2025 Combatting AML Fraud Risk

WIPFLI

01

Fraud factoids

FTC fraud factoids

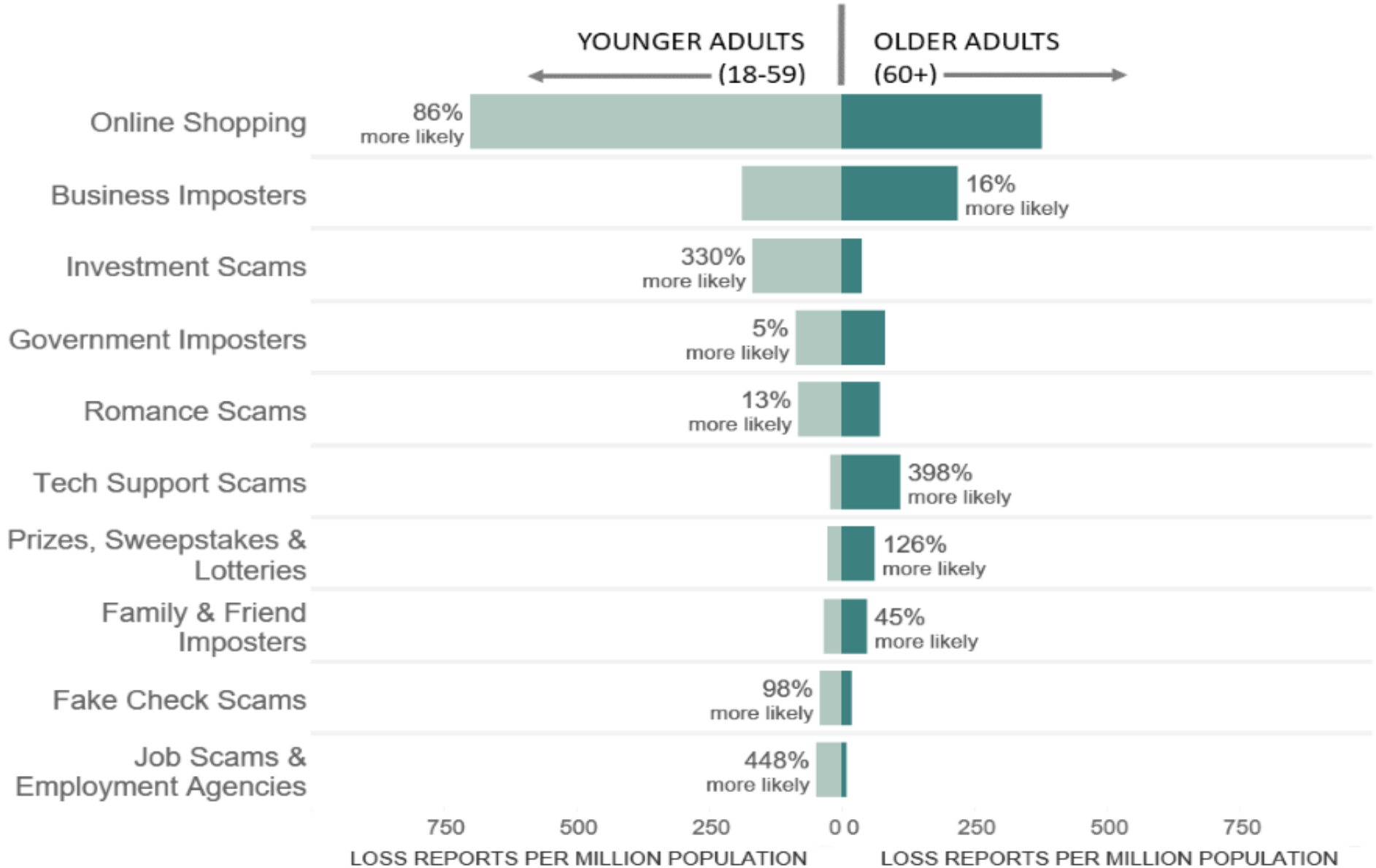
- FTC reported consumers lost nearly $10 billion in 2023 due to fraud. (Up from $8.8 billion in 2022)
  - Investment scams accounted for more than $4.6 billion, with the second highest being imposter scams at $2.7 billion followed by romance scam at $1.1 billion.
- The method of how scammers reach out to consumers:
  - Emails
  - Phone calls
  - Text messages
- Most common payment methods utilized:
  - Cryptocurrency (34%), wire transfer (27%), gift cards (7%), and payment apps (3%)

FTC fraud factoids

- In 2022, older adults (60 and over) are much more likely to report losses due to tech support scams, prize, sweepstakes/lottery frauds, family/friend imposters.
- Millennials, Gen X and Gen Z were much more likely to report losses due to online shopping fraud, which generally started out from an ad on social media.
  - They were also much more likely to report losses due to investment scams via bogus cryptocurrency investment scams.

2021 LOSS REPORTS BY AGE AND FRAUD TYPE

Losses to some types of fraud are more likely to be reported by younger adults, while others are more likely to be reported by older adults.



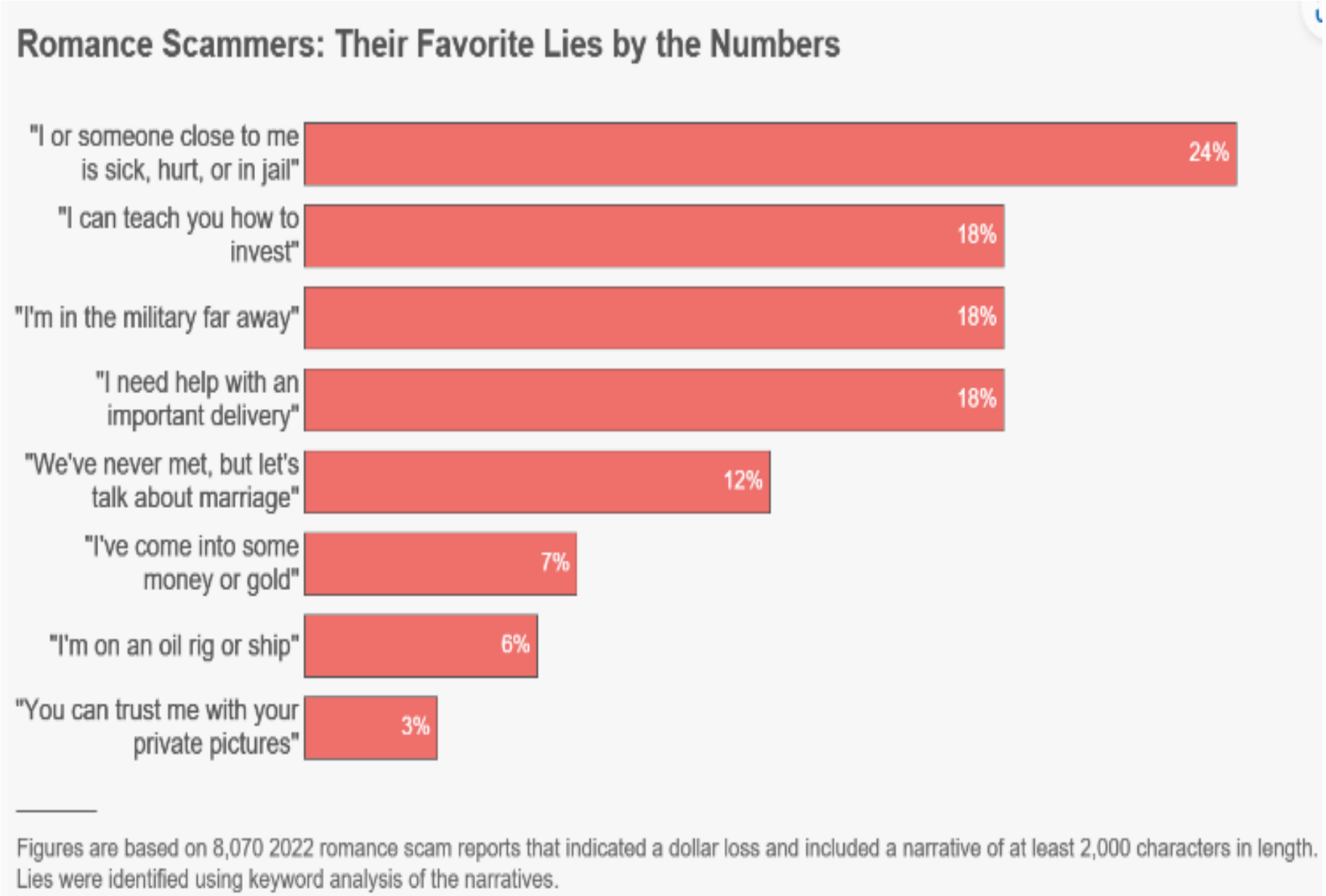
02

Fraud typologies

Fraud typologies

- Jobs & income opportunities that never existed
    - Mystery shopping (samples, exchange)
    - Car wrapping
    - Envelope stuffing
- Online selling
    - Offer deals that are too good to be true
    - Scammers send extra money via counterfeit/stolen check with instructions to return a portion.
    - Pose as real companies but sell fake or non-existent items.
- Romance scams

Lies by the numbers

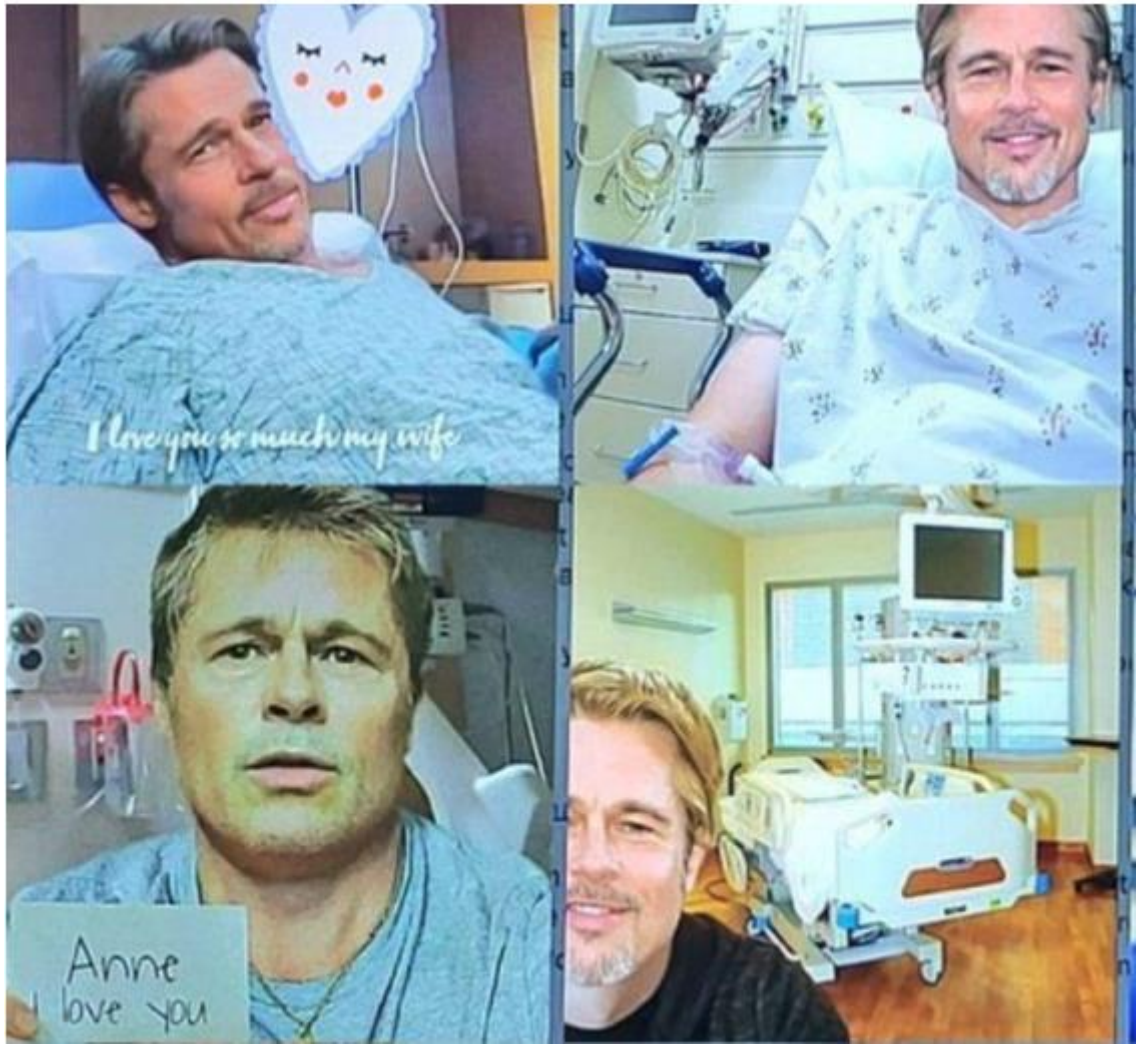


Romance scam example

- Country music signer. Trace Atkins, had to put out a public service announcement advising fans about fake fan Facebook, Twitter and Instagram accounts after hearing multiple victims being scammed.
- He said fraud victims were showing up to his concerts believing he invited them there or that they were engaged.
- They were scammed by fake VIP reps who reach out to fans on social media sites and then move the chat to private messaging.
- The were encouraged to send money to invest in a new album, buy a VIP celebrity meet and greet or even become romantically involved.
    - Trace Adkins has been married since 2019.

Romance scam example

- A wealthy French woman was duped into a year-long romance scam with an AI generated image of Brad Pitt. 50-year-old interior designer, “Anne” believed she was in a relationship with Brad and sent him $855,000 to help him with his kidney treatment.
- The scammers sent fake selfies of Brad in a hospital bed and even holding up personalized messages to her.
- She was contacted through Instagram by a person pretending to be Brad’s mother who used the AI photos to gain Anne’s trust.



03

Elder financial exploitation

Elder financial exploitation

- While EFE has state-specific statutes, an older adult is considered a person 60 years or older
- EFE is defined as an illegal or improper use of an older adult's funds, property, or assets; includes physical, emotional, or financial abuse
- Statutes may also include individuals who do not have the capacity to act on their own due to a disability (no minimum age)
- According to the FTC, in 2023, over $1.9 billion was reported but estimates the number is closer to $61.5 billion due to under reporting.

Elder financial exploitation

- Common scams
  - Romance scam
    - Scammers pose as interested romantic partners through dating websites to capitalize on their elderly victims' desire to find companions
  - Tech support scam
    - Perpetrators pose as technology support representatives and offer to fix non-existent computer issues, gaining remote access to victims' devices and thus, their sensitive information
  - Grandparent scam
    - Scammers pose as a relative, usually a child or grandchild, claiming to be in immediate dire financial need

Elder financial exploitation

- Government impersonation scam
  - Perpetrators pose as government employees (IRS) and threaten to arrest or prosecute victims unless they agree to provide funds or other payments
- Sweepstakes/charity/lottery scam
  - Perpetrators claim to work for legitimate charitable organizations to gain victims' trust or they claim their targets have won a foreign lottery or sweepstakes, which they can collect for a "fee"
- Home repair scam
  - Scammers appear in person and charge homeowners in advance for home improvement services that they never provide

Elder financial exploitation

- FIN-2022-A022 Behavioral Red Flags
  - Unusual changes in account contact information, such as updated emails or phone numbers
  - A customer with known cognitive impairment has unusual account activity
  - A customer who seems fearful or submissive and unable to answer basic questions about account activity, one who seems to be taking direction from a third party, or one who is fearful or submissive to their caretaker
  - A caregiver or family member who shows excessive interest in the customer's assets, does not allow the customer to speak for themselves, and is reluctant to leave the customer's side
  - A customer who mentions an online friend or romantic partner and wants to send money to join them in a business venture

Elder financial exploitation

- A customer who is agitated or frenzied about the need to send money immediately due to an “emergency” of a loved one, but the money is sent to an unconnected third party
- A new caretaker, friend, or relative who suddenly begins conducting financial transactions on behalf of the older person without documentation or suspect documentation (such as a POA)
- Your staff is unable to contact or speak directly to the customer
- Dormant accounts with large balances begin to show constant withdrawals or CDs are closed without regard for penalties
- A customer purchases large numbers of gift cards or inquires about buying Bitcoin
- Attempts to wire large sums of money or receives large wires (money mules)
- Frequent large uncharacteristic cash or ATM withdrawals, including daily maximum cash withdrawals from an ATM

Elder financial exploitation real life scenario

- A 60-year-old downstate Credit Union customer (member) lost $940,000 to a scammer who posed as the Credit Union's internal fraud investigator.
- She was contacted by the "investigator" to inform her that a CU employee was trying to illegally access her account and send out unauthorized wires.
- He convinced the victim to come into the local branch and conduct four separate wire transactions and provided an "explanation" for her to give to the CSR in case they questioned the transaction.
- He assured the victim these wires were just a ruse and would not be sent and not to be alarmed if she sees a wire debit from her account.
- She grew suspicious when the "investigator" stopped contacting her, which led her to contact the CU.
- The amount lost was her life savings.

Elder financial exploitation real life scenario – Part II

- Retired police chief in the western suburbs of Chicago had been sending wires in $25,000 increments to the Dominican Republic. The bank collected the purpose of the wire each time and all of the wires were related to buying property and building a vacation home.
- After the customer's savings were depleted, he tried to access his IRA accounts. Since he would have had significant penalties, the Branch Manager asked if he was really building a home or if he was sending money to a third party.
- The Chief whispered to the Manager, "I'm not supposed to share this information, but I actually won the lottery, and the funds are for upfront taxes on the $14 million he was about to receive."
- There was no lottery, and the customer lost over $400,000. He had responded to a direct message on his social media account.

AI fraud

Types of AI scams - FI concerns

- Employees are tricked into giving out sensitive customer data
  - Phishing scams – resembles a trusted source to click a link
  - Spear phishing - targeted to one employee or organization
    - Names of colleagues, managers, title are included
  - Voice cloning – is the really your customer on the phone?
- Opening accounts based on fraudulent identification and business documents
  - Synthetic identities
  - Deep fake voice and image of company executives

Synthetic identity fraud

- Synthetic identity fraud is increasing in the financial industry
- Two categories:
  - Manipulated synthetic fraud
    - Fraudulent identities generated are based on real identities but information such as a social security number, date of birth or other personal information is manipulated to hide credit history
  - Manufactured synthetic fraud
    - An identity is started by compiling data from multiple identities to create a new identity, then adding fake information to complete the new identity

Synthetic identity fraud

- Without a specific victim, it is difficult to detect and prevent fraud
  - No one to notify the FI that they have been a victim
  - Account may remain open for a long time without an alert
  - User can disappear and there is no recourse
- Victims are the FIs in these cases

05

Money mules and imposters

Don't be a Mule

Money mules are people who receive and transfer money obtained from victims of fraud. Transferring money/valuables on behalf of others only benefits criminals and may lead to serious consequences for you. DON'T be a mule!

Please note, no physical mail is associated with this notification.

uspis.gov/money-mule

Types of money mules

- Unwitting or unknowing
  - Those who are unaware
- Witting
  - Those who ignore red flags or act willfully blind
- Complicit
  - Aware of role and actively participate

Types of Money Mules

Unwitting or Unknowing

Individuals are unaware they are part of a larger scheme

- Often solicited via an online romance scheme or job offer
- Asked to use their established personal bank account or open a new account in their true name to receive money from someone they have never met in person
- May be told to keep a portion of the money they transferred
- Motivated by trust in the actual existence of their romance or job position

Witting

Individuals ignore obvious red flags or act willfully blind to their money movement activity

- May have been warned by bank employees they were involved with fraudulent activity
- Open accounts with multiple banks in their true name
- May have been unwitting at first but continue communication and participation
- Motivated by financial gain or an unwillingness to acknowledge their role

Complicit

Individuals are aware of their role and actively participate

- Serially open bank accounts to receive money from a variety of individuals/businesses for criminal reasons
- Advertise their services as a money mule, to include what actions they offer and at what prices. This may also include a review and/or rating by other criminal actors on the money mule's speed and reliability.
- Travel, as directed, to different countries to open financial accounts or register companies
- Operate funnel accounts to receive fraud proceeds from multiple lower level money mules
- Recruit other money mules
- Motivated by financial gain or loyalty to a known criminal group

Money mule red flags

- How to identify and prevent money mule scams
  - The customer claims they can earn a significant amount of “easy money”
  - The customer needs bank account information to provide to someone else
  - The customer states they will be an “agent” to help the other party avoid transaction charges or local taxes
  - Sudden purchases of gift cards that are out of pattern
  - Documentation provided by the customer includes poorly constructed sentences and bad grammar from the other party
  - Vague or inconsistent reason(s) for opening and account or sending/receiving a wire request

Imposter scams

- Imposter fraud
  - An imposter is a person who pretends to be someone else
    - A family member
    - A friend
    - A person you feel like you know but have not met in person
    - A company you do business with – maybe your bank
    - A company that can fix your computer
    - A company that gives out prizes
    - A charity that asks for donations

Imposter scams

- How to identify and prevent imposter scams
  - Customers tell you they were solicited “out of the blue”
  - The transaction needs to be rushed; the customer insists on getting it done quickly
  - The customer may be afraid of the consequences if they don’t pay
  - Similar “stories” are found on internet searches that were deemed to be fraud
  - The customer needs additional account information to give to someone else, including passwords, PINs, or account history

Imposter scams real life scenario

- A married couple requested a wire in the amount of $750,000 from their local Joliet bank office. They seemed to be in distress and urged staff that the wire needed to be sent immediately.
- Bank Officers talked to the customers, who told them their son was kidnapped and if they did not send these funds immediately, the kidnappers would kill him. They allowed the parents to talk to their son and they were able to identify his voice.
- While bank staff stated this is most likely a scam and if not, law enforcement should be involved, the couple was insistent and said they were mailed a finger belonging to their son.
- The wire was sent and two days later the couple came back and asked if it could be recalled. They were able to locate their son, who was traveling.
- Scammers were able to get details of the couple's wealth and son's travel from social media postings.

06

Pig butchering

FinCEN alert on “Pig Butchering” investment scam (FIN-2023-Alert005)

- As of March 2024, reported has claimed $75 billion since January 2020.
- These scams are referred to as "pig butchering" as they resemble the practice of fattening a hog before slaughter. The victims in this situation are referred to as "pigs" by the scammers who leverage fictitious identities, the guise of potential relationships, and elaborate storylines to "fatten up" the victim into believing they are in trusted partnerships.
- The scammers then refer to "butchering“ or "slaughtering" the victim after victim assets are stolen, causing the victims financial and emotional harm. In many cases, the "butchering" phase involves convincing victims to invest in virtual currency, or in some cases, over-the-counter foreign exchange schemes-all with the intent of defrauding them of their investment.

FIN-2023-Alert005

- Behavioral Red Flags
  - A customer with no history or background of using, exchanging, or otherwise interacting with virtual currency attempts to exchange a high amount of fiat currency from an existing or newly opened bank account for virtual currency or attempts to initiate high-value transfers to VASPs.
  - A customer mentions or expresses interest in an investment opportunity leveraging virtual currency with significant returns that they were told about from a new contact who reached out to them unsolicited online or through text message.
  - A customer mentions that they were instructed by an individual who recently contacted them to exchange fiat currency for virtual currency at a virtual currency kiosk and deposit the virtual currency at an address supplied by the individual.
  - A customer appears distressed or anxious to access funds to meet demands or the timeline of a virtual currency investment opportunity.

FIN-2023-Alert005

- Financial Red Flags
  - A customer uncharacteristically liquidates savings accounts prior to maturation, such as a certificate of deposit, and then subsequently attempts to wire the liquidated fiat currency to a VASP or to exchange them for virtual currency.
  - A customer takes out a HELOC, home equity loan, or second mortgage and uses the proceeds to purchase virtual currency or wires the proceeds to a VASP for the purchase of virtual currency.
  - A customer receives what appears to be a deposit of virtual currency from a virtual currency address at or slightly above the amount that the customer previously transferred out of their virtual currency account. This deposit is then followed by outgoing transfers from the customer in substantially larger amounts.

“Pig Butchering” real life scenario (ABC news)

- Lombard, Illinois woman Erika D* lost her life savings of nearly $1 million to a scammer using the "pig butchering" technique. Her husband passed away decades ago and recently Erika met a man online.
  - "He said that he loved me," she said. "Once he sent me a huge bouquet of flowers and the FBI said they were shocked that he did that.“ The FBI noted that part was just the “fattening up” stage.
- "He's working on an oil rig, and something broke down. Can I send him $20,000? And I said, 'Whoa.' I said, 'You know what? I need to pray about this,'" she said. "The second time I sent $35,000. Then two weeks later, another $35,000. His pastor is sending him $250,000. Can I match it? Which was a dumb thing."

“Pig Butchering” real life scenario (ABC news)

- Over time that money sent reached nearly $1 million. Erika said the scammer told her she would get double her money back in his investments. Instead, she now owes money back to her bank; cash which she took from her home equity loan. She also must pay taxes on her investment withdrawals.
- "There's $400 left. That's it, $400," she said.
- Erika was forced to sell her Lombard home and everything in it.

And finally….

- Heartland Tri-State Bank failed because its CEO, Shan Hanes embezzled over $47 million dollars from the Bank causing its collapse.
- In 2022, he clicked on a link which promised high dollar returns on crypto investments. After investing several hundred thousand dollars of personal funds and seeing a high rate of return, he illegally used Bank funds to invest further.
  - It appeared his “own” funds was actually monies embezzled from the local church and investment club.
- Through July 2023 he sent 11 unauthorized wires to purchase crypto on behalf of the Bank without authority to do so.
- The scheme unraveled when he approached a Bank customer for a $12 million loan to “help take his money out of the crypto investment.” The customer alerted regulators.
- In August 2024, Hanes was sentenced to 24-years prison in prison..

wipfli.com