Tarheel Advisors Newsletter

Volume 16, Issue 4

October, 2024

The Silence of the Scams

Each year, millions of Americans fall victim to financial fraud. Unfortunately, there are sophisticated operations utilizing a combination of phone calls, texts, and emails to swindle you out of your hard-earned money. It is not just Nigerian princes anymore, either. Like Hannibal Lecter, these scams have become far more cunning. Seniors are at greatest risk, and according to the FBI, in 2023, victims aged 60 and older lost more than $3.4 billion to cyber crime. This was an increase of 11% from 2022, and the average victim lost $33,915. However, the total was likely much higher as fraud victims are reluctant to report scams, often due to embarrassment. The AARP estimates that $28.3 billion is stolen from people 60 and over every year.

One of the most common forms of cyber crime has become online investment fraud, which itself totaled more than $1.2 billion last year. In August, Bloomberg News reported a story of an 83 year old woman, Annette Manes, who was the target of an elaborate scam that drained her life savings. Manes was aware of potential scams and, in one case, refused to send cash to someone claiming that her grandson was in jail and in need of money quickly. However, the scam that began in October 2022 was more intricate: Someone called Manes that month claiming to be from a bank's fraud department, telling her that an unscrupulous employee sold her information to fraudsters. They then introduced her to a colleague who was purportedly a fraud manager. The fraudsters convinced Manes that by going undercover and withdrawing money without telling the bank's other staff or her family, she could help them catch a rogue employee and other criminals targeting retirees. Sadly, this series of events led to Manes withdrawing tons of cash and leaving it in a bag on her driveway for a "runner" to pick up. She also withdrew funds from her brokerage account to replenish her bank account, wrote checks directly from her brokerage account and deposited them in other people's accounts, and added a stranger as an authorized user on all her credit card accounts. The fraudsters coached Manes on how to evade raising red flags by telling bank tellers the money was for a contractor or for her niece's college fees, and she made up her own explanations as well. Over the course of nine months, Manes transferred roughly $1.4 million to the fraudsters, most of it passing through her bank checking account. All of this happened under the watchful eyes of several large banks and Wall Street brokerage firms despite policies that should have flagged multiple suspicious withdrawals.

In another similar instance, a 93 year old woman, Ruth Rootenberg, was scammed out of $278,000 over the course of a few months by scammers posing as government agents. According to the reporting of Bloomberg News and a subsequently filed lawsuit, Ms. Rootenberg began to notice inexplicable "clicking" noises when she was on her computer and came to believe she had been hacked. She reported her suspicions to her brokerage firm and other institutions where she held money, but no blocks were placed on her accounts. Scammers posing as government agents later reached out to her to say her identity had been stolen and that they could help protect her assets. According to the lawsuit, "she was told to sign an online document and give the scammers remote access to her computer while she logged onto her brokerage accounts." "Every day, she would receive two calls asking her to log into her accounts and direct her money to different transactions." The scammers would monitor Ms. Rootenberg's activity and send her messages directing her what to say to financial institution representatives. Sadly, all of these events led to Ms. Rootenberg handing over nearly $80,000 of gold bars to a "runner" outside her retirement home as well as wiring large sums of money from her brokerage accounts to a gold bullion company. This transfer was allowed to take place even though a brokerage firm supervisor had previously noted the gold firm's

2023 CRIME TYPES *Continued*

COMPLAINANTS OVER 60 LOSS			
Crime Type	Loss	Crime Type	Loss
Investment	$1,243,010,600	Data Breach	$23,913,130
Tech Support	$589,759,770	Extortion	$23,093,451
BEC	$382,372,731	SIM Swap	$15,148,072
Confidence/Romance	$356,888,968	Overpayment	$7,496,049
Government Impersonation	$179,646,103	Employment	$6,835,684
Personal Data Breach	$109,724,027	Threats of Violence	$5,128,768
Other	$72,707,042	Spoofing	$2,623,837
Advanced Fee	$67,923,263	Harassment/Stalking	$1,930,347
Lottery/Sweepstakes/Inheritance	$67,396,206	Crimes Against Children	$1,159,939
Real Estate	$65,634,851	Ransomware	$635,548
Non-payment/Non-Delivery	$59,018,965	Malware	$261,144
Credit Card/Check Fraud	$37,862,023	IPR/Copyright and Counterfeit	$183,169
Identity Theft	$34,551,900	Botnet	$23,142

2024 Market Update

S&P 500	**+20.8%**
DOW	**+12.3%**
NASDAQ	**+21.1%**
RUSS 2000	**+10.0%**
International	**+14.1%**
BONDS	**+4.5%**
GOLD	**+27.1%**

Mortgage Rates

15-Year	**5.7%**
30-Year	**6.9%**

Did You Know?

* The median return for the DJIA since 1901 is 7.7% annually (7.9% under Republican Presidents and 7.7% under Democrat Presidents)

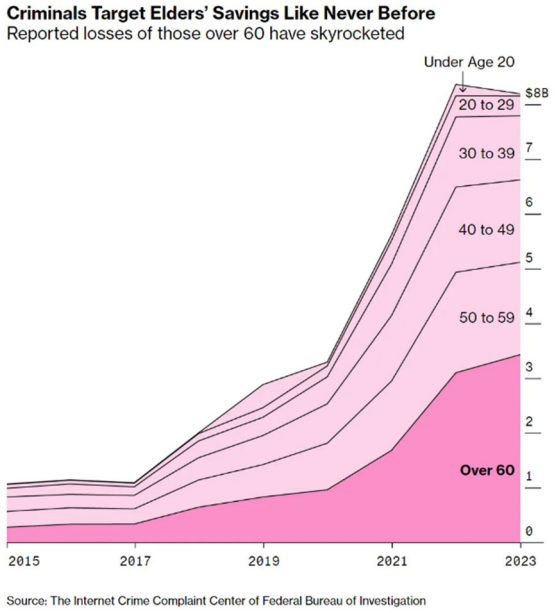
* The IRS has announced disaster tax relief for individuals or businesses affected by Hurricane Helene. This includes all of Alabama, Georgia, North Carolina and South Carolina and parts of Florida, Tennessee and Virginia. Taxpayers in these areas can delay 2024 4th quarter estimated tax payments as well as the filing of their federal 2024 tax return until May 1st.

* On September 18th, the Federal Reserve lowered interest rates for the first time in 4 years. Their benchmark rate was reduced by 50 basis points (bps) to a new target range of 4.75%-5.00%.

The Silence of the Scams (Continued)

connection to other scams.

Unfortunately, these types of scams are happening every day, and we've seen people fall victim to it first hand. They can be initiated via spam calls, emails or social media posts. Stopping them is impossible, and ignoring them is only half the battle. After all, the scammer just has to get it right once versus their potential victims that have to get it right 100% of the time.



One of the scariest parts of these stories is that the business models and regulations of the financial industry are woefully unprepared for these attacks. While the bulk of these scams are obvious and easily detected, they are likely occurring millions of times on a daily basis. For vulnerable populations, such as the elderly, this is extremely problematic. If caught on a bad day where you might not be at your sharpest, one can fall into a trap just like Ms. Manes and Ms. Rootenberg.

In most States, if you actively move money to a scammer, you have minimal protections or hope of ever seeing those funds again. Law enforcement can potentially recover funds, but the chances are unlikely. You can also sue your financial intermediary, but currently, they have minimal liability if you are the one authorizing the distributions on your own account. After all, this isn't identity theft or hacking; this is you asking for your own money, so products like identity theft insurance are minimally useful. So, how do you protect yourself?

According to the FBI's cyber crime division there are a couple of things you can do to defend and mitigate the risk:

- Recognize scam attempts and end all communication with the perpetrator.
- Search online for the contact information (name, email, phone number, addresses) and the proposed offer. Other people have likely posted information online about individuals and businesses trying to run scams.
- Resist the pressure to act quickly. Perpetrators create a sense of urgency to produce fear and lure victims into immediate action. Call the police immediately if you feel there is a danger to yourself or a loved one.
- Be cautious of unsolicited phone calls, mailings, and door-to-door service offers.
- Never give or send any personally identifiable information, money, jewelry, gift cards, or checks—or wire information or funds—to unknown or unverified persons or businesses.
- Ensure all computer anti-virus and security software and malware protections are up to date. Use reputable anti-virus software and firewalls.
- If you receive a pop-up or locked screen on your device, immediately disconnect from the internet and shut down the affected device. Pop-ups are regularly used by perpetrators to spread malicious software. To avoid accidental clicks on or within a pop-up, enable pop-up blockers.
- Do not open emails or click on attachments you do not recognize, and avoid suspicious websites.

Some other useful advice for everyone to know, is if you actually owe someone money, they will eventually send you a physical letter. Also, no legitimate entity will ever ask for payment via bitcoin, gold bullion, or gift cards. Immediately disengage if another party asks for these.

If you work with a large financial institution, you are often nothing but a name in a database to them. They have minimal ways to protect you from yourself in one of these scams. For those at the highest risk for fraud, our suggestion is to add a reliable family member or friend as a trusted contact or limited power of attorney (LPOA) on your financial accounts and to partner with a financial advisor at a local level. This provides an extra layer of protection and fiduciary capacity that helps to put a wall around your accounts. It is important that the financial advisor actually knows who you are and your current situation. This way they are able to flag and halt unusual distribution requests, and potentially get in touch with family members or the police on your behalf. While this will create an additional barrier of having to go through an extra person and steps for some transactions, the added layer of security is the best protocol available until the industry and legislation catch up to the problem. Unfortunately, protecting your nest egg isn't only about the investments any more. Making sure that there are multiple checks and balances in the process is equally important as you fight to silence the scams.

-Ryan Glover, CFP® & Walter Hinson, CFP®

Privacy Policy—In the course of providing advisory services, we may collect, retain, and use client information for the purpose of administering our operations, providing client service, and complying with legal and regulatory requirements. This information may come from sources such as account applications, investment policy statements, electronic or verbal correspondence from your brokerage, attorney, accountant or other advisor you may employ. We do not sell, exchange, or disclose client information with outside organizations unless the third party is essential in administering our operations or except as required or permitted by law. To further safeguard client information digitally, we maintain password protected systems, updated anti-virus and anti-spyware software, and encrypted hardware and software firewalls. Our regulatory ADV 2 is available at www.tarheeladvisors.com/adv2.pdf.

2024 ADV Part 2 Changes— Ryan Glover has an outside business interest in JDG Creative, LLC.