

Anti-Financial Crime Briefing

FinCEN Advisory on Elder Financial Exploitation

Summary

In support of World Elder Abuse Day, on June 15, 2022, the Financial Crimes Enforcement Network (FinCEN) released an advisory alerting financial institutions to “the rising trend of elder financial exploitation (EFE) targeting older adults”.¹ According to the Department of Justice (DOJ), elder abuse, including EFE, affects at least 10% of older adults each year in the United States, with more than US\$3 billion lost to financial fraud annually as of 2019.² Though EFE is the most common form of elder abuse, most incidents go unidentified and unreported due to fear, embarrassment, and lack of resources.³

Key Takeaways

- Elder financial exploitation (EFE) has been increasing over the years, with schemes generally involving either theft of assets by a trusted person or scams involving transfers of money to unknown/imposter fraudsters.
- Common elder scams include government imposter scams, romance scams, emergency/person-in-need scams, lottery/sweepstakes scams, and tech/customer support scams.
- Red flag indicators can include both behavioral and transactional suspicious activity. It is important for analysts to report suspicious activity tied to EFE.

Context

Why are elderly victims targeted?

Elder financial exploitation (EFE) is defined as “the illegal or improper use of an older adult’s funds, property, or assets”.⁴ There are many reasons elderly victims are targeted; FinCEN cites reasons including: having accumulated lifelong savings, facing declining cognitive or physical abilities, isolation from family/friends, lack of comfort with technology, and reliance on others for their wellbeing, financial management, and social interaction, with COVID-19 “exacerbating all of these vulnerabilities”.⁵

A growing trend

In 2020, the Consumer Financial Protection Bureau (CFPB) estimated US\$3.4 billion in suspicious transactions related to EFE, “an increase in \$2.6 billion from 2019”.⁶ In 2021, the Federal Trade Commission (FTC) estimated that older adults accounted for 35% of victims

1. FinCEN, June 15, 2022, “FIN-2022-A002: Advisory on Elder Financial Exploitation”, https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN_Advisory_Elder_Financial_Exploitation_FINAL_508.pdf

2. Ibid.

3. Ibid.

4. Consumer Financial Protection Bureau, United States Department of the Treasury, and FinCEN, August 30, 2017, “Memorandum on Financial Institution and Law Enforcement Efforts to Combat Elder Financial Exploitation”, https://www.fincen.gov/sites/default/files/2017-08/8-25-2017_FINAL_CFPB+Treasury+FinCEN_Joint_Memo.pdf

5. FinCEN, June 15, 2022, Op. Cit.

6. Ibid.

associated with filed fraud reports. Therefore, it is clear that EFE is increasing with time, and financial institutions need to be aware of the illicit financial flows and potential red flag indicators tied to elder financial exploitation.

Common EFE Schemes

Generally, EFE schemes involve either elder theft or elder scams. The perpetrators will often be known or trusted persons of the older adults in theft schemes, while scams can include fraudsters with no known relationship to their victims. In addition to assets being stolen, the victim's personally identifiable information (PII) can be stolen and sold on the black market.

Fraud

Elder fraud schemes often involve family members (46% of elder theft cases between 2013–2019⁷), while trusted persons including neighbors, financial service providers, friends, associates, or those in close proximity account for many other cases. Perpetrators will use deception, intimidation, and coercion against older adults for “access, control, and misuse”⁸ of their finances; they will also take advantage of any physical or cognitive disability. This can include but is not limited to: exploiting legal guardianships, power of attorney arrangements, or the use of fraudulent investments. Perpetrators may steal social security benefit checks, liquidate savings/retirement accounts, transfer assets/property, and max out credit cards.

Scams

In elderly scams, perpetrators “defraud victims into sending payments and disclosing PII under false pretenses or for a promised good the victim never receives”. “Perpetrators are usually located outside of the United States and have no known relationship to the victim”.⁹ They will contact the victim as a fictitious person via methods such as phone call, email, social media, mail, and online dating apps. Perpetrators request payments through transfers at money service businesses (MSBs) but are “increasingly requesting payments via prepaid access/ gift cards, convertible virtual currency, ATM deposits, money orders, or tracked deliveries of cash”.¹⁰ Some victims may also unknowingly serve as money mules for criminals.

Financial Institution Considerations

Red flags

A list of both behavioral and transactional red flags tied to EFE payments can be found in the FinCEN advisory. Some important red flags to note include:¹¹

- An older customer's account shows sudden and unusual changes in contact information, including new connections to emails, phone numbers, or accounts that may originate overseas
- Dormant accounts with large balances begin to show constant withdrawals

7. FinCEN, June 15, 2022, Op. Cit.

8. Ibid.

9. Ibid.

10. Ibid.

11. FinCEN, February 11, 2022, “Fact Sheet on the Rapid Response Program (RRP)”, https://www.fincen.gov/sites/default/files/shared/RRP_Fact_Sheet_Notice_FINAL_508.pdf

- An older customer sends multiple checks or wire transfers with memo line descriptions including “winnings”, “taxes”, or “tech support services”
- Closing of certificates of deposit (CDs) or accounts without regard to penalties

SAR requirements

The FinCEN advisory includes a reminder to financial institutions of their suspicious activity reporting requirements and the ability to share information under the USA Patriot Act. The advisory also includes a SAR best practice section for suspected EFE activity. When filing a SAR tied to EFE, an analyst should use these tips to increase the effectiveness of the SAR.

SAR filing considerations

- SAR field #2 (“Filing Institution Note to FinCEN”) reference: **EFE FIN-2022-A002**
- SAR check box: **check SAR Field 38(d) for Elder Financial Exploitation**

SAR narrative best practices, as applicable:

- Provide a statement in the narrative documenting the age and location (county/city) of the target or victim. Provide details about the reporting entity’s response, e.g. whether accounts were closed, whether the person was warned that transactions appear to involve fraud, if the person was not permitted to conduct new transactions, etc.
- Indicate whether any amount was refunded to the victim.
- Cross report the circumstances leading to the filing of the SAR directly to law enforcement and, as applicable to your state, report to Adult Protective Services (APS). Indicate in the LE contact field if law enforcement or APS was contacted.
- Reference and maintain supporting documentation, including photos or video footage, in the narrative, and expedite responses to law enforcement requests for supporting documentation.

Provide contact information – including name, email, or phone number – for a direct liaison within the AML/BSA or fraud department related to the SAR, so that law enforcement or APS can request documentation in a timely manner.

Supporting victims

In the advisory, FinCEN summarizes the Rapid Response Program (RRP) that helps victims and their financial institutions to recover funds stolen as the result of certain cyber-enabled financial crime schemes, including cyber-enabled fraud against older adults. The RRP factsheet can be found [here](#).

FinCEN also advises financial institutions to refer their older customers to the DOJ’s National Elder Fraud Hotline at 833-FRAUD-11 (833-372-8311), for support, resources, and assistance. If there is any indication of physical danger or imminent threat, FinCEN encourages institutions to report this activity to local authorities. In addition, institutions should contact Adult Protection Services and Area Agencies on Aging within their local area. Questions about the advisory should be sent directly to the FinCEN Resource Center at frc@fincen.gov.

Key Actions for Compliance

- Ensure SAR filing procedures and quality control steps are in place to include the appropriate reference (and corresponding nexus) in the SAR form and narrative, and indicate the connection between the suspicious activity being reported and the red flags or activities highlighted in the alert.
- Validate that appropriate team members are aware of the SAR form and SAR narrative considerations identified in EFE FIN-2022-A002, to make sure the SAR form requests made by FinCEN are addressed.
- Ensure appropriate staff, including front-line tellers, customer-facing employees, and call center representatives are frequently trained on the applicable behavioral red flags identified within the advisory.
- Include examples of red flag indicators of elder financial exploitation in training updates.
- Evaluate your transaction monitoring program to ensure the red flags identified in the alert would be identified within your systems.
- When filing an 8300 form involving suspicious transactions relevant to this advisory, select box 1b (“suspicious transactions”) and include the “EFE FIN-2022-A002” in the “Comments” section of the report.
- When conducting a 314(b) information sharing request, consider indicating that the reason for the request is respective to possible elder financial exploitation.

Authors

Tiffany Polyak, CAMS, Project Coordinator/Researcher

Lauren Kohr, Senior Director, AML – Americas

June 2022

About ACAMS

ACAMS is the largest international membership organization dedicated to providing opportunities for anti-financial crime (AFC) education, best practices, and peer-to-peer networking to AFC professionals globally. With over 90,000 members across 180 jurisdictions, ACAMS is committed to the mission of ending financial crime through the provision of anti-money laundering/counterterrorism-financing and sanctions knowledge-sharing, thought leadership, risk-mitigation services, ESG initiatives, and platforms for public-private dialogue. The association’s CAMS certification is the gold-standard qualification for AFC professionals, while the CGSS certification is its premier specialist qualification for sanctions professionals. ACAMS’ 60 Chapters globally further amplify the association’s mission through training and networking initiatives.

For more resources on ESG and social impact issues, visit the ACAMS Insights hub:

www.acams.org/insights