", 876 Area code fraud, etc.)

Each year, more than 12 million Americans are struck by identity theft which has been the top consumer complaint to the FTC for 13 consecutive years. And according to a recent study by FINRA, over $50 billion is lost per year as a result of financial fraud.

Identity theft occurs when someone steals personal information that could be used to falsely apply for credit or for government benefits. A recent study by Javelin Strategy & Research found that Identity theft alone affected 12.6 million victims in the US in 2012, which means every 3 seconds someone's identity is stolen. These cons managed to steal almost $21 billion dollars last year. **Identity fraud is the number one category for reported frauds across the United States,** and for good reason – it can happen to anyone, anytime.

The numbers you see on this slide account for Identity Theft alone. The total effect of all Frauds and Scams been estimated in the past by the Federal Trade Commission to affect some 25 Million Americans each year.

Americans age 65 and older are more likely to be targeted and 34% more likely to lose money once targeted than those in their 40s.

Fraud Trends & Behavior

Identity Theft

✓**Phishing**

✓**Stealing Mail**

✓**Bogus Job Offers**

✓**Social Media**

FRAUD WATCH NETWORK

INSERT ID THEFT STORY…..

Here are three common ways con artists steal your identity:

- **Phishing** – Someone contacts you via email and says there is some problem with your bank account/Medicare account/ credit care account, etc. and you need to verify the account with a Social Security Number, bank routing number or birth date. During this time of year, they may say they are with the IRS.
- **Stealing mail or sensitive documents** – Personal information is taken from your trash, your office or from social media websites or even your mailbox and used to steal your identity. Blank credit card application forms should also be destroyed before throwing away.
- **Bogus job opportunities** – Con artists post bogus job offers on various employment websites, requiring forms to be filled out or requesting you call or send a complete résumé. The scammer may use or sell your personal information provided in the job application.

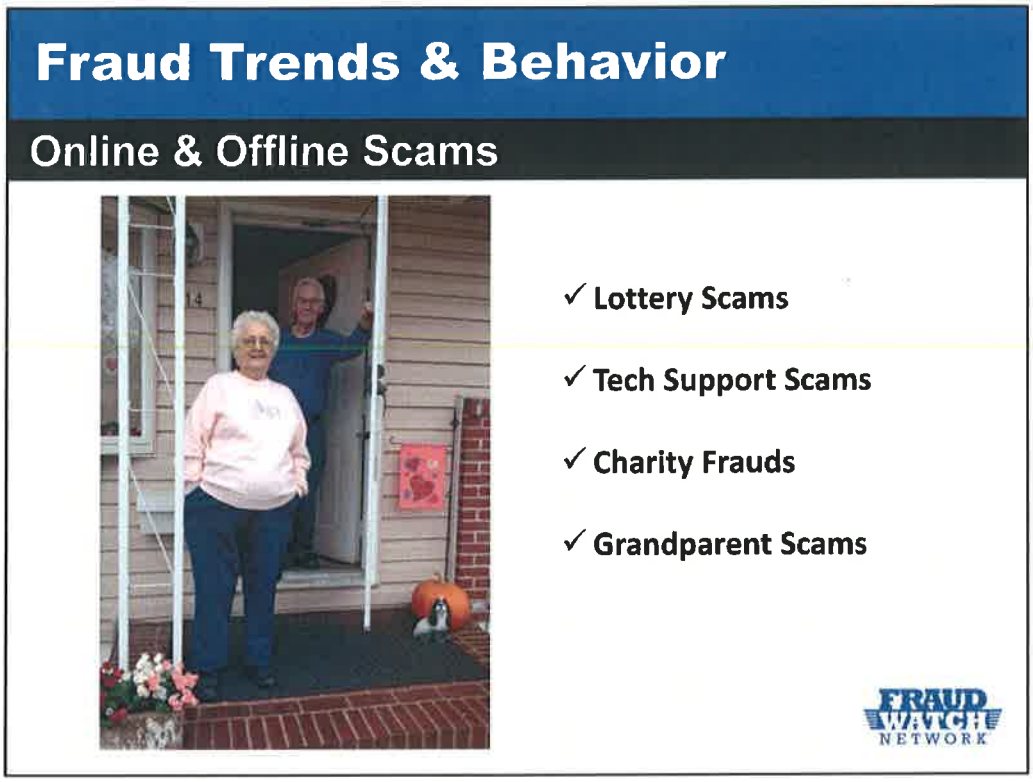
Investment fraud is another very common scam to be on the look out for.

Meet Steve. He is 58 years old, married, makes more than $50,000 per year, has a BA and a master's degree...and he is a professional stock broker. He lost $40,000 to a fraudulent oil and gas operation out of Dallas, Texas.

Other common investment frauds include:

- Gold Coins – You hear an ad on the radio that describes how the world economy is shaky and the only thing you can really rely on during periods of economic uncertainty is precious metals. You call a toll-free number and are pitched on buying gold and silver coins that will undoubtedly go up significantly in value. What you are not told is that the coins are being sold at a 300-500% mark up and you will lose money the minute you buy them.

- Some free Lunch Seminars - The scammer invites a hundred people to a seminar, where he or she presents an unbeatable investment opportunity. You must sign up right then and there. You can't sign up later because he or she is leaving town in two hours, and so will your money.



In addition, there are a wide variety of online & offline scams that you need to protect yourself and your loved ones from. One of the bigger scams making the news today is lottery scams.

Jean was one such victim. Jean received a call from a man in Jamaica who told her she had won the $7.9 million dollar Jamaican lottery. All she had to do was pay the taxes to collect. Over a six-month period, this man called Jean hundreds of times and convinced her to wire over $30,000 in taxes and processing fees to Jamaica.

Other common scams to be on the look out for are:

- Tech Support Scams – You receive an email or phone call claiming to be from the Microsoft Corporation and they claim there is a problem with your computer and they need to install an anti-virus program for $99. You are then led to a website where the con "proves" there is a problem. Afraid of what will happen if you don't take action, you allow the con to take remote control of your computer and they actually install a virus and charge you for it.
- Disaster-related Charity Fraud – Every time there is a major natural disaster somewhere in the country, scammers come out of the woodwork sending emails to raise money for the victims of the disaster. You think the money is going to help victims, but it is really going to line the pockets of a criminal.
- Grandparent Scams – You receive a call from a someone posing as a law Enforcement Officer or your grandchild indicating that they have been arrested and need $ ASAP for bail; they don't want their parents to know, etc.
- 876 Area Code Scams – Call from Jamaica area code re: winning the lottery. (Just like Jean.) Need to pay processing fee. Say the have someone in the area ready to give you your check as soon as you send the fee. Calls are often abusive and threatening if you do not pay the fees.
- Travel Scams – You receive a solicitation saying you can enjoy steep discounts on travel to many parts of the world by joining a travel club - for a fixed fee that is often in the thousands of dollars. You find out later that the discounted fares for cruises and other travel were either not as low as represented or not available.

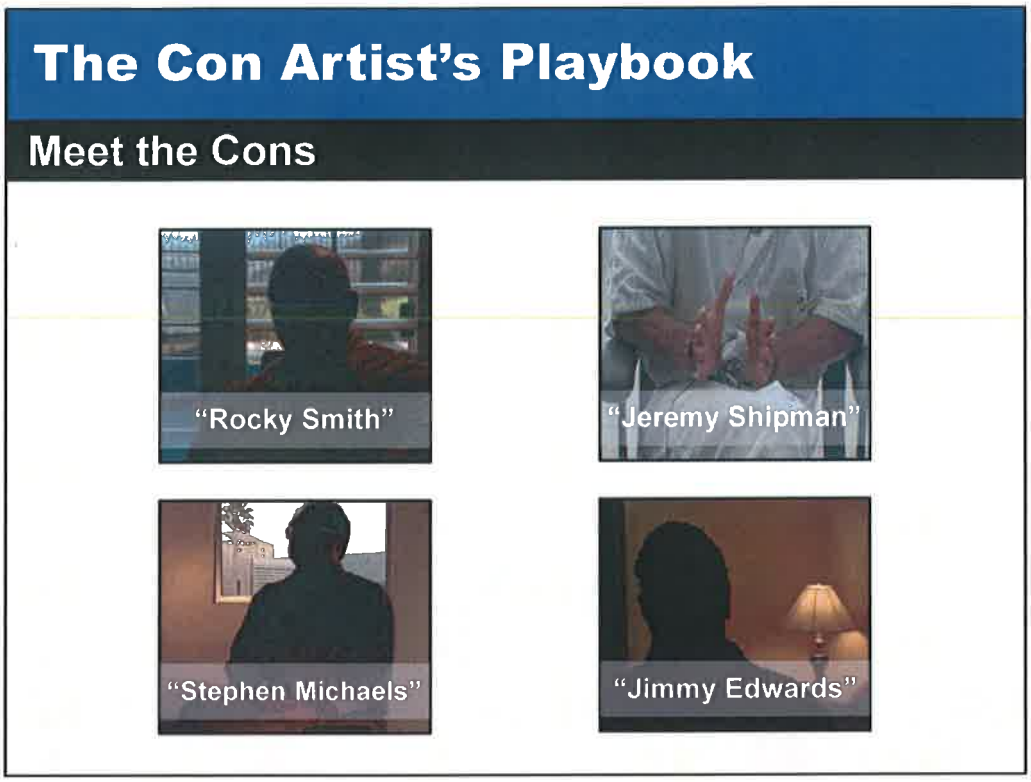
- E-mails you didn't solicit asking you to "click" on links within the e-mail; don't do it!

The Con Artist's Playbook

Where did the insights come from?

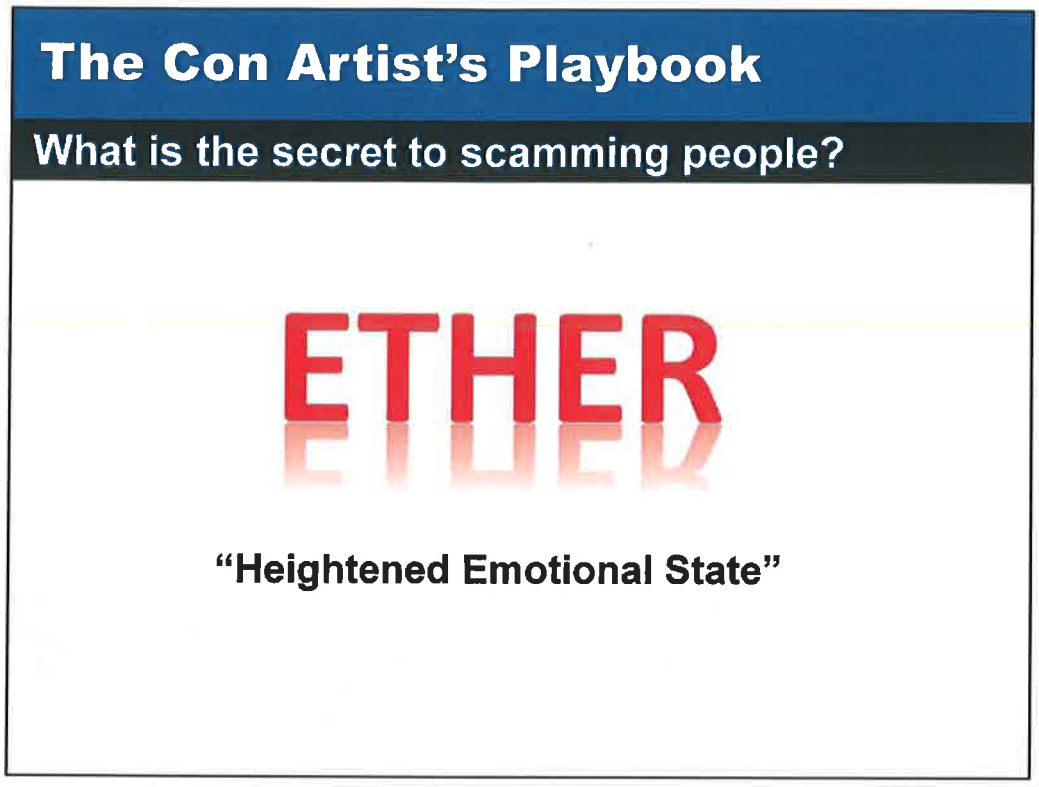
Now, we'd like to help you get inside of the minds of these fraudsters by taking a look at the "Con Artist's Playbook".

The two key sources for understanding how fraud works have been jail house interviews with convicted con artists and analysis of hundreds of undercover audiotapes provided by law enforcement.



Here is a snapshot of **some of the con artists we have interviewed** over the years:

- **Rocky Smith worked as a consultant – training con artists** - in numerous fraudulent boiler rooms in the 1980s and 1990s (boiler rooms are where con artists gather and together dial for their next victims.)
- **Jeremy Shipman worked in numerous gold coin scam rooms** over a five-year period.
- **Stephen Michaels owned multiple fraud boiler rooms** over a career that spanned 20 years.
- **Jimmy Edwards** was kind of the star of the scammers, **having worked in over 30 boiler rooms over an eight-year period**.



When authorities ask convicted con artists to describe the trick to scamming people out of their money, they all say the same thing: "Get them under the ether."

So what is ether? **Ether is a heightened emotional state that makes it hard to think clearly and make rational decisions**. Think about the first time you fell in love. Were you thinking clearly? Probably not.

Here's how Rocky described it: "I wanted to keep the victim up in the altitude of the ether, because once they drop into the valley of logic, I've lost them."

So how do they get you to that point?

The Con Artist's Playbook

Persuasion Tactics

- **Phantom Riches**
- **Profiling**
- **Scarcity**
- **Source Credibility**
- **Fear & Intimidation**

We received over 500 undercover audiotapes made by law enforcement between 1995 and 2010. **We coded them to see which persuasion tactics were used most by cons.** Let's take a closer look at **the five most common tactics** identified by cons.

The Con Artist's Playbook

Phantom Riches

"I have a check for you for $232,000 that I have been holding for over a year now."

"And the grand prize is $25,000 in cold, hard cash."

"The Florida lottery is up to $30 million dollars this Saturday night! If you join our club, you will have 4,800 tickets – that's 4,800 chances to win."

Phantom riches are something you want, but can't have. These claims of unlimited wealth are designed to get your ether up, to get you so aroused by the prospect of these **huge returns** that you can't think of anything else and your logical reasoning goes out the window. Researchers **say this is the number one tactic** found in undercover audiotapes of con pitches. Jeremy sold over priced coins to seniors. He describes the use of phantom riches this way. "We would tell people that gold would absolutely double in value in the next one to two years and that the prospect would be able to rely on it making them far more money than any other investment vehicle."

Note: A good place to mention the "If it sounds too good to be true, it probably isn't true!" rule.

The Con Artist's Playbook

Profiling

"If you don't mind my asking, how long has your husband been deceased?"

"Let me ask you something. It sounds like you have a wonderful home there. How much is that mortgage each month?"

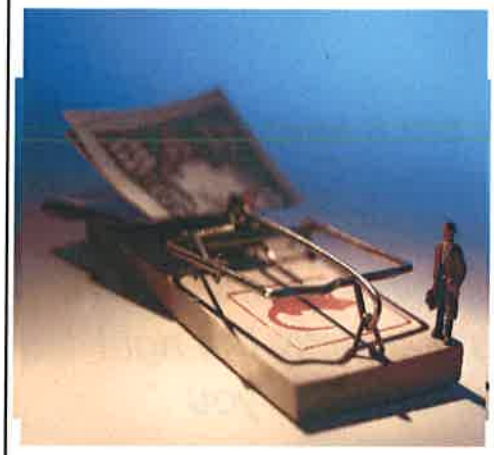
Scammers will develop a victim profile **by asking a series of personal questions so he or she can find your emotional trigger.** Once they know what your emotional trigger is, then they know which tactics will work with you. Here is how Jimmy describes the con artists' use of profiling to scam people.

"The con gathers an arsenal of information **by being personable and being friendly**. They are making notes: Two children, one with a mental illness, one brother lost in Vietnam. They're using all that information to put together their arsenal and profile the person they are on the phone with so they know which buttons to push to bring the emotion up in that person. **When I wrap that in tons of emotion, the logic goes out the window, the emotion kicks in, now I've endeared you to me, now I'm no longer the predator on the phone, I'm Jim from New York."**

Presenter could also talk about why they target the elderly: often have a nest egg or need more money, lonely, trusting & polite (won't hang up), generally make poor witnesses, less likely to report (ashamed of being duped).

The Con Artist's Playbook

Scarcity



"We only have four units left on this investment offer so you need to make a decision soon or you will miss out."

"You were one of only 17 people selected to win the grand prize."

"There are only 24 hours left before this offer will expire, so you have to act now."

How many of you have seen going out of business sales that seem to last forever? Or "one-day only" sales that happen every other week?

Scarcity sells because it taps into our evolutionary fear of running out of food and water. When you think there is a limited supply of something, you rush to get it. So the con artist will try to paint a picture that what they have to offer is rare or available only for a limited time. Here is how Stephen used the scarcity tactic.

"Now John, back in 1860 from the Philadelphia mint, there were 22,625 of these coins minted. Of those 22,000, only 4 have survived. Only four for God's sakes, just four remain and are available only from me."

By claiming that there are only four coins left, he gets you to start panicking that if you don't buy now, you may never be able to again.

The Con Artist's Playbook

Source Credibility

"I am a senior vice president here with an MBA and certified to deal with seniors, and I believe this is exactly the right product for you ."

Con artists often try to **build credibility** by using a well-known celebrity, appearing successful, claiming affiliation with a reputable organization or touting a special credential or experience. Sometimes they even use a well respected individual from your church or organization (unbeknownst to them) to gain credibility.

The **IRS** is perhaps the government agency most commonly mimicked in fraudulent attempts to get your personal information. They may even claim to be with Medicare, Social Security or your medical provider. Keep in mind that federal and state agencies will not "call" you or "e-mail" you, unless you contact them first. If they need information or verification from you, they will typically snail mail you.

Another very common scam is for the con artist to claim to be from **Microsoft** in an attempt to gain access to your computer.

The Con Artist's Playbook

Fear & Intimidation

"Once I got a hold of a victim, I would never let go. Even when they told me they were out of money, I would never let go. Go borrow the money."

The use of fear and intimidation is a tactic that has emerged in recent years to badger you into handing over money. It is not uncommon for some con artists from other countries to **call a potential victim 50-60 times a day** to get them to invest.

Remember Jean's story from earlier – the one about lottery fraud? Well, when Jean finally stopped answering her phone, he left voice mail messages on her answering machine:

"Why you don't want to pick up the [bleep] phone?. Pick up the [bleep] phone when I am calling you and stop playing games with me. I know where you live; do you want me to come over there and set your home on fire?"

The Grandparent Scam is also an example of the "fear & intimidation" tactic.

Debt Collectors use this tactic as well.

Prevention Strategies

What Cons Agree On…

Victims:

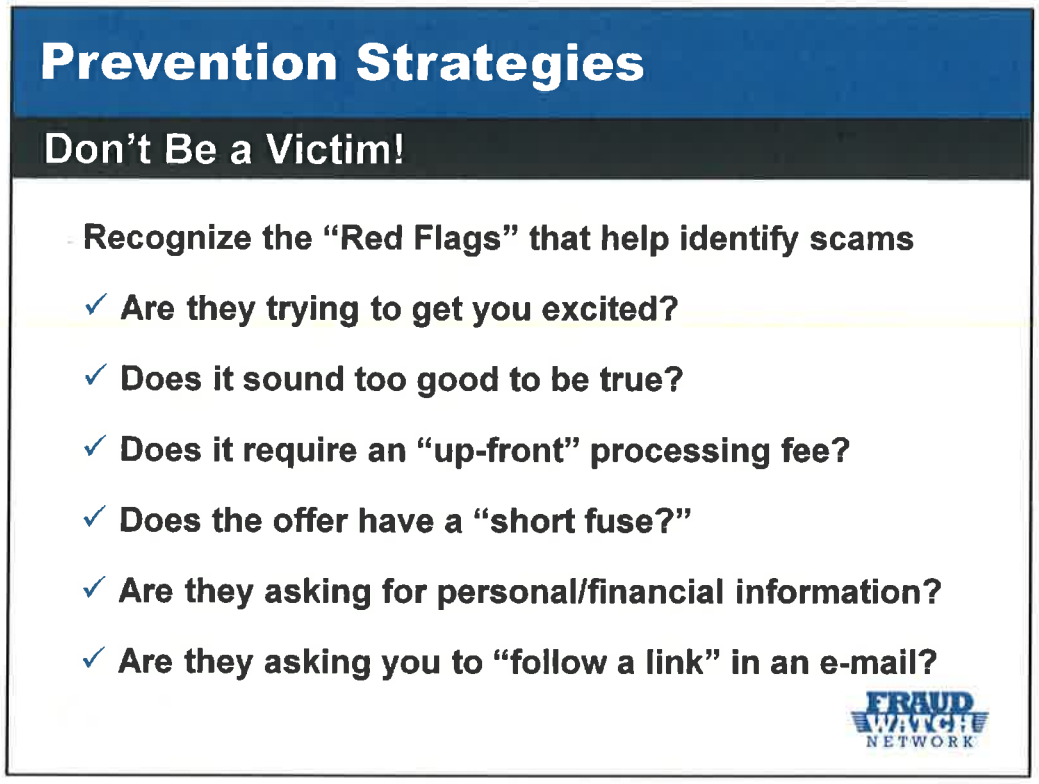
- ✓ **Get Excited Easily**
- ✓ **Don't Consider Why it's a Scam**
- ✓ **Don't Ask Questions**
- ✓ **Don't Read Information**

FRAUD WATCH NETWORK

So now that we know how scammers think, **let's take a look at what you can do to protect yourself and your family against identity theft and fraud.**

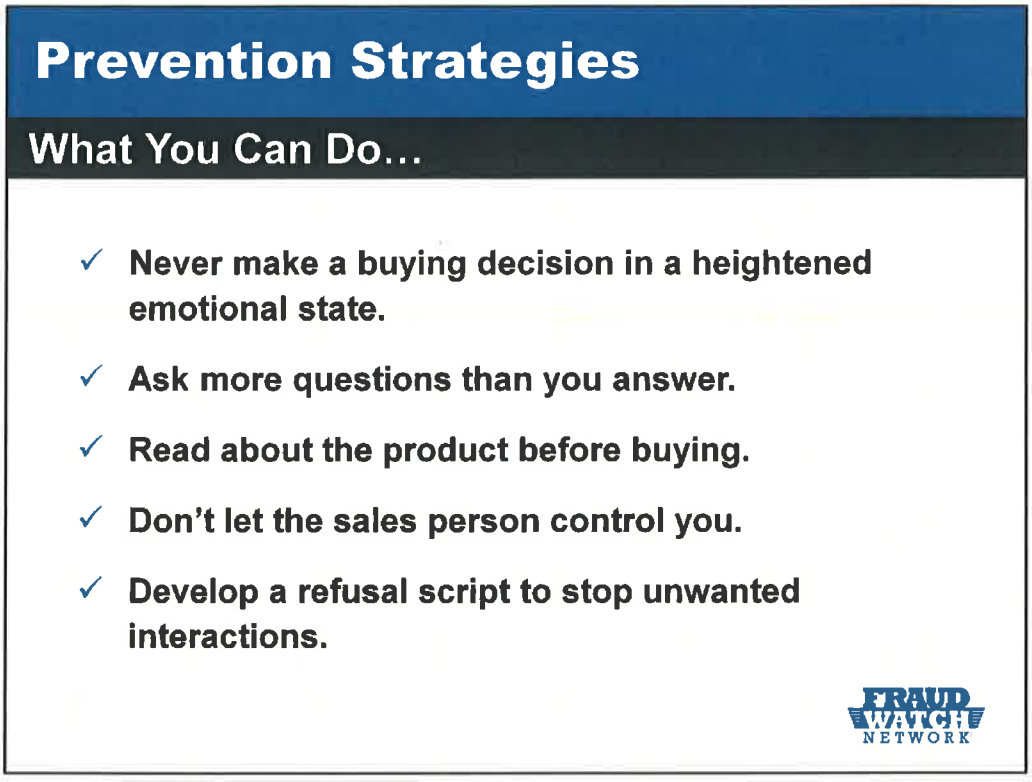
All con artist's agree that victims:

- Get excited easily & act on impulse.
- Don't consider why this offer could be a scam, instead they are looking for why it will make them money.
- Don't ask questions, they answer questions.
- Don't read information - they rely on the salesman to tell them what it says.



If you can recognize the "Red Flags" you can generally avoid being scammed.

- Are they using one of the previously discussed tactics such as trying to get you excited about the offer?
- If it sounds too good to be true it probably isn't true. The "free" item should really be free. If there are processing fees, shipping or handling, avoid it.
- Free is "Free" and should not involve an up front processing fee; if the offer does, avoid it and the fees may be never ending!
- Truly legitimate offers don't have a "short fuse" and you should be allowed to "check something out" or "request additional written information" on it without losing out on the offer. If they won't allow time for this; avoid it.
- Legitimate institutions will not ask for you to provide personal/sensitive and/or financial information over the phone or via e-mail. (Please note that I did not say "Internet" as there are various secure internet sites that are fine to use. Look for the padlock and/or "https" in the website address.)
- And so on....



There are a number of things you can do to protect you and your loved ones from the tactics that con artists use.

- ✓ **Never make a buying decision in a heightened emotional state.** Stay calm; excitement is exactly what they want.

- ✓ **Ask more questions than you answer.** Don't let them control the conversation. If the offer is truly legitimate, they will be willing to answer your questions and there won't be a "short fuse" to the offer.

- ✓ **Read about the product before buying.** If you are really interested, ask for information to be sent to you regarding the offer/product/trip, etc. Again, if legitimate they should be willing to send you information without saying that you will lose the "opportunity." If it is a Charity you are not familiar with or question, wait and check it out on a Charity review website before you pledge.

- ✓ **Don't let the sales person control you.** If you really don't want to hear what they have to say, feel free to say that you are really not interested and hang up.

- ✓ **Develop a refusal script to stop unwanted interactions.** I have an outline I follow for calls for charitable contributions where I ask questions of the caller. (ie: what % of my contribution would actually go to the cause? Is the caller from the organization or are they a firm hired to solicit contributions? etc.) Suggest that

the group/senior center might want to develop a refusal script for its members.

Prevention Strategies

What You Can Do...

- **Protect Your SSN & Personal Information**
- **Monitor Your Bills & Financial Accounts**
  - **finra.org/brokercheck & sec.gov**
  - **800-289-9999**
- **Watch Over Your Credit Reports**
  - **annualcreditreport.com**
  - **877-322-8228**

FRAUD WATCH NETWORK

You can also take these steps to protect you and your loved ones from online and offline identity theft and fraud:

- Protect Your Social Security Number (SSN), Medicare card & Personal Information
  - Don't carry your Social Security card or Medicare card in your wallet.
  - Don't print your SSN or driver's license number on your checks.
  - Shred sensitive information including medicine bottle labels.
  - Limit the number of credit cards you carry.
  - Keep copies of credit cards (front and back) in a safe place in case a card is lost or stolen.
- Monitor Your Bills & Financial Accounts
  - Watch for missing bills and review your monthly statements carefully. Contact your creditors if a bill doesn't arrive when expected or includes charges you don't recognize.
  - Don't invest in anything you are not absolutely sure about. Do your homework on the investment, company, and salesperson to ensure they are legitimate. Look them up at finra.org/BrokerCheck and sec.gov.
- Watch Over Your Credit Reports
  - You are entitled to one free credit report each year from each nationwide credit bureau. To get your free report, go to annualcreditreport.com or call 1-877-322-8228.

- Protect Personal Identification Numbers (PINS) & Passwords
  - Don't carry your PINS and passwords in your wallet or purse.
  - Avoid using easily available information for your PINs or passwords such as your mother's maiden name, your or a family member's birth date, your SSN or phone number, or a series of consecutive numbers (i.e., 1, 2, 3, 4).
  - Choose a different PIN for each account.
- Protect Your Information Online
  - Beware of emails that claim to come from a bank, Internet Service Provider, business or charity and ask you to confirm your personal information or account number. If you receive one that is suspicious, forward the email to spam@uce.gov.
  - Avoid conducting personal or financial business on shared/public computers or over public wireless hotspots.
  - Install the latest version of established anti-virus software.
  - Make sure websites are secure, especially when shopping online. A secure website will begin with "https" not the usual "http."
- Protect Your Mail
  - Call 1 (888) 5-OPT-OUT or visit optoutprescreen.com to stop pre-approved credit card applications that a thief could steal and use to get credit in your name.
  - Place outgoing mail into a locked mailbox such as a blue postal service box.

- Don't leave incoming mail sitting in an unlocked mailbox. (esp. during Tax season!)
- Cut down on junk mail by contacting the Direct Marketing Association at dmachoice.org.

Prevention Strategies

What You Can Do...

- Sign Up for Do Not Call Registry
  - donotcall.gov or 888-382-1222
- Double-Check References
- Verify Charities
  - charitywatch.org
  - charitynavigator.org

FRAUD WATCH NETWORK

Be Cautious of Scams & Frauds:

✓ **Never give personal information** to telemarketers who call you on the phone. To cut down on unwanted telemarketing calls, sign up for the Do Not Call Registry at donotcall.gov or call (888) 382-1222.

✓ **Double-check references** for door-to-door sales, home repair offers and other products. Verify that businesses and others who contact you are who they claim to be before you provide any personal information. If you think the request for information is legitimate, contact the company at a number you know is valid to verify the request.

✓ **Check out a charity before donating** to make sure they are legitimate at charitywatch.org or charitynavigator.org to see what type of a rating they have. (Note: to legally be classified as a "charity organization" they only need to spend 1% of what they collect for the actual "cause"! The other 99% can go toward fundraising and Administration. (I prefer to donate to organizations that spend

about 80% or more toward the actual “cause”; you may feel differently.)

Prevention Strategies/Resources

Fraud Watch Network

aarp.org/fraudwatchnetwork

- **Access Information & Resources**
- **Receive Watchdog Alerts**
- **Hear Stories**
- **Get Help & Report**

FRAUD WATCH NETWORK

AARP's Fraud Watch Network is a go-to resource for everyone, whether or not you're a member. On aarp.org/fraudwatchnetwork, you'll find:

- **Information and resources**: Anyone interested in learning what to look out for can access our information and resources for free.
- **Watchdog Alerts**: Stay up to date on the latest scams and get access to a network of people who can show how to avoid being scammed. As criminals develop new ways to target victims, we'll provide you warnings and critical information so you can always be on your guard.
- **First-hand accounts from victims**: Hear stories from victims who will share their experiences to help you protect your hard-earned money and show you what it takes to recover if you've been defrauded.
- **One-stop Resource for Getting Help**: Find out what to do if you or someone you know has been victimized.
- **Contacts to get additional information or Report** suspected or attempted Frauds/Scams to your local police and others as may be appropriate.

Become part of this Fraud Watch Network by passing this information along to others who might need it as well.

Calling this number will take you to the **Fraud Fighter Call Center** where highly trained AARP volunteer Fraud Fighters are standing by to offer **peer counseling, support and referral services** to fraud victims and their family members.

If no computer access, call toll-free: **1-877-908-3360**.

Call you local Police Department and let them know what has happened.

You can also call the NH Attorney General's office, explain why you are calling and they will connect you with the appropriate bureau or send you a complaint form.