Keeping up with fraudsters: Continuing the battle

Agenda

1 Introduction & statistics

2 Current fraud trends

3 Regulatory guidance

4 Questions

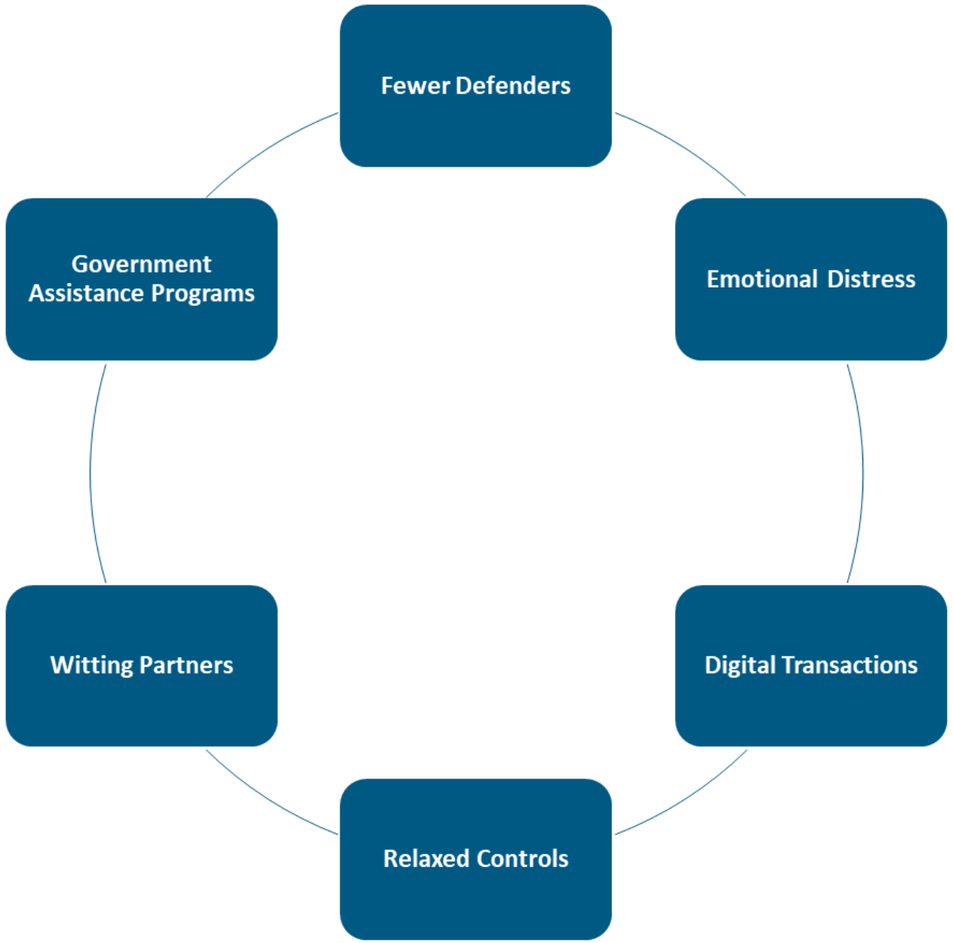
Introduction

The pandemic effect

The COVID-19 Impact - Natural Disaster

- Largest disaster in decades
- Financial devastation
- Loss of life and health
- The perfect storm for fraudsters

A golden opportunity for cybercriminals & fraudsters



Today’s World

- WFH is staying
- Isolation
- Greater online presence
- Need for newer, safer technology

The new normal

And…

An increase in fraud!

Fraud Statistics

Federal Trade Commission

2022 Statistics

Consumers lost $8.8 billion to fraud

44% increase over prior year

2.4 million fraud reports

Down from the annual record in 2021 of 2.9 million

FIs - $4 in costs for every dollar lost

That’s $35 billion

2023 is on target for increase

Too big to ignore!

Top scams of 2022

- Imposter scams
- Online Shopping
- Prizes, sweepstakes, lotteries
- Investment scams
- Business and job opportunities

Highest losses

- **Social media:** 1.2 billion total loss
  - Highest overall reported loss

- **Phone calls:** $1,400 median loss
  - Highest per person reported loss

FBI: 2021 Internet Crime Report

- 847,376 complaints (a record)
- 7% Increase from 2020
- Reported losses exceeding $6.9 billion

Fraud trends

Cybercrime

Cybercrime

- **Cyber threats:** any crime by use of a computer
  - Most serious threat to businesses and government entities
  - $1.5 trillion annually to the criminals
    - **Malware:** Hardware or software intentionally included or inserted in a system for a harmful purpose
    - **Ransomware:** A form of malware targeting human and technical weaknesses to make critical data or systems inaccessible – then demanding a ransom to release data

- Cyber attacks occur every 11 seconds
- $6 trillion is the estimated global impact of cyber crime in 2021
- $13 million is the average cost to organizations resulting from cyber crime
- 48% of cyber breaches involve small businesses

abrigo™

Cybercrime Red Flags

- Spelling of account names does not match the identity documentation
- Pictures in identity documentation are fuzzy or blurry
- Images of identity documentation have visual irregularities that suggest digital manipulation
- Customer’s physical description on identity documentation does not match other images of the customer
- Customer refuses to provide supplemental identity documentation or delays producing requested documentation.

Cybercrime Red Flags

- Customer logins occur from a single device or IP address across multiple seemingly unrelated accounts
- The IP address associated with logins does not match the stated address in identity documentation
- Customer logins occur during high network traffic times to avoid detection
- A customer notifies the financial institution to change account communication and authentication methods and then promptly attempts to move funds to an account that had not previously received payments from the customer

Business and investment fraud

Business and investment fraud (cont.)

- **Business email compromise (BEC)**: Criminals send email message that appears to come from a known source
- **Advance fee schemes**: Investors are asked to pay a fee upfront for an investment deal to go through
- **Nigerian letter (419 fraud):** Sender requests help facilitating the illegal transfer of money to get funds out of Nigeria
- **Ponzi schemes**: Use current investors' money to pay previous investors
- **Pyramid schemes**: Asks the investor to bring in new investors to make a profit or recoup their investment
- **Paycheck protection program** (PPP) and other government program fraud: Fraudulent loans, unemployment fraud, check fraud, etc.

Consumer fraud

Consumer fraud (including elder fraud)

- **Synthetic identity fraud:** Uses a combination of personally identifiable information to fabricate a fake person or entity to commit fraud for personal or financial gain.
- **Money mules:** Someone who transfers or moves illegally acquired money on behalf of someone else
- **Romance scams:** A criminal adopts a fake online identity to gain a victim's affection and trust
- **Skimming:** When devices illegally installed on ATMs, point-of-sale (POS) terminals or fuel pumps capture data or record cardholders' PINs
- **Spoofing and phishing (includes smishing and vishing)**: When someone disguises an email address, sender name, phone number, or website URL to convince you that you are interacting with a trusted source

Consumer fraud (cont.)

- **Grandparent scams:** Criminals pose as a relative—usually a child or grandchild—claiming to be in immediate financial need
- **Government impersonation scam:** Criminals pose as government employees and threaten to arrest or prosecute victims unless they agree to provide funds or other payments
- **Sweepstakes/charity/lottery scam:** Criminals claim to work for legitimate charitable organizations to gain victims' trust. Or they claim their targets have won a foreign lottery or sweepstake, which they can collect for a "fee."
- **Home repair scam:** Criminals appear in person and charge homeowners in advance for home improvement services that they never provide

Check fraud

- $18 billion in annual losses
- 500 million checks
- Over a million checks daily

Check fraud by mail red flags

- Non-characteristic large withdrawals on a customer's account via check to a new payee
- Customer complains of a check or checks stolen from the mail and then deposited into an unknown account
- Customer complains that the intended recipient never received a check they mailed
- Checks used to withdraw funds from a customer's account appear to be of a different check stock
- Existing customer with no history of check deposits has new sudden check deposits and withdrawal or transfer of funds

Check fraud by mail red flags (cont.)

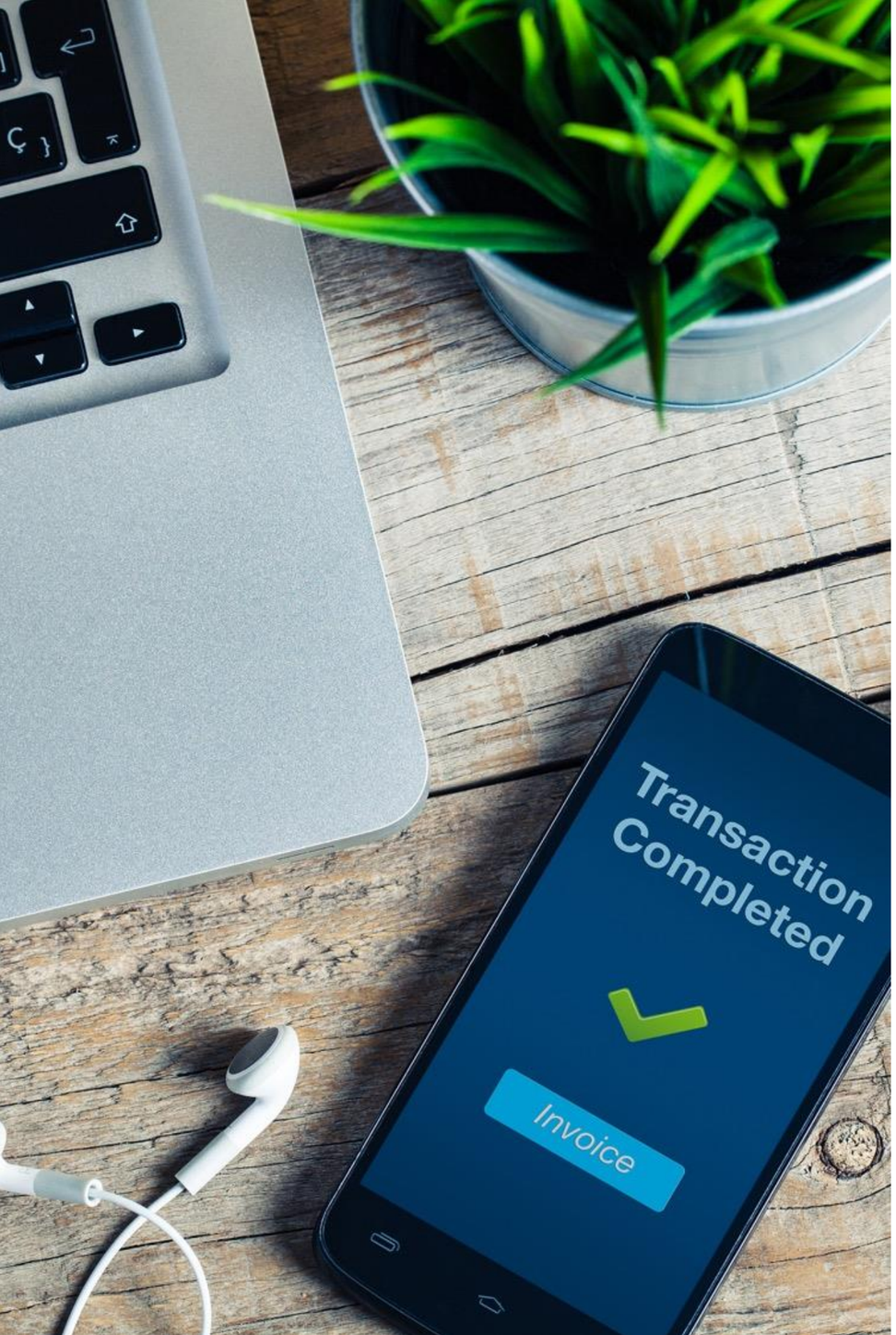
- Non-characteristic deposit of checks followed by rapid withdrawal or transfer of funds
- Examination reveals faded handwriting underneath darker handwriting, making the original writing appear overwritten
- Suspect accounts may have indicators of other suspicious activity, such as pandemic-related fraud
- New customer opens an account seemingly used only for depositing checks, followed by frequent withdrawals and transfer of funds
- A non-customer that is attempting to cash a large check or multiple checks in person and, when questioned, provides an explanation that is suspicious or potentially indicative of money mule activity

Check fraud by mail typologies

- **Check washing**: The use of a chemical process to “wash” the ink off of a check to be replaced with a new payee and possibly a new amount

- **Photocopying:** The mass duplication of checks through sophisticated photocopying

Regulatory Guidance



FinCEN Prioritizes:

- Extortion
- Social engineering
- Phishing/malware
- Business email compromise
- Ransomware

FinCEN Priorities

FinCEN Priorities - Fraud

Released June 30, 2020 – Eight priorities to fight financial crime threats

- Fraud is believed to represent the largest share of illicit proceeds in the United States

- Proceeds from fraudulent activities may be laundered through a variety of methods, including transfers through offshore entities, accounts controlled by cyber actors, and money mules

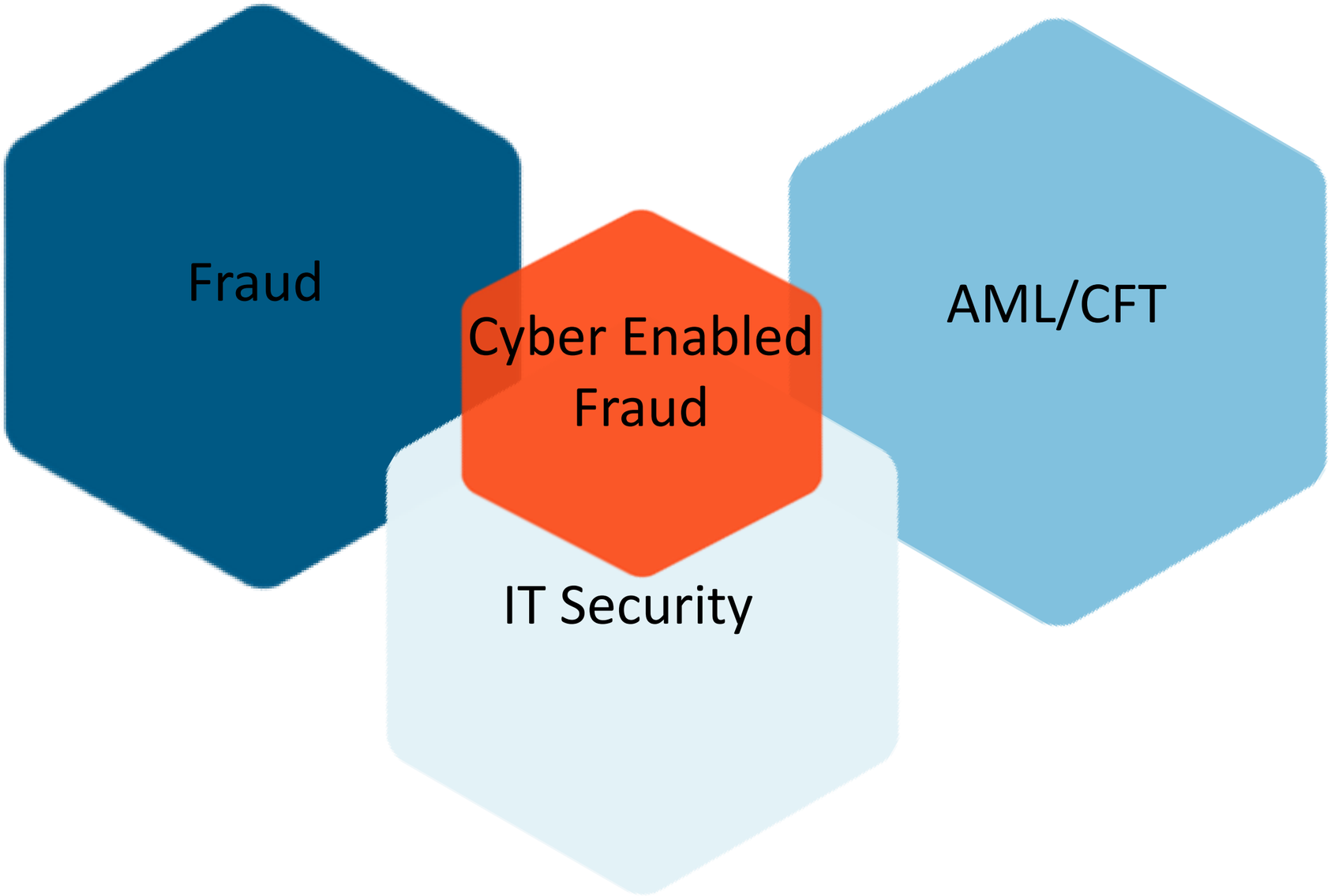
https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

FinCEN Priorities - Cybercrime

Cybercrime is defined as any illegal activity committed via the internet or otherwise involving computer technology.

- Cybercrime is one of the most significant threats posed to financial institutions

Collaboration



FinCEN Guidance

- Advisory on Cybercrime and Cyber-Enabled Crime (FIN-2020-A005)
- Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19) (FIN-2020-A003)
- Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (FIN-2021-A004)

abrigo™

FIN-2020-A005
Cybercrime & Cyber-Enabled Crime

- Targeting and Exploitation of Remote Platforms and Processes
- Phishing, Malware, and Extortion
- Business Email Compromise (BEC) Schemes

FIN-2020-A003
Imposter Fraud

Criminals acting as government officials, non-profit groups, universities, or charities

- Offering fraudulent or non-delivery of products or services:
  - Cures
  - Tests
  - Vaccines
- Price Gouging & Hoarding
  - PPE (including other face masks)
  - Hand sanitizer
  - Bleach
  - Toilet Paper

FIN-2020-A003
Money Mule Schemes

Bad actors recruiting individuals to transfer illegally acquired money on behalf of the fraudsters, typically using multiple accounts (i.e., solicitation to work from home for an unrealistic salary)

FIN-2020-A004
Ransomware

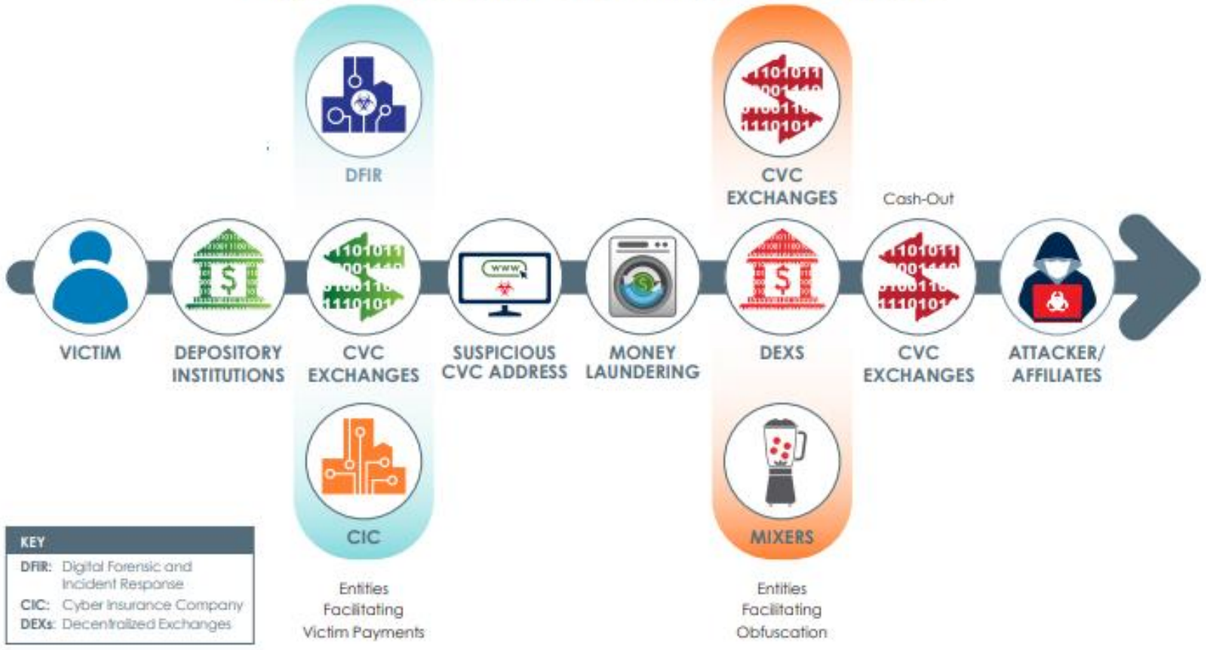
Increasing Sophistication of Ransomware Operations

- Big Game Hunting Schemes
- Ransomware Partnerships
- “Double Extortion” Schemes
- Use of Anonymity-Enhanced Cryptocurrencies (AECs) (i.e. Monero)
- Use of “Fileless” Ransomware

FIN-2021-A004

Advisory on ransomware and the use of the financial system to facilitate ransom payments

Figure 1. Movement of CVC in Ransomware Incidents



FIN-2022-A002

Advisory on Elder Financial Exploitation

- Elder theft: Schemes involving the theft of an older adult's assets, funds, or income by a trusted person

- Elder Scams: Scams involving the transfer of money to a stranger or imposter for a promised benefit or good that the older adult did not receive

Elder fraud red flags - behavioral

- An elder’s account shows sudden and unusual changes in contact information or new connections to emails, phone numbers, or accounts
- A customer with known physical, emotional, and cognitive impairment has unexplainable or unusual account activity
- An older customer appears distressed, submissive, fearful, anxious to follow others’ directions related to their financial accounts, or unable to answer basic questions about account activity
- An older customer mentions how an online friend or romantic partner asks them to receive and forward money to one or more individuals on their behalf or open a bank account for a “business opportunity.”

Elder fraud red flags – behavioral (cont.)

- During a transaction, an older customer appears to be taking direction from someone with whom they are speaking on a cell phone, and the older customer seems nervous, leery, or unwilling to hang up
- An older customer is agitated or frenzied about the need to send money immediately in the face of a purported emergency of a loved one, but the money would be sent to the account of a seemingly unconnected third-party business or individual
- A caregiver or other individual shows excessive interest in the older customer's finances or assets, does not allow the older customer to speak for himself or herself or is reluctant to leave the older customer's side during conversations
- An older customer shows an unusual degree of fear or submissiveness toward a caregiver or expresses a fear of eviction or nursing home placement if money is not given to a caretaker

Elder fraud red flags – behavioral (cont.)

- The financial institution is unable to speak directly with the older customer, despite repeated attempts to contact him or her
- A new caretaker, relative, or friend begins conducting financial transactions on behalf of an older customer without proper documentation
- An elder's financial management changes, such as through a power of attorney, trust, or estate planning, to a different family member or a new individual
- An older customer lacks knowledge about his or her financial status or shows a sudden reluctance to discuss financial matters

Financial red flags

- Dormant accounts with large balances begin to show constant withdrawals
- An older customer purchases large numbers of gift cards or prepaid access cards
- An older customer suddenly begins discussing and buying CVC
- An older customer sends multiple checks or wire transfers with descriptors in the memo line such as “tech support services,” “winnings,” or “taxes”
- Uncharacteristic, sudden, abnormally frequent, or significant withdrawals of cash or transfers of assets from an older customer’s account
- Sudden or frequent non-sufficient fund activity

Financial red flags (cont.)

- An older customer receives and transfers money interstate or abroad to recipients with whom they have no in-person relationship Frequent large withdrawals, including daily maximum currency withdrawals from an ATM
- Uncharacteristic nonpayment for services, which may indicate a loss of funds or access to funds
- Debit transactions that are inconsistent for the older customer
- Uncharacteristic attempts to wire large sums of money
- Closing of CDs or accounts without regard to penalties

Key Takeaways

Key Takeaways

- Many typologies exacerbated by the pandemic continue to provide criminals success while more complex schemes, such as cryptocurrency scams, are surfacing
- A worsening economy increases the fundamentals of fraud, pressure, opportunity, and rationalization, including an increase in potential fraud by internal sources - your trusted employees
- Update your financial institution's enterprise-wide risk assessment with expected trends and plan your fraud mitigation processes
- Be one step ahead by detecting and preventing fraud schemes before they become hard dollar losses

Questions?

Thank you