Fraud Warriors Inc.

A 501(3)c Not-for-Profit Corporation

Host: Doug Frawley CFP®, CPA, MBA

Investment Advisor Representative

What we will cover in Part I:

- Magnitude of Financial Fraud
- Things That Scammers Say
- What to do When you Spot a Scammer
- Introduction to Artificial Intelligence (AI)
- AI in our Daily Life
- Deepfake Tech and Fraud
- AI-Powered Phishing Attacks
- Synthetic Identity Fraud
- Chatbot Impersonation

Top 5 Fraud Categories

INVESTMENT SCAMS

ONLINE SHOPPING SCAMS

PRIZES, SWEEPSTAKES, AND LOTTERIES

INTERNET SERVICES

BUSINESS AND JOB OPPORTUNITIES

Magnitude of Financial Fraud in 2023 (US) - FTC

Consumers reported losing $10 billion to fraud in 2023.

Increase of $1.2 billion over 2022

Consumers reported losing more money to investment scams—more than $ 4.6 billion—a 23% Increase over 2022.

Some of the things Scammers say (FTC)

- ***"Act now!"*** **That's a scam**. Scammers use pressure, so you don't have time to think. But pressuring you to act now is always a sign of a scam. It's also a reason to stop.
- ***"Only say what I tell you to say."*** **That's a scam**. The minute someone tells you to lie to anyone — including bank tellers or investment brokers — stop. It's a scam.
- ***"Don't trust anyone. They're in on it."*** **That's a scam**. Scammers want to cut you off from anyone who might slow you down.
- ***"Do [this] or you'll be arrested."*** **That's a scam.**Any threat like this is a lie. Nobody needs money or information to keep you out of jail, keep you from being deported, or avoid bigger fines. They're all scams.
- ***"Don't hang up.***" **That's a scam**. If someone wants to keep you on the phone while you go withdraw or transfer money, buy gift cards, or anything else they're asking you to do: that's a scammer. DO hang up.

Only Scammers will say (con't):

- "***Move your money to protect it"*** **is a scam**. Nobody legit will tell you to transfer or withdraw money from your bank or investment accounts. But scammers will.
- ***"Withdraw money and buy gold bars"*** **is a scam**. Always. Every time.
- ***"Withdraw cash and give it to [anyone]"*** **is a scam**. Doesn't matter who they say: it's a scam. Don't give it to a courier, don't deliver it anywhere, don't send it. It's a scam.
- ***"Go to a Bitcoin ATM"*** **is a scam**. Nobody legit will ever insist you get cryptocurrency of any kind. And there's no legit reason for someone to send you to a Bitcoin ATM. It's a scam.
- ***"Buy gift cards" is a scam***. There's never a reason to pay for anything with a gift card. And once you share the PIN numbers on the back, your money's as good as gone.

What to do when you spot a scammer!

1

If you see or hear any version of any of these phrases, you've just spotted a scammer.

2

Instead of doing what they say, stop. Hang up. Delete the email. Stop texting. Block their number — anything to get away from them.

3

And then, tell someone you trust and report the scam to the FTC: ReportFraud.ftc.gov.

4

•The FTC shares these reports with approximately 2,800 federal, state, local, and international law enforcement professionals

Introduction to Artificial Intelligence (AI)

- AI as a branch of computer science dedicated to creating systems that can perform tasks which typically require human intelligence.
- It is important to have an understanding of AI, as it becomes more integrated into various aspects of life.
- **AI Defined**: AI enables computers to perform tasks that typically require human cognitive abilities.
- Examples: Delivery robots, AI voiceovers, Virtual assistants, and Healthcare diagnostics.
- Impact: AI is transforming industries, enhancing efficiency, and aiding decision-making.

Types of AI & Applications

- Narrow AI: Specialized for specific tasks (e.g., virtual assistants).
- General AI: Human-level intelligence (still theoretical).
- Superintelligent AI: Beyond human capabilities (future possibility).
- Healthcare: Diagnosing diseases, drug discovery, and personalized treatment.
- Business: Enhancing customer service, automating processes, and predicting trends.
- Transportation: Self-driving cars and delivery drones.
- FRAUD!! Criminals use AI extensively to scam people out of billions annually!

AI in daily life

Manufacturing Robots	Self-Driving Cars	Smart Assistants	Healthcare Management	Automated Financial Investing
Virtual Travel Booking Agents	Social Media Monitoring	Marketing Chatbots	FaceID on iPhones	Recommendation Algorithms (e.g., Netflix)

Deepfake Technology and Fraud

- Criminals can use deepfake technology to create video or audio clips that convincingly mimic the speech and appearance of a trusted individual, such as a company CEO. They might then use this fake media to convince employees to transfer funds or reveal sensitive information.
- **Case Study:** In 2019, a UK-based energy firm was scammed out of $243,000 when fraudsters used AI-based software to mimic the German CEO's voice, instructing an executive to make a transfer to a Hungarian supplier, with the funds eventually routed to Mexico and other locations.

AI-Powered Phishing Attacks

- Machine learning can aid in crafting personalized phishing emails that are more likely to deceive the recipient.
- By analyzing data from social networks and previous breaches, AI can generate messages that appear to come from a trusted colleague or family member, thus increasing the likelihood of a successful scam.
- **Case Study**: In early 2021, researchers observed a spike in AI-driven phishing tools being sold on the dark web.
- These tools automate the creation of phishing websites or emails that are incredibly convincing, using machine learning to improve over time based on which tactics are most successful.

Synthetic Identity Fraud

- Fraudsters use AI to create synthetic identities, amalgamating real and fake personal data to form new, fraudulent identities that can be used to apply for credit, open bank accounts, or conduct illicit transactions.
- **Case Study**: Synthetic identity fraud is the fastest-growing type of financial crime in the United States, according to the Federal Reserve.
- AI enables the mass generation and testing of synthetic identities until they find combinations that successfully pass verification processes.

Chatbot Impersonation

- Scammers might use AI-powered chatbots to impersonate customer service agents from financial institutions, convincing victims to divulge account information or make payments to the fraudsters.
- **Case Study**: In a reported scam, individuals received messages through social media platforms from bots claiming to represent a bank or service provider.
- These bots engaged in conversation and directed users to login pages that steal their credentials.

Credit Card Fraud with AI Optimization

- AI can analyze vast amounts of transaction data to determine patterns that are likely to go undetected by fraud prevention systems.
- Using these insights, criminals can execute a high volume of fraudulent transactions with a higher success rate.
- **Case Study**: Through machine learning, fraudsters optimize the timing, value, and type of fraudulent credit card transactions to evade anomaly detection, maximizing the amount that they can steal before the card is blocked.

What we will cover in Part II

- Other AI-Related Scams
- Ponzi Scheme, Affinity Fraud, Churning, Pump and Dump
- 25 Tips to Avoid Being a Victim
- Common Financial Advisor Fraud
- Financial Advisor Red Flags
- What is a Fiduciary?
- Fee-only vs. Fee-based
- How to Protect Yourself

Other AI-Related Scams

- **AI-scripted Scam Calls:** AI systems are programmed to make scam calls that are interactive and adapt to victims' responses, often pretending to be from government agencies to extract funds or personal details.
- **Fraudulent Online Reviews:** AI is used to generate a large number of fake product reviews to manipulate consumer purchasing decisions, leading to purchases of substandard or non-existent products.
- **Scam Bots on Dating Apps:** Bots, powered by AI, engage users on dating apps, build a rapport, and then lure them into paying money for various fabricated reasons such as travel expenses to meet up.

Other AI-Related Scams (con't)

- **AI-powered Email Scams:** Personalized emails crafted by AI target individuals with seemingly legitimate investment opportunities or requests for help, luring them into financial scams.
- **AI-Related Scams:** Criminals produce deepfake videos that appear to show individuals in compromising situations and then extort them for money with threats of releasing the footage.
- **Impersonation of Public Figures:** AI is used to create audio or video clips of public figures making false statements, leading to fraudulent fundraising or misinformation-based scams.
- **AI-assisted Account Takeover:** Using AI to analyze and crack passwords and security questions more efficiently, leading to unauthorized access of personal accounts for financial gain.

AI-Related Scams (con't)

- **Fake Social Media Profiles:** Scammers use AI to create and manage realistic-looking social media profiles to befriend and manipulate individuals into revealing personal information or sending money.
- **AI-generated Voice Phishing (Vishing):** Fraudsters use AI to clone voices from a few samples of speech, making calls to victims that seem to be from their loved ones or bank officials, asking for money or sensitive data.
- **Romance Scams with AI-generated Images:** Using AI to generate attractive, yet fake profile pictures, scammers engage in online relationships to defraud individuals looking for romantic partners.

25 Tips to Avoid Being a Victim

- Be skeptical of unsolicited contacts, especially those that request personal information.
- Never share sensitive information like passwords, PINs, or Social Security numbers.
- Verify the identity of individuals or organizations through independent means before transacting.
- Use two-factor authentication where possible to secure your accounts.
- Regularly update passwords and make them complex, using a combination of letters, numbers, and symbols.
- Check privacy settings on social media to prevent oversharing information.
- Look for inconsistencies in stories or messages that could indicate a scam.
- Be wary of unexpected attachments or links in emails, even from known contacts.

25 Tips to Avoid Being a Victim (con't)

- Monitor bank and credit card statements regularly for unauthorized transactions.
- Install and update antivirus and anti-malware software on your devices.
- Don't make financial decisions based on unsolicited emails or messages.
- Avoid public Wi-Fi for financial transactions or accessing sensitive information.
- Know that government agencies do not call to demand immediate payments or personal details.
- Be cautious of online romance and never send money or gifts to someone you haven't met in person.
- Watch out for high-pressure tactics urging you to act quickly.
- Ensure websites are secure (look for "https" and a padlock icon) before entering payment information.

25 Tips to Avoid Being a Victim (con't)

- Research charities before donating to ensure they're legitimate.
- Be cautious of too-good-to-be-true investment opportunities, especially those promising high returns with low risk.
- Use credit cards for online purchases; they often provide better fraud protection than other payment methods.
- Keep your operating system and applications up-to-date with the latest security patches.
- Educate yourself on the latest scams by subscribing to alerts from consumer protection agencies.
- Be wary of requests for payments via wire transfer, gift cards, or cryptocurrency, as these are often irreversible and untraceable.
- Perform reverse image searches on profile pictures to check for use across multiple profiles.
- If you suspect fraud, contact your bank immediately to place holds on any suspicious transactions.

Most Important Tip!

- Follow Fraud Warriors to stay informed and, as always, stay vigilant!
- We will continually update our website to include the latest scams, as they are continually evolving.
- Be sure to subscribe to our site at the bottom of each page to get updates of the latest online scams.
- **Up Next**: Financial Advisor Fraud Tactics & Red Flags; Fiduciary Defined; and 'Fee-Only' vs. 'Fee-Based' advisors explained.

Common Financial Advisor Fraud Tactics

PONZI SCHEME

AFFINITY FRAUD

CHURNING

PUMP & DUMP

PONZI SCHEME

A Ponzi scheme is a fraud where current investors are paid "returns" with money that is raised from new investors. It is named after Charles Ponzi, who orchestrated the fraud in the 1920s.

Today, Bernie Madoff is more closely associated with the Ponzi scheme for the reported $65 billion fraud that was discovered in the wake of the 2008 financial crisis, the biggest Ponzi scheme in history.

Madoff died in 2021 after serving 10 years of a 150-year prison sentence.

AFFINITY FRAUD

The Affinity Fraud targets a particular group with its ploy, usually in conjunction with a Ponzi scheme.

The scam is effective because we tend to trust other members of our "tribe." The group may share the same religion, cultural background, or geographic region.

More recently a local Naples Church was preyed upon and church members in a $35M Affinity Fraud Ponzi Scheme.

Churning

Churning involves an advisor buying and selling securities frequently in order to earn a commission on each transaction. This practice used to be common among stock brokers, but commissions on stock trades have essentially been eliminated thanks to online brokers.

However, the practice could still happen with mutual funds, which is something to watch out for in your account.

If a change is necessary between different funds, you can typically find a new fund within the same fund family that meets your needs, which can help avoid unnecessary fees.

Pump and Dump

Pump and dump scams often involve penny stocks that have been inflated due to misleading information or market manipulation, allowing the scammers to profit once the share prices have been bid up.

Be sure to research any investment recommendations thoroughly, even if they come from an advisor.

You should be extremely skeptical of penny stock recommendations because of potential frauds and the limited financial information available.

Financial Advisor Red Flags

Guaranteed Investment Returns

High Pressure Sales Methods

Writing Checks Directly to the Advisor

Not Being Responsive

Financial Advisor Red Flags

Constantly trying to sell you products that you are not interested in or that do not fit your profile

Short-term focus rather than long-term

•Lack of transparency regarding fee structure and how they are compensated

Don’t be afraid to walk away if an offer doesn’t seem right.

What is a Fiduciary? –Smartasset.com

- Fiduciaries are legally bound to put their client's best interest ahead of their own.
- An investment fiduciary is anyone with legal responsibility for managing someone else's money, such as a member of the investment committee of a charity.
- Registered investment advisors and insurance agents have a fiduciary duty to their clients.
- Broker-dealers may be subject to the less stringent standard set by the SEC Regulation Best Interest, implemented in 2019. They can take commissions.

Fee-only vs. Fee-based –Smartasset.com

- Fee-based may earn money based on a percentage of assets under management or AUM. In addition, they can earn commissions when executing trades, selling insurance, or selling you mutual fund shares.
- There is a financial incentive to sell you the products from which they earn a commission, even if it isn't necessarily the best product for you.
- Fee-only advisors earn money exclusively through the fees that their clients pay, typically based on AUM. They do not receive payment from any other source. If they do, they are not fee-only.
- With a fee-only financial advisor, you're more likely to get unbiased and objective investment advice

Protecting Yourself

Be sure you're working with a registered investment advisor (RIA), which are required to act as fiduciaries for their clients.

RIAs are also required to file regular reports with the Securities and Exchange Commission and have compliance programs in place, among other requirements.

Verify your financial advisor's (any financial professional) credentials.

Top 10 Financial Advisor Credentials (Forbes.com)

- **CPA** : Certified Public Accountant
- **CFA**: Chartered Financial Analyst
- **CFP**: Certified Financial Planner
- **ChFC**: Chartered Financial Consultant
- **RIA**: Registered Investment Advisor

Top 10 Financial Advisor Credentials (Forbes.com)

- **IAR**: Investment Adviser Representative
- **CFF:** Certified Financial Fiduciary
- **RICP:** Retirement Income Certified Professional
- **CPWA:** Certified Private Wealth Advisor
- **CLU:** Chartered Life Underwriter

Protecting Yourself

- **1. Vet and Verify:**
- Thoroughly vet your financial advisor's background.
- Check for any disciplinary actions or complaints.

- **2. Use Reputable Resources:**
- **Certified Financial Planner (CFP):** Verify credentials at cfp.net
- **Chartered Financial Analyst (CFA):** Check certifications at cfainstitute.org
- **BrokerCheck by FINRA:** Research advisors, brokers, and firms at brokercheck.finra.org

Closing Thoughts

- **Closing Thoughts:**
- Choosing the right financial advisor is essential for your financial wellbeing.
- Take the time to research and make informed decisions.

Thank You!

- Feel free to reach out for any further advice or questions:
- doug@fraudwarriors.org