CHAPTER 14

KEEPING SAFE FROM SCAMS AND FRAUD

The prevalence of scams has risen sharply in the past few years. Not only are they happening more frequently, but they've also become far more sophisticated and deceptive than ever before. It's no longer the familiar "Nigerian Prince" email riddled with typos and asking for help to unlock millions of dollars. Today's scams are more convincing. They're more targeted. With the advances in AI, we should expect them to become even harder to detect.

If a scammer successfully targets one of your clients, much of your work can be undone in an instant. It won't matter how sound your planning was, how well their portfolio performed, or how disciplined they were—if they fall victim to a scam, the damage can be devastating. That's why this must become an essential part of your planning and coaching moving forward. Advisors need to help clients stay alert, stay informed, and protect themselves. Otherwise, all the sacrifice and discipline exercised could be for nothing.

Over the past year, I've sent several targeted emails to my investment clients containing specific information, warnings, and recommended actions to stay safe. Many responded with appreciation, and a few shared recent experiences of being targeted themselves. This needs to become a greater focus in our work. I'm certain that in the months and years ahead, I'll be bringing this up more and more. In my first 24 years as an investment advisor, I can't recall ever discussing scams or fraud with clients. But times have changed, and so must we.

Scammers Know More Than We Think

In early 2025, I emailed my clients a warning about scams. One client replied with a story that stuck with me. She'd received a call from a company she'd dealt with before, but something felt off. To appear legitimate, the caller recited her Social Security number.

That's what made it so unsettling; they already had her information. They used it to build trust and try to extract more. Thankfully, she didn't share anything else. But it was a wake-up call. We have to assume our personal data is already out there. What once felt "secure" may no longer be. And with AI making scams more convincing, the risks are growing.

This script highlights common scams as of early 2025 and how to stay protected. But scams evolve. To stay informed, consider performing online searches for the latest scams, use AI tools, and/or follow content creators who expose scammers.

Common Scams & Tactics (as of 2025)

Spoofing – Spoofing involves altering data we typically rely on to verify someone's identity. The most common types today are email and phone spoofing. In email spoofing, the message appears to come from a trusted person or company but is actually sent by a scammer. Similarly, phone spoofing makes it seem like the call is coming from a legitimate number by displaying a familiar name on caller ID when it's actually a fraudster.

If someone falls for a spoof, they may unknowingly share sensitive personal information or install malware on their device. Malware is often designed to steal secure data by recording keystrokes, capturing usernames and passwords, and ultimately giving the scammer access to the victim's accounts. In extreme cases, scammers can completely take over accounts and initiate unauthorized transactions like wire transfers.

Phishing –In a phishing scam, the fraudster tries to obtain secure information by impersonating someone the victim is familiar with, such as a company or individual they've dealt with before. Scammers use emails, texts, calls, and fake websites that appear legitimate to trick victims into giving up sensitive data. They'll often spoof phone numbers or email addresses to make their communication seem real. Links in phishing emails typically lead to fake sites that steal login credentials or other valuable information, which can then be used for financial gain or sold on the dark web.

Phantom Purchase Scam – This scam begins with an email thanking the recipient for a purchase they never made. A fake receipt or link is included to "view" the order details. Alarmed and confused, the person clicks the link or opens the attachment, potentially installing malware or a virus. The goal is to capitalize on the urgency and confusion to compromise the victim's system.

AI Deepfake Scam – Scammers are now using AI and deepfake technology to mimic the voice of someone the victim knows, often a family member. This makes it incredibly difficult to recognize the scam, especially if the request seems plausible or urgent.

This same tactic could also be used against financial advisors. A deepfake version of a client's voice, combined with spoofed phone numbers and phishing techniques, could make the scam nearly undetectable. Most advisors rely on phone calls to verify financial transactions, many firms even require it. In the near future, this may no longer be sufficient. Using a private code word or phrase may be necessary to add an extra layer of security.

Romance Scam – These scams are among the hardest to recognize, especially for the victim. To outsiders, the signs are often obvious, but to the person involved, the emotions are real and intense. Scammers typically begin on social media using fake profiles, building what feels like a trusting relationship over time. Eventually, the scammer asks for financial help due to an emergency or hardship. It often starts small but escalates. The emotional investment makes it difficult for the victim to see the deception.

Tech Support Scam – In this scam, someone poses as a representative from a well-known tech company, claiming the victim's computer is infected with malware or a virus. They offer to "help" by requesting remote access to fix the issue, often charging a fee in the process. Once they gain access, they may install malware or steal sensitive information, including payment data. Even after the fake tech support session ends, they may continue to extract data from the device.

Seniors are frequent targets of this scam. A popular YouTuber, Kitboga, poses as an elderly woman to engage with and expose scammers. His videos are both

entertaining and educational, and watching content like his (or from other scam-baiting creators) can help people stay informed about the latest tactics used by scammers.

Investment/Making Money Scam – These scams fall into the "too good to be true" category. They promise high returns with little or no risk, often under the guise of new or alternative investments like cryptocurrency. As interest in these assets grows and AI enhances scammers' tools, we can expect these schemes to become more common. The desire for big gains can blind even savvy investors to the red flags.

Another version of this scam involves sweepstakes or lottery "winnings." Victims are told they've won a prize and just need to provide some information to claim it. But the odds of such a win are astronomically low, if something seems serendipitous, it likely isn't real. Always consult a trusted family member or financial advisor before sharing personal information or taking action.

There are many other scams out there, and new ones are emerging all the time. Staying alert and helping clients stay protected must be a priority. The best defense is a proactive offense: educate, prepare, and act before a scam happens.

Protecting Clients (and Yourself) from Scams

There is no comprehensive list of safeguards that guarantees you would be protected from every scam. Even if there was, it would likely be incomplete by the time you read this. It isn't hard to protect yourself from a scam so long as you know what is happening and the tactics scammers employ. Below I list a few ways we can protect ourselves based on the scams that are known and prevalent today:

- Create a Secure and Unlikely Password. Phrases and passwords that include special characters with at least eight digits are recommended. It is also recommended that each login have a unique password and use a trusted password manager to remember them all. Use Two-Factor Authentication (2FA) when possible.

- Never Share Password or 2FA code. Never give anyone your password or Two-Factor Authentication Code (when a company emails or texts you a code to login to your account). This includes someone claiming to be from the company you do business with. They will never ask for your password nor authentication code—unless they are a scammer.

- Take Your Time, Slow Down! Scammers rely on catching you off guard and their request is often accompanied by a sense of urgency.

- Do Not Buy a Gift Card to Pay a Company/Person. No legitimate business (or professional) wants to be paid in gift cards. While cryptocurrencies may be emerging as a payment method, the rule still stands: Never use non-traditional payment methods, no matter the person/company or reason.

- Do Not Keep it a Secret. Scammers may urge you not to tell anyone, especially in romance and investment scams. This is a huge red flag. Always share what's happening with someone you trust. An outside perspective can help you spot red flags and see things more clearly.

- Limit Public Social Media Sharing. Scammers will look at your social media to learn more about you. The more personal information you share, the more convincing they can come across.

- Verify Person/Firm Contacting You. If you didn't request an email, text, or call, it could very well be a scam, no matter if you have done business with the company. Hang up. Call the known phone number (not the number given to you) to verify if it is legitimate.

- Don't Click on Links in Email or Text. This is especially true if you didn't request the email. These emails can look very real, and if you are in a hurry, you may not notice before clicking.

- Never Grant Remote Access to Your Device. Whether it is a computer, tablet, or phone. If you feel something needs to be fixed, talk to someone you trust about it before. If it is a legitimate concern, go see an IT repair company in person…there are many out there.

- Install Strong Antivirus Software. Choose comprehensive protection with automatic updates, malware, and phishing detection—avoid cheap or free options.
- Hold Cash Savings in a Brokerage Account. Many scams these days involve electronically transferring funds from one bank account to another using services such as Zelle. This adds a layer of security against scams like Zelle fraud, especially if the account is monitored by a trusted advisor.
- Freeze Your Credit Reports. Assume your Social Security number is exposed. Freezing your credit at all three bureaus (Experian, Equifax, TransUnion) prevents new accounts from being opened in your name and can be easily lifted or "thawed" if needed.

Encourage your clients to reach out anytime they, or someone they know, encounter something suspicious or unsettling. Offering this kind of support adds significant value to your service and strengthens your value proposition. For more on building your value proposition, see Chapter 29.

Chapter Summary

- It does an investor no good to save and invest wisely if they are going to lose it all in a scam. This is now an essential part of wealth management.
- We should assume that our SSN and other identifiable information is available to scammers and fraudsters.
- Scams are proliferating today in both type and level of deception. Advances in AI could make some scams near indetectable.
- Knowing how scams work can help your clients defend themselves from becoming a victim.
- There are many tactics your clients can use to further protect themselves. Sharing these tactics and updates on scams can become a valuable part of "client reviews."