09.22.26 | FINANCIAL LITERACY

Protecting Your Wealth: Recognizing and Avoiding Financial Scams

Michael Davide – Chief Compliance Officer

Financial scams have become increasingly sophisticated. Fraudsters no longer rely solely on poorly written emails or suspicious phone calls. Today's scams may involve convincing websites, text messages that appear to come from legitimate financial institutions, impersonation of government officials, fraudulent investment opportunities, and even artificial intelligence that can imitate the voice or appearance of someone you know.

Older adults can be particularly attractive targets because they may have accumulated significant retirement savings and other assets over their lifetimes. According to the FBI, reported fraud losses among people age 60 and older exceeded $7 billion in 2025, with investment schemes accounting for a significant portion of those losses.

Understanding how these scams work—and knowing what to do when something does not seem right—is an important part of protecting your financial security.

1. GOVERNMENT AND FINANCIAL INSTITUTION IMPERSONATION SCAMS

One increasingly common scam begins with a phone call, email, text message, or computer alert claiming that something is wrong with your bank, investment, Social Security, Medicare, or other account.

The caller may claim to represent your bank, a government agency, law enforcement, or another trusted organization. You may be told that your identity has been stolen, your account has been compromised, or criminals are attempting to steal your money.

The scammer then offers a solution: Move your money somewhere "safe." In reality, the destination belongs to the criminal.

What should you do?

Do not transfer money based upon an unsolicited call, email, text, or security alert. Hang up and independently contact the institution using a telephone number you already know or obtain from its official website, account statement, or the back of your credit or debit card.

Never assume a caller is legitimate simply because your caller ID displays the name of your bank, the IRS, Social Security Administration, police department, or another familiar organization. Caller ID information can be manipulated.

2. INVESTMENT AND CRYPTOCURRENCY SCAMS

Investment scams can be especially damaging because they frequently involve large amounts of money.

A fraudster may contact someone through social media, text message, an online advertisement, or even a dating website. After establishing trust, the person introduces an investment opportunity that supposedly offers exceptional returns with little risk.

Cryptocurrency has become particularly prevalent in these schemes. Criminals may spend considerable time developing a personal, professional, or romantic relationship before introducing an investment. Victims may even be directed to sophisticated-looking websites or apps showing fictitious account balances and investment gains.

A common tactic is to allow a victim to make a small withdrawal early in the relationship. This creates confidence that the investment is legitimate and encourages the victim to invest substantially more.

Be particularly suspicious when someone you met online:

- introduces you to an investment opportunity;
- promises unusually high or guaranteed returns;
- encourages you to purchase cryptocurrency;
- asks you to transfer assets from an established investment or retirement account;
- directs you to a particular investment website or application;
- pressures you to invest quickly; or
- tells you not to discuss the opportunity with your financial advisor or family.

Before making a significant investment based upon an unsolicited opportunity, talk with your financial advisor or another trusted financial professional.

A legitimate investment opportunity should withstand independent scrutiny.

3. ROMANCE AND RELATIONSHIP SCAMS

Romance scams are particularly troubling because the criminal first establishes an emotional relationship with the victim.

The relationship may develop over weeks or months. Eventually, the individual requests money for an emergency, medical expense, travel, business opportunity, or investment.

The person may claim to live or work overseas and repeatedly find reasons why meeting in person is impossible.

Technology is making these schemes more convincing. Artificial intelligence and deepfake technology can potentially be used to make online interactions appear more authentic.

Be cautious whenever someone you have never met personally asks you to send money, cryptocurrency, gift cards, or financial information–regardless of how long you have communicated with the person.

4. THE “GRANDPARENT” OR FAMILY EMERGENCY SCAM

You receive a frantic telephone call: *“Grandpa, I’m in trouble.”*

The caller claims to be a child or grandchild who has been arrested, hospitalized, involved in an accident, or stranded somewhere and urgently needs money.

Another individual may then get on the telephone claiming to be a lawyer, police officer, doctor, or bail bondsman. The caller may insist that the situation is confidential and tell you not to contact other family members.

Artificial intelligence makes this scam increasingly concerning because criminals may be able to imitate a person’s voice using recordings obtained online.

If you receive an emergency request involving a family member, stop and verify it independently.

Call the family member directly using the number you normally use. If you cannot reach the person, contact another family member who can verify the situation. Do not rely on the telephone number provided by the caller.

5. TECH SUPPORT AND COMPUTER SCAMS

A warning suddenly appears on your computer claiming that it has been infected with a virus. The message provides a telephone number for “Microsoft Support,” “Apple Support,” your bank’s security department, or another familiar company.

When you call, the person asks for permission to remotely access your computer. This can give the criminal access to sensitive information and potentially your financial accounts.

Never give an unsolicited caller remote access to your computer.

If you believe there is a legitimate problem with your device, contact the manufacturer or a trusted technology professional independently.

6. PHISHING EMAILS, TEXT MESSAGES AND PHONE CALLS

Fraudsters frequently impersonate banks, investment firms, credit card companies, delivery services, government agencies, and other familiar organizations.

These attacks are commonly referred to as phishing when conducted through email, smishing when conducted through text messages, and vishing when conducted through telephone calls.

A message may say:

"We detected suspicious activity on your account. Click here immediately to verify your identity."

Do not click the link. Instead, open the institution's application yourself or type its known website address into your browser. You can also call the institution using a telephone number you independently verify.

Never provide a one-time security code or multifactor authentication code to someone who contacts you.

7. SWEEPSTAKES, LOTTERY AND PRIZE SCAMS

"You've won $2 million!"

There is only one problem: Before receiving your winnings, you must pay taxes, processing fees, legal expenses, or insurance.

This is a classic warning sign. Legitimate sweepstakes do not require winners to send money in order to receive a prize. Never send money, gift cards, cryptocurrency, or financial information to claim an unexpected prize.

Recognizing the Warning Signs

Although scams take many different forms, they often share common characteristics. Be especially cautious when someone:

- creates an extreme sense of urgency;
- tells you that you must act immediately;
- tells you not to discuss the situation with your family, financial advisor, bank, or attorney;
- requests payment through cryptocurrency, gift cards, cash, or wire transfer;
- asks you to withdraw a large amount of cash;
- asks you to move money to a "safe" or "protected" account;
- asks for remote access to your computer;
- requests your password or authentication code;
- promises unusually high or guaranteed investment returns; or
- becomes angry, threatening, or increasingly aggressive when you ask questions.

Urgency and secrecy are two of the strongest warning signs of financial fraud.

A SIMPLE RULE: STOP, VERIFY AND DISCUSS

When confronted with an unusual financial request, remember three words:

STOP

Do not allow someone else's sense of urgency to become yours.

You generally have time to investigate before sending money or providing information.

VERIFY

Independently verify who is contacting you.

Do not use the telephone number, email address, website link, or contact information provided by the person requesting the money.

DISCUSS

Before making an unusual or significant financial transaction, discuss it with someone you trust.

That might include a spouse, adult child, financial advisor, attorney, accountant, or another trusted individual.

Scammers frequently attempt to isolate their victims. Bringing another person into the conversation can provide an important second perspective.

STEPS YOU CAN TAKE TODAY

You do not need to wait until you encounter a scam to protect yourself.

Use unique, strong passwords for important financial accounts and consider using a reputable password manager rather than reusing the same password across multiple websites.

Enable multifactor authentication whenever it is available. This provides another layer of security if someone obtains your password.

Consider establishing a trusted contact on your investment accounts. A trusted contact does not have authority to transact in your account but may provide your financial institution or advisor with someone to contact when there are concerns about your welfare or potential financial exploitation.

Monitor bank, credit card, and investment accounts regularly and investigate transactions you do not recognize.

Consider placing security alerts on financial accounts that notify you of transactions, password changes, or other important account activity.

Finally, talk about scams with family members. Financial fraud should not be an embarrassing subject. Criminals deliberately use sophisticated psychological techniques and technology to make their schemes believable.

BEFORE YOU SEND MONEY – CALL YOUR GRIMES ADVISOR

Something doesn't feel right? Don't act yet.

Before sending money, transferring investments, purchasing cryptocurrency, withdrawing a large amount of cash, or providing sensitive financial information in response to an unexpected request, **stop and contact your Grimes & Company advisor.**

In particular, be on alert if someone:

- says you must act immediately;
- tells you to keep the transaction secret from your family, bank, financial advisor, attorney, or accountant;
- asks you to move money to a "safe," "secure," or "protected" account;
- requests payment by cryptocurrency, gift card, wire transfer, or cash;
- asks for your password, PIN, or one-time security code;
- asks for remote access to your computer or mobile device;
- claims a family member is in an emergency and needs money immediately; or
- promises guaranteed or unusually high investment returns.

When in doubt, do not send the money. Call Grimes & Company first.

A short conversation with your advisor may help determine whether a request is legitimate before money leaves your account.

WHAT TO DO IF YOU THINK YOU HAVE BEEN SCAMMED

Act quickly. The sooner financial institutions and law enforcement are notified, the greater the possibility that additional losses can be prevented.

1. Stop communicating with the suspected scammer. Do not send additional money, even if you are told another payment will recover money already lost.
2. Contact your bank, custodian, credit card company, and financial advisor immediately. Explain what occurred and ask whether pending transactions can be stopped or recalled.
3. Change compromised passwords. If someone had access to your computer or accounts, change passwords from a different, trusted device.
4. Protect your credit. If personal identifying information was compromised, consider placing a fraud alert or credit freeze with the major credit reporting agencies.
5. Preserve the evidence. Save emails, text messages, telephone numbers, receipts, wire instructions, cryptocurrency

addresses, screenshots, and other communications.

6. Report the incident. Internet-related fraud can be reported to the FBI's Internet Crime Complaint Center at IC3.gov. Fraud can also be reported to the Federal Trade Commission at ReportFraud.ftc.gov.
7. Be alert for recovery scams. Victims of fraud may be targeted again by criminals claiming they can recover the stolen money for an upfront fee.

YOUR FINANCIAL SECURITY IS PART OF PROTECTING YOUR WEALTH

Wealth management is about more than investing assets. It is also about protecting the wealth that you have spent a lifetime building.

At Grimes & Company, the security of our clients' financial information and assets is a paramount focus. We encourage clients to contact us whenever they receive an unusual financial request, suspicious communication, unexpected investment opportunity, or instructions to transfer money—even if they are simply unsure whether something is legitimate.

When in doubt, contact us before acting.

Taking a few minutes to verify a request can prevent a financial decision that may be difficult or impossible to reverse.

We also encourage clients to discuss these issues with parents, grandparents, children, and other family members. Awareness remains one of the most effective defenses against financial fraud.

If you have questions about protecting your accounts or believe that you or a family member may have been targeted by a financial scam, please contact your Grimes & Company advisor.

IMPORTANT DISCLOSURES:

This information is provided for general educational and informational purposes only and is not intended as legal, tax, cybersecurity or identity-theft recovery advice. The appropriate steps may vary based on individual circumstances. If you believe you have been the victim of identity theft or fraud, consider contacting the appropriate financial institution, credit bureau, government agency and/or qualified professional promptly.