

Better Brain Fridays

Keeping You Safe:
Understanding Fraud and Scams for
Better Brain Health

A person is holding a smartphone in their right hand. The phone's screen shows a white padlock icon at the top, indicating it is locked. Below the lock, a numeric keypad is visible, with the number '1' being the most prominent. The background is a blurred laptop keyboard and a document, suggesting a workspace or office environment.

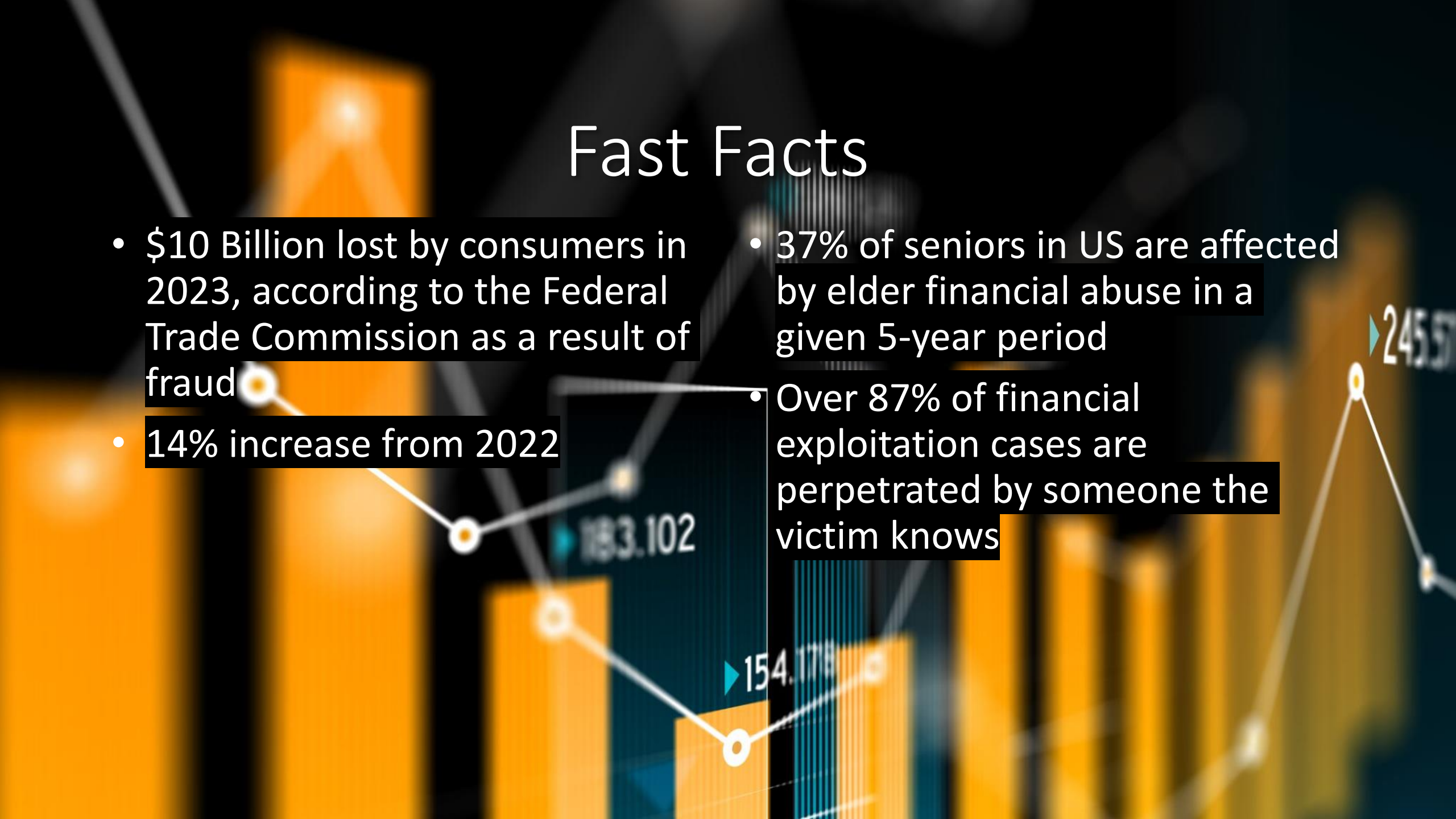
- Fraud Manager – Royal Credit Union
- APRP – Accredited Payments Risk Professional
- Certified Financial Counselor – CUNA
- Certified Fraud Specialist – BankerCollege Professional Certification
- 12 years in Credit Union Industry



A photograph of an elderly couple embracing outdoors. The man, bald and wearing a light grey cardigan over a blue and white striped shirt, is kissing the woman on the cheek. The woman has short white hair and is wearing a light-colored top. They are standing in front of a dense green background, possibly a willow tree. The text "Grandpa Paul" is overlaid in white, centered on the image.

Grandpa Paul

Fast Facts

- \$10 Billion lost by consumers in 2023, according to the Federal Trade Commission as a result of fraud
 - 14% increase from 2022
 - 37% of seniors in US are affected by elder financial abuse in a given 5-year period
 - Over 87% of financial exploitation cases are perpetrated by someone the victim knows
- 
- The background features a stylized data visualization. It includes several vertical orange bars of varying heights. A white line graph with circular markers is overlaid on the bars, showing an upward trend. Some data points are labeled with numbers: 183.102, 154.178, and 245.5. The overall aesthetic is modern and professional, using a color palette of orange, white, and dark blue.

Scams and Trends

[Home Repair Scams \(ftc.gov\)](#)

[Health Insurance Scams \(ftc.gov\)](#)

[Grandkid and Family Scams \(ftc.gov\)](#)

[Business Impersonator Scams
\(ftc.gov\)](#)

[Pass It On "You've Won" Scams
\(ftc.gov\)](#)



Home Repair Scams

Here's how they work:



Someone knocks on your door or calls you. They say they can fix your leaky roof, put in new windows, or install the latest energy-efficient solar panels. They might find you after a flood, windstorm, or other natural disaster. They pressure you to act quickly and might ask you to pay in cash or offer to get you financing.

But here's what happens next: they run off with your money and never make the repairs. Or they do shoddy repairs that make things worse. Maybe they got you to sign a bad financing agreement that puts your house at risk.

Here's what to do:

- 1. Stop. Check it out.** Before making home repairs, ask for recommendations from people you trust and check that the companies have licenses and insurance. Get three written estimates. Don't start work until you have reviewed and signed a written contract. And don't pay by cash or wire transfer.
- 2. Pass on this information on to a friend.** You may see through these scams. But chances are, you know someone who could use a friendly reminder.



Health Insurance Scams

Here's how they work:



You get a call or see an ad offering you big discounts on health insurance. Or maybe someone contacts you out of the blue, says they're from the government, and asks for your Medicare number to issue you a new card.

Scammers follow the news. When it's Medicare open season, or when health insurance is a big story, scammers get busy contacting people. They want to get your Social Security number, financial account numbers, or insurance information.

Think about these questions. Is that discount insurance plan a good deal? Is that "government official" really from the government? Do you really have to get a new health insurance card? The answer to all three is almost always: No.

Here's what to do:

- 1. Stop. Check it out.** Before you share your information, call Medicare (1-800-MEDICARE). Do some research, and check with someone you trust.
- 2. Pass this information on to a friend.** You probably know about these scams. But you might know someone who could use a friendly reminder.



Grandkid and Family Scams

Here's how they work:



You get a call: “Grandma, I need money for bail.” Or maybe an email from someone claiming to be your brother or a friend who says they’re in trouble. They need money for a medical bill. Or some other kind of emergency. The caller says it’s urgent — and tells you to keep it a secret.

But is the caller who you think it is? Scammers are good at pretending to be someone they’re not. They can be convincing: sometimes using information from social networking sites, or hacking into your loved one’s email account, all to make it seem more real. And they’ll pressure you to send money before you have time to think.

Here's what to do:

- 1. Stop. Check it out.** Look up your family member’s phone number yourself and call another family member to check out the story.
- 2. Pass this information on to a friend.** You may not have gotten one of these calls, but chances are, you know someone who will get one — if they haven’t already.



Business Impersonator Scams

Here's how they work:



You get a call, email, text, or message on social media that looks like it's from a business you know. It says there's a problem with your account, or you won a prize. It tells you to call a number or click a link.

But the message isn't really from a familiar business, it's from a scammer. If you call, they'll tell you to send payment or give personal information. They'll say you must pay with gift cards, cryptocurrency, or by wiring money, which no honest business will do. Or they'll ask for your Social Security number or access to your computer.

But it was never really that business contacting you, there wasn't a problem, and there was never a prize.

Here's what to do:

- 1. Stop.** If you get an unexpected call, email, text, or message on social media — even if it looks like it's from a business you know — don't click any links. And don't call phone numbers they give you. These are often scams.
- 2. Pass this information on to a friend.** You may not have gotten one of these messages, but chances are, you know someone who has.



“You’ve Won” Scams

Here’s how they work:



You get a call, letter, email, or text saying that you won! Maybe it’s a vacation or cruise, a lottery or a sweepstakes. The person calling about your prize is so excited. They can’t wait for you to get your winnings.

But here’s what happens next. They say there are fees, taxes, or customs duties to pay. Then they ask for your credit card number or bank account information. Or they insist you can only pay with cash, gift cards, wire transfers, cryptocurrency, or a payment app.

If you pay a scammer or share information, you lose. There is no prize. Instead, you get more requests for money, and more false promises that you won big.

Here’s what to do:

- 1. Keep your money — and your information — to yourself.** Never share your financial information with someone who contacts you and claims to need it. And never pay anyone who insists you send cash or can only pay with cash, gift cards, wire transfers, cryptocurrency, or a payment app.
- 2. Pass this information on to a friend.** You probably ignore these kinds of scams when you see or hear them. But you probably know someone who could use a friendly reminder.



Protecting and Preventing

Ways to Protect Yourself Against Fraud

- Review periodic statements and online banking frequently
- Set up alerts for transactions so you're aware of what coming in and out of your account(s)
- Use a password service like LastPass
 - Reduces the need for memorized passwords, less/no passwords are reused
- Place freezes or alerts on account opening services and at credit bureaus
- Stay vigilant and be cynical
- Reputable companies will not require an immediate decision
- If it sounds too good to be true, it is
- Maintain friendships and relationships with family
 - Getting a second opinion is important!
 - Also reduces risk of romance scams
- Increase your awareness of new schemes
- Know your financials processes – be alert when something is out of the ordinary

It happened, now what?

- Report it
 - Use the resources on the following page to report
- Contact your financial
 - They can place restrictions and notes to provide guidance and help in the future
- Tell Your Story
 - Share with friends, family



Resources

- <https://ovc.ojp.gov/program/stop-elder-fraud/providing-help-restoring-hope>
 - 833-Fraud-11 (833-372-8311)
- <https://www.ic3.gov/Home/ComplaintChoice>
- <https://reportfraud.ftc.gov/>
- www.Identitytheft.gov
- File a police report with your local precinct – methods vary
- <https://consumer.ftc.gov/features/pass-it-on/resources>
- <https://www.usa.gov/credit-freeze>
- <https://www.chexsystems.com/security-freeze/information>

Questions

