Otoño Consulting, LLC

Stephanie W. Telles, MBA, CFE
Founder & CEO

# BEHIND THE SCAM

## UNVEILING FRAUDSTER PSYCHOLOGY TO EMPOWER MODERN ELDERS

*Presented to:*

NEW MEXICO AGING SERVICES

**NEW MEXICO CONFERENCE ON AGING**
**46TH ANNUAL | OCTOBER 28, 2024**

# GENERAL DISCLAIMER

Otoño Consulting, LLC provides non-authoritative guidance on fraud and other organizational practice education. The information in this presentation should not be viewed as an official position of any standard setters. The information provided in this presentation is for general informational and educational purposes only. While every effort has been made to ensure that the information presented is accurate and up to date, it should not be considered as legal, financial, or professional advice. Participants are advised to consult with qualified professionals for specific advice tailored to their situation. The presenter and the organizing body of this presentation do not assume any responsibility for errors, omissions, or contrary interpretations of the subject matter herein. No part of this presentation is intended to malign any religion, ethnic group, club, organization, company, individual, or anyone or anything. The scenarios and/or case studies presented are for illustrative purposes only and may not reflect all aspects of real-life cases of fraud. Audience discretion is advised, especially for content that may be sensitive or triggering. This presentation may contain forward-looking statements that are based on current expectations, forecasts, and assumptions and involve risks and uncertainties. These statements are not guarantees of future performance, and actual results could differ materially from those anticipated in these statements. The presenter and the organizing body are not responsible for any actions taken by individuals as a result of this presentation, nor for any personal, financial, legal, or other consequences that may arise from the application of the information provided.



Otoño Consulting, LLC

# What is fraud?

*Fraud* happens when someone tricks or deceives others to gain something for themselves and becomes a crime when someone knowingly lies or hides important information to make another person act in a way that harms them.


In other words, if someone lies to take your money or property, that's fraud.

# By the numbers: 2023 National Snapshot

| | |
|---|---|
| Complaints by individuals 60+ | 101,068 |
| Total Losses | 3,427,717,654 |
| Increase from 2022 | 11% |
| Average Dollar Loss | $33,915 |

# By the numbers: 2023 New Mexico Snapshot

| 759 | $17,784,632 | 28% | $23, 431 |
|---|---|---|---|
| Number of Complaints by Individuals 60+ | Total Losses | Increase from 2022 | Average Dollar Loss |


WHAT DO ALL
FRAUDSTERS HAVE
IN COMMON?

# They were trusted.

Elder fraud and financial abuse devastates incomes across all levels, deepens health care inequities, disrupts families, limits access to health care, and raises the incidence of mental health challenges among modern elders.

This form of abuse inevitably strips away human rights and dignity. Despite increased public awareness, fueled by high-profile cases, elder fraud and financial abuse remains largely underreported, overlooked, and under-prosecuted.

# Fraudsters Use Human Behavior—We Can, Too!

We can use the same behavioral analysis fraudsters rely on for manipulation as a means of self-defense.

By understanding what motivates fraudsters and knowing how they exploit typical behaviors, you can take proactive steps to protect yourselves, making fraud prevention a daily habit rather than a reactive response.

# WHY DO PEOPLE COMMIT FRAUD?

Donald Ray Cressey 1960,
Photo Credit: https://prabook.com/web/donald_ray.cressey/1696775

The most widely accepted explanation for why some people commit fraud is known as the Fraud Triangle.

The Fraud Triangle was developed by Dr. Donald Cressey, a criminologist whose research on embezzlers produced the term "trust violators."

# The Fraud Triangle


The Fraud Triangle suggests that if three things are present, they are very likely to commit fraud.

# Understanding the Fraud Triangle

- **Pressure (Why Fraudsters Do It)**
  - They're motivated by money or personal problems.
- **Opportunity (How They Do It)**
  - They look for ways to take advantage of you when you're not on guard.
- **Rationalization (How They Justify It)**
  - They convince themselves their actions are harmless or justified.

# Understanding Motives: Why Fraudsters Do What They Do

Most fraudsters are motivated by money, pressure, or greed. Knowing that they are often desperate or opportunistic allows us to stay vigilant.

For example, if someone is pressuring you for quick decisions about money or personal information, it's likely they're trying to take advantage of a moment of vulnerability. Take your time, ask questions, and seek advice before making decisions.

# Recognizing Opportunities: Fraudsters Thrive on Gaps in Our Defenses

Fraudsters look for opportunities when we are distracted, trusting, or unfamiliar with new technology. We can close those gaps by being more cautious with personal information, questioning unsolicited offers, and learning about common scams.

By understanding that they target moments when we let our guard down, we can actively create barriers that make it harder for them to succeed.

# Behavior Modification: Simple Actions Can Deter Fraud

Fraud prevention doesn't always mean being on constant alert–it means building habits that naturally protect us.

For instance, regularly checking bank statements, using strong passwords, and verifying identities before sharing information can significantly reduce the opportunity for fraud.

These small, proactive behaviors can make it much harder for fraudsters to exploit us.

# Leverage Relationships for Protection

Fraudsters often try to isolate their victims, especially elders, by creating a sense of urgency or secrecy.

By building a circle of trust with family, friends, or advisors, you can create a system where you consult others before making big decisions.

Sharing concerns and seeking advice can help prevent you from being isolated and targeted.

# Using Skepticism as a Tool

Fraudsters prey on the natural human desire to trust others, especially those who seem kind or authoritative. But healthy skepticism can protect you.

If something feels off or too good to be true, take a moment to pause, reflect, and ask questions. Fraudsters want you to act quickly; by slowing down and seeking second opinions, you remove their advantage.

# Empowerment Through Education: Know the Common Scams

Fraudsters rely on you not knowing the tactics they use, whether it's a phishing email, a fake charity, or a lottery scam.

By staying informed and continuously learning about common fraud schemes, you empower yourself to recognize suspicious behaviors and act accordingly. Awareness is your greatest tool in fighting fraud.

Otoño Consulting, LLC

# Thank You!


https://www.otonoconsulting.com/

Stephanie@otonoconsulting.com

505-244-8942

Stephanie W. Telles, MBA, CFE
Founder & CEO



Otoño Consulting, LLC

# Caregivers Against Senior Financial Exploitation

Benjamin Schrope, Acting Director

New Mexico Securities Division

OUR PRIORITY IS YOUR PROTECTION

NMRLD

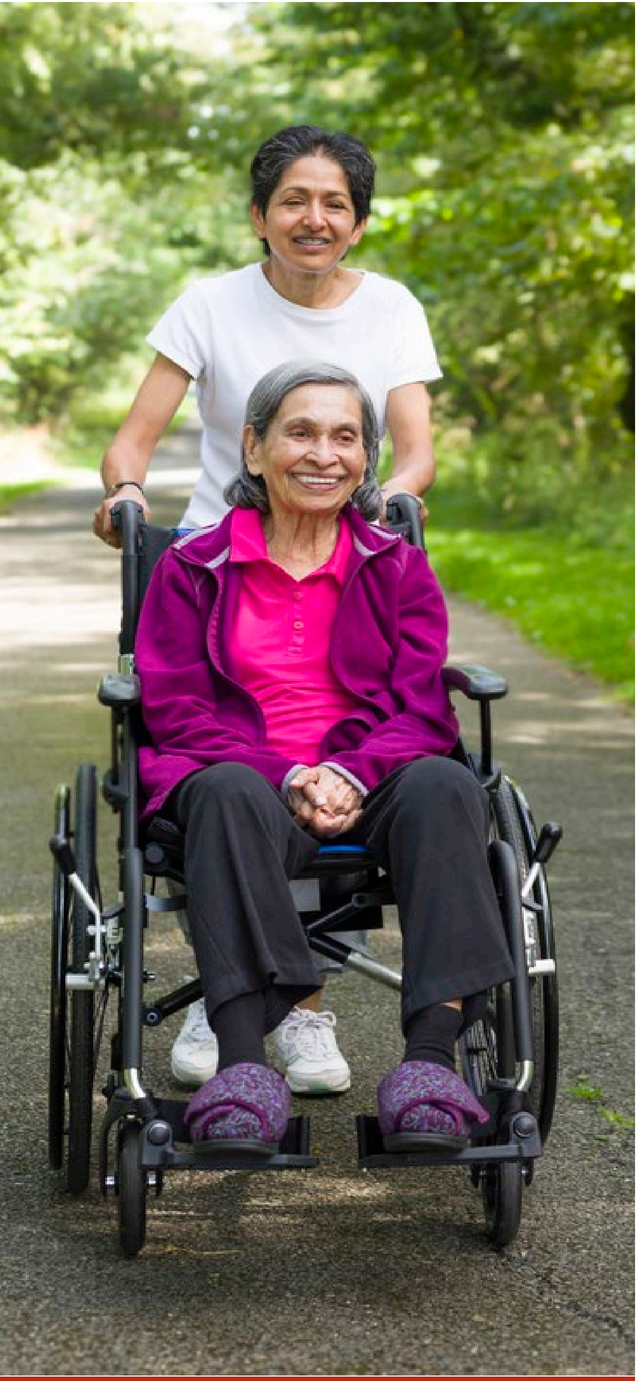
NEW MEXICO
REGULATION &
LICENSING DEPARTMENT

The **New Mexico Securities Division** is a regulatory agency with the State of New Mexico, organized to **protect the public** from unfair and deceptive **investment practices**.


# WHAT IS A SECURITY?

**A security is a broad financial term used to describe a wide range of investments, including stocks, bonds, promissory notes, limited partnership interests, and in some cases, cryptocurrencies.**

# CAREGIVERS ARE CRITICAL TO OUR SENIORS' WELL-BEING



# What type of caregiver are you?

## FORMAL

Caregiving services range from hired in-home care to paid care providers in a care setting:

- In-home caregivers provide services that range from light housekeeping and companionship to skilled health care
- Adult day care centers provide social activities, assistance, and supervision during the day, and offer relief to family caregivers
- Long-term care facilities such as nursing homes and assisted living facilities offer medical and personal care

## INFORMAL

Spouses, family members, friends:

- Unpaid helpers for older, sick, or disabled relatives, friends, and neighbors
- Care includes helping others handle daily activities such as bathing, managing medications, or preparing meals on their own
- Often starts gradually or may be triggered by a major medical event
- May have to manage financial and legal matters

# STATISTICS

**Estimated Number of U.S. Adults Who Are Caregivers:**

# 53 Million

**89% care for a relative or other loved one**

**About half of caregivers are caring for a parent or parent-in-law**

**12% cares for a spouse**

**43% of care recipients reside in their own home, and 40% reside in their caregiver's home**

**Approximately 61% of all caregivers are female, and 39% male**

**Source**: *Caregiving in the U.S. 2020,* AARP and the National Alliance for Caregiving Report, and The Family Caregiver Alliance: National Center on Caregiving

# Senior Financial Exploitation: Human Cost

The risk of dementia rises with age.

- In 2024, an estimated 6.9 million Americans age 65 and older are living with Alzheimer's dementia; 73% are age 75 or older

- By 2050, the number of people age 65 and older with Alzheimer's disease is expected to double, absent medical breakthroughs to prevent or cure the disease

# Perpetrators

Elder financial exploitation is approximately **$28.3 billion** annually

- **72% ($20.3 billion)** committed by people the victim knows
  - relatives, caregivers, friends, neighbors
  - perpetrators familiar to the victim are likely to make gradual moves, gaining access to funds by obtaining joint ownership or power of attorney status on their victims' accounts
- **28% ($8 billion)** committed by strangers
  - "wrong" numbers, romance scams, tech support scams, etc.
  - strangers usually rely on quick and irreversible transactions such as gift cards, wire transfers, and cryptocurrency

**Source**: *The Scope of Elder Financial Exploitation: What It Costs Victims,* AARP BANKSAFE INITIATIVE, 2023

# COMMON SCAMS AND SCHEMES AFFECTING SENIORS

# ADVANCE FEE FRAUD

- Involve requests for up-front money or account details to secure investor's involvement in their transaction
- Millions of dollars are promised in return for a product or service once the transaction is complete
- Examples are bogus prize scams, lottery scams, sweepstakes scams

# CHARITY FRAUD

- The act of using deception to get money from people who believe they are making donations to charities
- Common after high-profile disasters
- May also occur when a legitimate charity represents that funds will be used for a specific purpose, but the money is used for other purposes

# CONSTRUCTION AND HOME REPAIR FRAUD

- A person or company has been paid to perform a job, but either the job was not performed or the work was performed poorly or not completed
- A typical scenario involves an uninvited door-to-door solicitation from a contractor claiming to have a “special price” on roofing, siding, windows, asphalt, or other services

**TIP:**
**ALL CONTRACTORS AND HANDYMEN MUST BE LICENSED WITH THE NEW MEXICO CONSTRUCTION INDUSTRIES DIVISION**

# CREDIT CARD FRAUD

- The perpetrator obtains credit card information and uses it to charge items to victim's account
- Information could be obtained many ways such as physical theft, stolen from unsecured websites, or a skimmer device at a gas station or ATM card reader

# GOVERNMENT IMPOSTER SCAMS

- Con artists impersonate government employees using aggressive and sophisticated tactics
- For example, may use fake names and phony IRS identification badge numbers
- Con artists take advantage of people's deep fear of the IRS to scare them into providing sensitive information or money by phone, email, or regular mail

# GRANDPARENT SCAM

- A con artist calls or emails the victim posing as a relative in distress or someone claiming to represent the relative (such as a lawyer or law enforcement agent)
- The "relative" of the grandparent explains they are in trouble and needs their grandparent to wire them funds
- The victim is urged not to tell anyone, such as the parent of the “grandchild”
- The grandparent never hears from their fake grandchild again and is tricked out of hundreds or even thousands of dollars

# HOME OWNERSHIP OR LOAN FRAUD

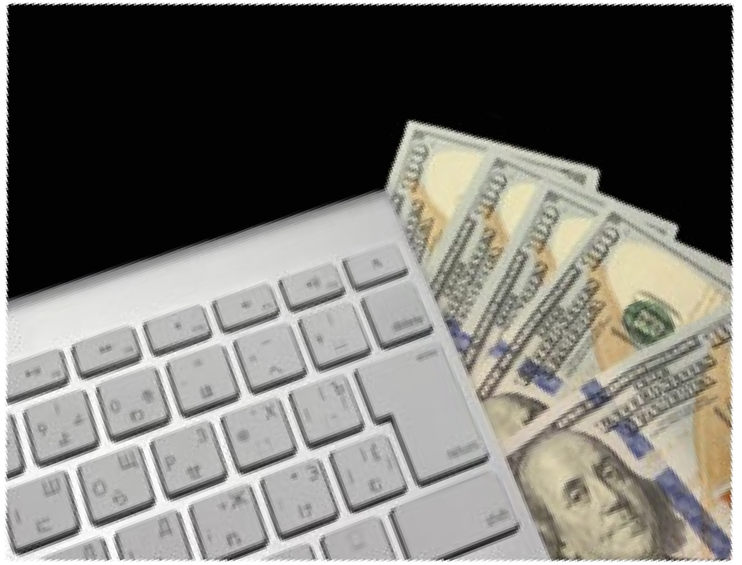
- **Signing Blank Documents:** The homeowner is tricked into signing a lien document or deed transfer that has been disguised as other paperwork. Or, a homeowner signs a blank document and the signature is used on a lien or transfer document.
- **Trusting People:** Seemingly trustworthy people befriend senior homeowners, gain their trust, and have them sign over their homes or set up home equity loans that allow the "friend" to unjustly access the homeowner's equity.
- **Deed Forgeries:** Scam artists forge the homeowner's signature on a blank "grant deed" in order to transfer ownership of property. With the phony deed, the scam artist can borrow against the equity in the home.

# LOTTERY AND SWEEPSTAKES SCAMS

- Calls or online solicitations that claim you were automatically entered in a sweepstakes you've never heard of before
- Con artist will ask the senior to play "fees" upfront before having access to winnings
- Once the con artist gets payment, the senior never receives any prize/winnings and the money is gone
- A person calls and says they have a winning state lottery ticket, but need help paying an upfront fee to collect on it

# TECH SUPPORT REPAIR SCAMS

- The scammer wants you to believe you have a serious problem with your computer, such as a virus
- They want you to pay for tech support services you don't need
- Will often attempt to pressure victim into paying by wiring money, putting money on a gift card, prepaid card, or cash reload card, or using a money transfer app



# INVESTMENT FRAUD

## Investment property schemes

The scams, sometimes pitched as "investment clubs," involve the purchase of properties at artificially inflated prices pitched as investment opportunities to naïve real estate investors who are promised improbably high returns and low risk

# INVESTMENT FRAUD

## Ponzi schemes

- The product being offered can be anything—foreign exchange, a stock trading model, securitized instrument, investment pool, precious metal, etc.
- High returns are usually promised
- Risk is often minimized
- There's often no legitimate product
- Investors are paid with money from new investors

# INVESTMENT FRAUD

## Private placements

- A “private placement” is an offering of unregistered securities to a small or limited pool of investors
- In a private placement, a company sells shares of stock or interest in the company, such as warrants or bonds, in exchange for cash from the investor

# INVESTMENT FRAUD

## Promissory note schemes

- A promissory note is a form of debt – similar to a loan or an IOU – that a company may issue to raise money.
- Typically, an investor agrees to loan money to a company for a set amount of time. In exchange, the company promises to pay the investor a fixed return on their investment, usually principal plus annual interest.
- While promissory notes can be legitimate investments, those marketed broadly to individual investors often turn out to be scams.

# INVESTMENT FRAUD

## Unregistered persons

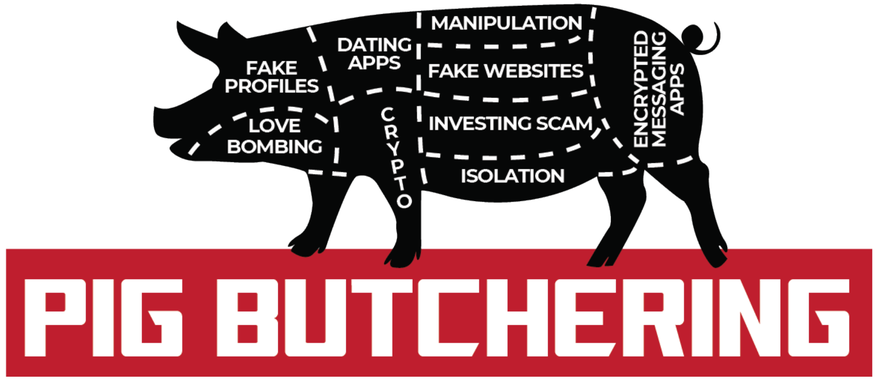
- Unregistered persons who sell securities perpetrate many of the securities frauds that target retail investors
- Always check whether the person offering to sell you an investment is registered and properly licensed, even if you know them personally

# ROMANCE SCAM

- Con artists use dating sites, apps, phone calls, and social media to scout for lovesick men and women
- After developing a relationship and gaining trust, the con artist says they are in need of money for an emergency such as to get out of a debt, a bad investment, medical bills, travel expenses, etc.
- They will promise to pay the victim back, but the victim will never see the money again

# PIG BUTCHERING SCAM

- Scammer makes contact with the target over long periods of time
- Scammer may start off contact by sending a wrong number text, email, social media message, or even through dating app
- Gaining trust before ultimately manipulating the targets into phony investments, usually in cryptocurrency, and disappearing with the money/funds.



# CRYPTOCURRENCY SCAMS

- The FBI warns of a spike in cryptocurrency investment schemes
- Investment fraud related to cryptocurrency rose from $2.57 billion in 2022 to $2.96 billion in 2023
- Increase in companies falsely claiming an ability to recover funds lost in cryptocurrency investment scams
- Criminals pose as non-fungible token (NFT) developers to target internet users interested in NFT acquisition


**IF YOU ARE ASKED TO SEND MONEY BY CRYPTOCURRENCY, IT IS A SCAM!**

# INVESTMENT FRAUD IS EVOLVING

## Artificial Intelligence and Deepfakes

Scammers use AI to create fake images, and even deepfake videos, designed to mislead you, often by faking an endorsement by a celebrity or pretending to be a relative.

- Create a word that only friends and family know to help identify potential scams
- Always check with the New Mexico Securities Division before investing money

## Fake Websites and Apps

Scammers send potential investors to convincing websites and apps created specifically to perform fraud.

- Be cautious of sites and apps you've never heard of
- Check app reviews carefully
- Always make sure the security is registered before investing

# VULNERABILITY FACTORS

# VULNERABILITY FACTORS

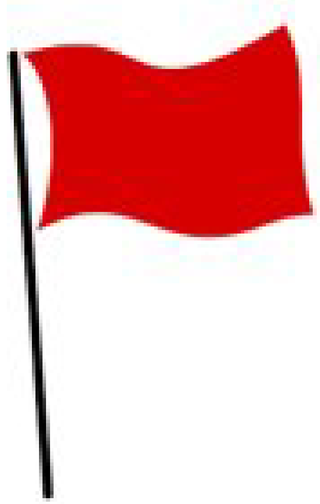
- Recent loss of spouse or partner and/or social isolation
- Financially responsible for adult child, grandchild, or other family member
- Recent change in health
- Socially isolated, depressed, or lonely
- Frequent mistakes in managing finances
- Excessive anxiety about finances

# VULNERABILITY FACTORS

- Running out of money at the end of the month
- Willingness to listen to telemarketing or other calls from unknown parties
- Pressure from children or others to share money or change will/trust
- Dependent on someone to provide everyday care, transportation, or other services

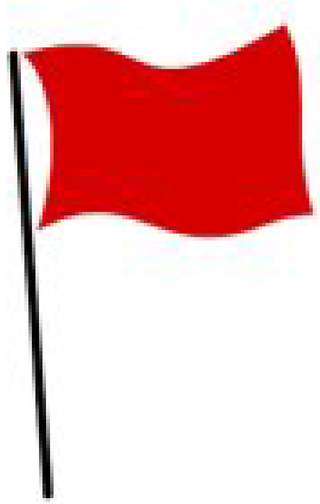
# RECOGNIZING RED FLAGS OF ELDER FINANCIAL ABUSE

# RED FLAGS of SENIOR FINANCIAL ABUSE



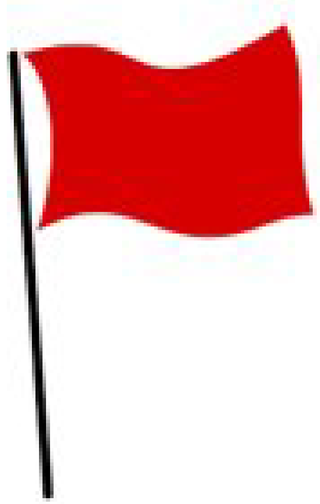
- Senior has moved away from existing relationships and toward new associations with other “friends” or strangers
- Senior displays unexplained or unusual excitement over a financial windfall or prize check; may be reluctant to discuss details

# RED FLAGS of SENIOR FINANCIAL ABUSE



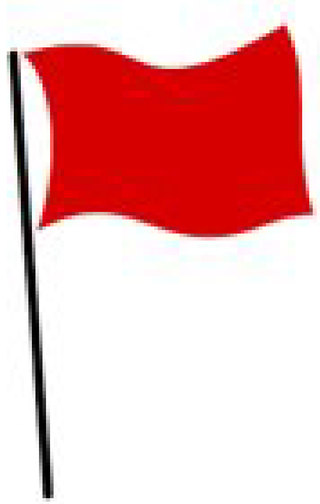
- Noticeable neglect or decline in appearance, grooming, or hygiene
- Sudden involvement of previously uninvolved relatives claiming their rights to the senior's affairs and possessions
- Abrupt changes to financial documents such as power of attorney, account beneficiaries, wills and trusts, property title, and deeds
- Unexplained disappearance of funds or valuable possessions

# RED FLAGS of SENIOR FINANCIAL ABUSE



- Suspicious signatures on the elder's checks or other documents
- Using elder's checks, debit, or credit cards without permission
- Significant increase in monthly expenses paid which may indicate that expenses for persons other than the elder are getting paid

# RED FLAGS of SENIOR FINANCIAL ABUSE



- Senior lacks knowledge about his/her financial status or shows reluctance to discuss financial matters
- Ongoing financial arrangements that the victim does not understand or recall giving consent
- Borrowing money with no intent to repay

# REPORTING SENIOR FINANCIAL FRAUD OR EXPLOITATION

# REPORTING TO ADULT PROTECTIVE SERVICES

If you have reason to believe there has been, or is about to be, abuse, neglect, or financial exploitation of a vulnerable adult or senior, it should always be reported to Adult Protective Services (APS):

Phone: **1-866-654-3219**

Website: **AGING.NM.GOV/protecting-adults**

If you are in doubt, call APS. APS will determine whether the senior needs assistance, and if not, APS may refer the senior to the appropriate local resources.

# REPORTING TO LAW ENFORCEMENT

Non-emergency reports can be made to local law enforcement agencies.

Remember, if you believe the customer is in **immediate danger**, always call 911.

# REPORTING TO YOUR STATE SECURITIES REGULATOR

New Mexico Securities Division:

- Assists with the investigation or referral of cases involving investment fraud
- Educates seniors on how to identify red flags for financial fraud and exploitation and how to protect themselves

Phone: **1-800-704-5533** or **505-476-4580**

Website: **RLD.NM.GOV/securities-division**

# HELPFUL RESOURCES

# RESOURCES

New Mexico Securities Division: **1-800-704-5533** or **505-476-4580** | **RLD.NM.GOV/securities-division**

North American Securities Administrators Association (NASAA): **www.nasaa.org**

Securities Exchange Commission (SEC): **www.investor.gov**

Commodity Futures Trading Commission: **www.cftc.gov**

Consumer Financial Protection Bureau: **www.consumerfinance.gov**

Internet Crime Complaint Center (IC3): **ic3.gov/Home/FileComplaint**

Financial Industry Regulatory Authority (FINRA): **www.finra.org/investors#**

FINRA Securities Helpline for Seniors: **844-57-HELPS (844-574-3577)**

# ADDITIONAL RESOURCES

Department of Health and Human Services **(www.hhs.gov)**

Federal Trade Commission **(www.ftc.gov)**

American Bar Association **(www.americanbar.org)**

National Adult Protective Services **(www.napsa-now.org)**

NMRLD

NEW MEXICO
REGULATION &
LICENSING DEPARTMENT

**New Mexico Securities Division**

# Protecting New Mexico Investors

**Compliance:** Check the license or registration of your broker/adviser

**Enforcement:** Report fraud

**Education:** Educational informational materials or additional presentations

**1-800-704-5533**

**RLD.NM.GOV/SECURITIES-DIVISION**