Protecting Your Financial Accounts

Speaker:

Kathleen Owens - Fiduciary, Financial Planner

KareBears of PebbleCreek Speakers Program

March 2025

What you can do to help protect yourself from financial exploitation and fraud

Your **ACTION PLAN** is highlighted in red!

Aurora Financial Planning & Investment Management LLC
Registered Investment Adviser, CRD # 291658
Aurorafinancialpim.com
858- 205-7651

1.

Smart Phone – How to protect your smart phone from getting hacked

Mobile Smart Phones are an attractive target for hackers due to their heavy usage and the amount of information they carry.

Despite security measures, mobile banking apps can still have vulnerabilities that hackers can exploit, especially if users don't practice safe habits like using strong passwords and avoiding public Wi-Fi.

- Do not use your phone for financial transactions.
- Do banking at home on your home computer with secure Wi-Fi.
- Another risk with having banking & investment account apps on your phone: what if your phone is lost or stolen? Thieves could potentially access your banking apps on a stolen phone and make unauthorized transactions.
- The less vital information you have on your phone, the safer you will be.

Exceptions:

One Exception is: Apple Pay. This payment method can be linked to your credit card; thus, you can easily dispute a fraudulent credit card charge.

Another exception of Android users is Google Pay. It substitutes actual card numbers with virtual ones for security.

2.

Safety of Credit Cards versus Debit Cards

- Credit card payments have more protection for you than debit cards. You can easily dispute an incorrect or fraudulent credit card charge, with a debit card not so much.
- Debit card have less protection than credit cards. With a debit card you will be liable for $50 or up to $500 depending on how fast you can report the fraud: Two days to report fraud for $50 liability. Within 60 days for liability to be limited to (usually) $500.
- Bonus reason to use credit cards: You can earn cash back, or points with credit cards. This is not offered on debit cards. Also, you have more time to pay your credit card charges. With a debit card, the money is taken from your account when you make the purchase.

3.

Know Your Adviser

- If you use the services of a financial advisor and you have an advisor designated to you, do they, and their staff really know you?
- It is very important, and another layer of protection for your accounts, that your adviser and their staff know you.
- Test your adviser: Call them. Do they recognize your voice? Do they know your spouse's name? Do they know what type of accounts you have with them: brokerage, IRA, Roth, CD or annuity?
- Large firms are targeted by hackers because these firms have hundreds of advisors and staff managing hundreds of accounts. It is difficult for these advisors and their staff to **really** know each one of their clients, and know their habits.

3. continued:

- Hackers impersonate clients at these firms and are able to steal millions, by wire transfer from these accounts each year.

Additional Protection by Working with A Financial Adviser

- Licensed financial advisers are required to be on the lookout for financial exploitation of a client.
- Advisers look for suspicious activity on the client's account and any changes in the client's behavior or routine.
- The law (Arizona) applies to a person age 65+
- The adviser may notify your ***trusted person*** you have designated on your account(s), or adult protective services and the corporation commission.
- It is strongly advised to designate a **trusted person (trusted contact)** on each of your financial accounts!
- This trusted person can be your spouse, your child, relative, or any person you trust and who knows you well.

Who is Ultimately Responsible for Protecting Your Account?

Is it the financial adviser, the client or the Broker Dealer?

(The Broker Dealer is the firm that holds the clients account)

3. Continued:

Who is ultimately responsible in this event that occurred in 2023?

- A large broker dealer, Morgan Stanley was ordered to pay $843,000 in compensatory damages to a senior investor in Florida.
- M. Kessler, age 75, alleged the firm was negligent in failing to prevent financial exploitation after she lost nearly $1.75 million to fraudsters posing as government officials.
- Scammers convinced Kessler that her identity had been stolen and she needed to convert her assets to cash, gold and cryptocurrency that would be deposited into a U.S. Treasury account for safe keeping.
- Kessler alleged that Morgan Stanley should have investigated her “uncharacteristic” requests to withdraw the money and also that it failed to take “reasonable” steps to ensure she had established a **trusted contact** for her account as required by Finra rules.
- Morgan Stanley in a counterclaim said it had acted prudently given the circumstances. Kessler, who had shown no indications of cognitive impairment, made misstatements to her advisor about the purpose of the withdrawals, including saying that she was helping her daughter purchase a home.

Would having a **trusted contact** have prevented this fraud from occurring?

4.

Trusted Contact

- Designate a trusted contact on all of your financial accounts.

5.

Protect your Account Statements

PAPER STATEMENTS

- Paper statements should be locked-up at all times.
- Make sure all of your financial firms have your correct address.
- Be aware if your bank has been bought/merged with another bank. Who is your new bank? Are you getting your statements?

DIGITAL STATEMENTS

- **Select a storage method that is easy for you**
- Using an **external hard drive** is an excellent, and secure method to store your bank and investment accounts. An external hard drive is a device that can be connected and unconnected to your home computer.
- Your financial adviser can help you set-up and move your digital account statements onto an external hard drive. Some advisers may offer storage options to their clients.
- Another method is "**Cloud Storage**" Dropbox, Google Drive, Microsoft Drive, QuickBooks and Quicken offer cloud storage for your PDF files.
- **Pros**: Secure and convenient.
- **Cons**: Need internet connection, cost, high learning curve.

- **Remember**: banks store your account statements on your portal access for a limited time. If you need a bank statement from more than 2 years ago, it can be more difficult to get a copy of that statement from the bank. It depends on the bank, how far back your account statements will be easily accessible.

#6

How Long Should You Keep Financial Statements?

- Keep records indefinitely if you do not file a tax return. (source: IRS)
- Keep records for **7 years** if you file a claim for a loss from worthless securities or bad debt deduction.
- Keep records for **6 years** if you do not report income that you should report, and it is more than 25% of the gross income shown on your return.
- Keeping **financial account statements** is **VERY IMPORTANT** for cost basis reporting.
- **Cost Basis**: We need to know <u>when</u> you purchased a security (stock, bond, of fund), and <u>how much you paid</u> to buy the security, so the cost basis can be calculated.
- The cost basis determines the amount of capital gain or loss you realize when you sell an investment, which could directly impact your tax liability: how much profit or loss you made on a security based on the price you originally paid for it, including any commissions or fees, allowing you to accurately report your gains and losses on your tax return.

#7

Who has access to your accounts?

Home healthcare workers, friends, relatives are people that can have access to your financial accounts.

Financial exploitation of older people is getting worse and worse. It's necessary that we must take the steps to secure our financial data.

- **Background checks- a background check should be done on any home healthcare worker coming into your home.**
- **References – While a reference is not a 100% guarantee that a person is trustworthy, it might prevent letting the wrong person into your home.**
- **Protect Data- Get in the habit of not leaving account statements, medical reports or other documents with your personal information lying around. Someone can quickly take a photo of your statement, or medical report which might have the full account statement number, your date of birth, or Social Security number.**

Estimated Losses to Persons over age 65

In 2023, in total, $28.3 billion was stolen.

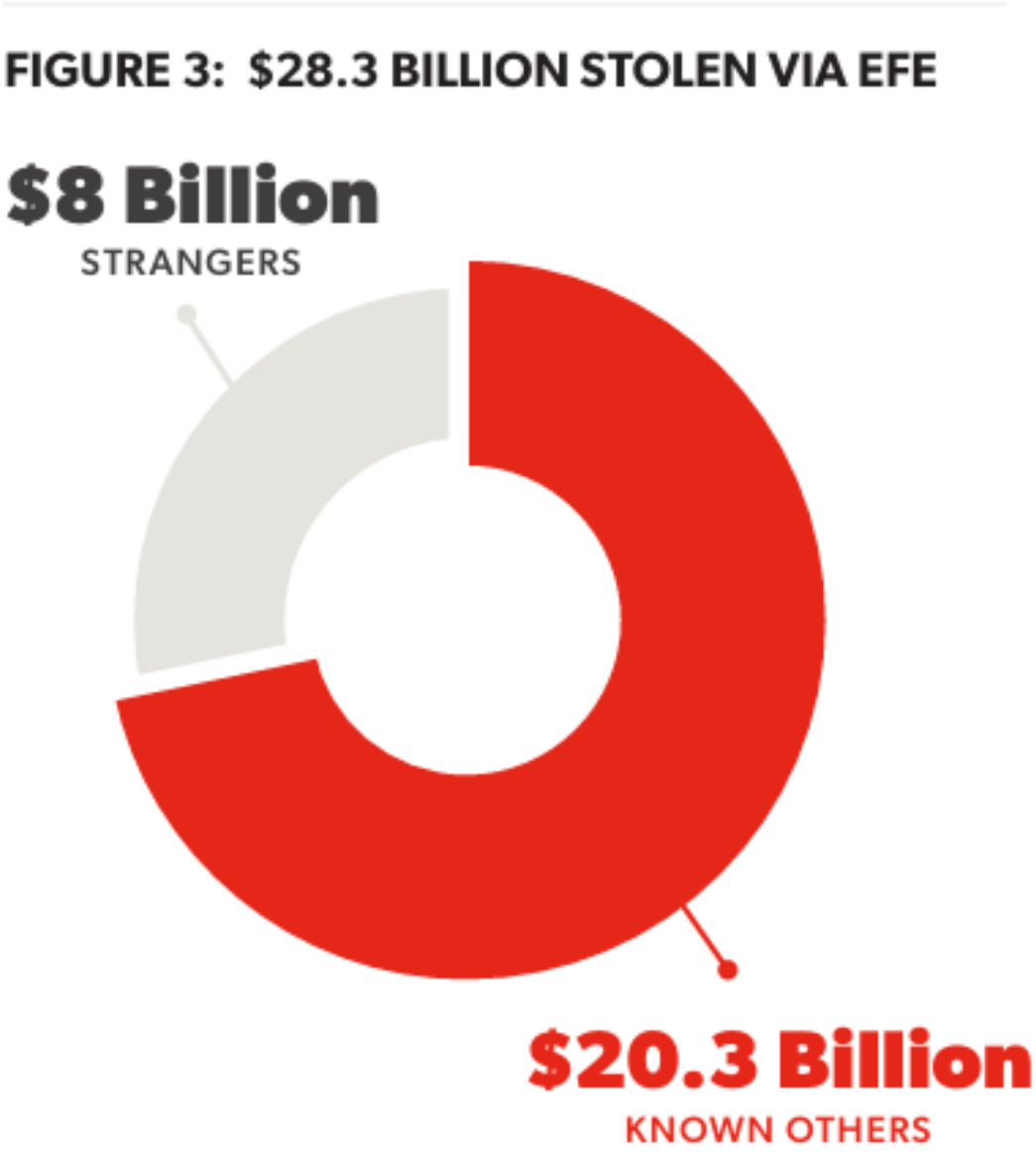
Family, friends, and caregivers—were responsible for stealing $20.3 billion.

That translates to 72% of dollars being taken by someone that was known.

While strangers were responsible for 28%, or $8 billion.

(source: AARP, June 2023)

Chart of Estimated Losses to Persons over age 65 "Elderly Financial Exploitation" (EFE)



#8

Let's Talk about the IRS (Internal Revenue Service

How the IRS will contact you

- We (the IRS) typically contact you the first time through regular U.S. mail delivered by the U.S. Postal Service. To verify the IRS sent the **letter or notice**, you can search for it on IRS.gov. Some letters are sent from private collection agencies.
- **Other ways we may contact you**:
- Email - We email you only with your permission, with a few exceptions like criminal investigations.
- Text message - We text you only with your permission.
- Phone - We might call to discuss your case, verify information or set up a meeting.
- Fax - We might send a fax to verify or request employment information.
- In-person visit - These are rare. Find out how and when IRS employees visit you or your business. We generally send a letter before we visit.

What the IRS won't do

- **WE DON'T** - Contact you or take payment on social media. Get trusted tax information on our official social media accounts.
- Accept gift cards or prepaid debit cards as payment
- Threaten to call law enforcement or immigration officials
- Take your citizenship status, driver's license or business license
- Leave pre-recorded voicemails (robocalls)
- Mail tax debt resolution advertisements (Source: IRS.gov)

There is NO Urgency with the IRS

- The IRS does not work quickly.
- If you have a legitimate dispute, on average taxpayers now can expect IRS Appeals to take **about a year** to resolve disputes.
- IRS Appeals employees will never ask for your credit card or banking information.

For more information and to schedule an appointment, contact:

Kathleen Owens, Fiduciary, Financial Planner
kathleen@aurorafinancialpim.com
858-205-7651

AURORA
Financial Planning
Investment Management