FinCEN ADVISORY

FIN-2022-A002 **June 15, 2022**

Advisory on Elder Financial Exploitation

Amid rampant fraud and abuse targeting older adults, FinCEN urges financial institutions to detect, prevent, and report suspicious financial transactions.

Elder financial exploitation (EFE) is defined as the illegal or improper use of an older adult's funds, property, or assets.[1]

SAR Filing Request:
FinCEN requests that financial institutions reference the advisory by including "**EFE FIN-2022-A002**" in SAR field 2 ("Filing Institution Note to FinCEN"), and mark the check box for elder financial exploitation.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to the rising trend of EFE targeting older adults[2] and to highlight new EFE typologies and red flags since FinCEN issued the first EFE Advisory in 2011.[3] FinCEN is also issuing this advisory in support of World Elder Abuse Awareness Day, which has been commemorated on June 15 every year since 2006 and provides an opportunity for communities around the world to promote a better understanding of abuse and neglect of older adults by raising awareness of the related cultural, social, economic, and demographic factors.[4]

According to the U.S. Department of Justice, elder abuse, which includes EFE among other forms of abuse, affects at least 10 percent of older adults each year in the United States,[5] with millions of older adults losing more than $3 billion to financial fraud annually as of 2019.[6] Despite the

1. EFE is one type of elder abuse, which includes physical, emotional, and financial abuse. Elder abuse and EFE definitions vary statutorily by state. For more information on the definition of EFE, *see* Consumer Financial Protection Bureau (CFPB) and FinCEN, "Memorandum on Financial Institution and Law Enforcement Efforts to Combat Elder Financial Exploitation," (Memorandum on EFE) (August 30, 2017); *see also*, U.S. Department of Justice (DOJ) webpage, Elder Abuse and Elder Financial Exploitation Statutes.
2. For purposes of this advisory and consistent with other U.S. government agencies' use of the term, an older adult is considered an individual 60 years of age or older. *See* Federal Trade Commission (FTC) Report, "Protecting Older Consumers, 2020-2021," (Older Consumers Report) (October 18, 2021), at p. 1.
3. *See* FinCEN, "Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation," (2011 Advisory) (February 22, 2011).
4. For more information about World Elder Abuse Awareness Day, *see* Administration for Community Living (ACL), World Elder Abuse Awareness Day.
5. For more information on EFE, *see* DOJ, About Elder Abuse.
6. *See* Internet Crime Complaint Center (IC3), "Perpetrators Use Various Methods to Deceive and Defraud Elderly Victims For Financial Gain," (September 19, 2019). Fraud (of all types) is the largest proceeds-generating offense in the United States and is one of the FinCEN June 2021 anti-money-laundering/counter-financing-of-terrorism (AML/CFT) National Priorities.

fact that EFE is the most common form of elder abuse, the majority of incidents go unidentified and unreported as victims may choose not to come forward out of fear, embarrassment, or lack of resources.[7] Older adults are targets for financial exploitation due to their income and accumulated life-long savings, in addition to the possibility that they may face declining cognitive or physical abilities, isolation from family and friends, lack of familiarity or comfort with technology, and reliance on others for their physical well-being, financial management, and social interaction.[8] The COVID-19 pandemic exacerbated these vulnerabilities for many older adults.[9] In 2020, over 62,000 suspicious activity reports (SARs) related to EFE were filed, totaling what the Consumer Financial Protection Bureau (CFPB) estimates to be $3.4 billion in suspicious transactions, an increase from $2.6 billion in 2019. This is the largest year-to-year increase since 2013.[10] This trend has continued with over 72,000 SARs related to EFE filed in 2021 and, according to the Federal Trade Commission (FTC), older adults now account for 35 percent of the victims associated with filed fraud reports in cases when a consumer provided an age.[11]

The U.S. government has multiple initiatives in place to counter perpetrators and facilitators of EFE.[12] In support of this whole-of-government approach, FinCEN collaborates with law enforcement, regulatory agencies, and financial institutions to ensure that SARs appropriately identify and report suspicious activity potentially indicative of EFE. Financial institutions are uniquely situated to detect possible financial exploitation through their relationships with older customers. They therefore play a critical role in helping to identify, prevent, and report EFE to law enforcement and their state-based Adult Protective Services,[13] and any other appropriate first

7. *See* CFPB and FinCEN, Memorandum on EFE, *supra* Note 1. *See also,* FTC Older Consumers Report, *supra* Note 2.
8. *See* CFPB and FinCEN, Memorandum on EFE, *supra* Note 1.
9. *See* DOJ Office of Public Affairs (OPA), "Associate Attorney General Vanita Gupta Delivers Remarks at the Elder Justice Coordinating Council Meeting," (December 7, 2021); *see also,* DOJ OPA, "Statement of Attorney General Merrick B. Garland on World Elder Abuse Awareness Day," (June 15, 2021); and "Associate Deputy Attorney General Paul R. Perkins Delivers Remarks at the ABA/ABA Financial Crimes Enforcement Conference," (December 9, 2020).
10. *See* CFPB, "Suspicious Activity Reports on Elder Financial Exploitation."
11. *See* FinCEN, SAR Stats; and FTC, "Consumer Sentinel Network: Data Book 2021," (February 2022), at p. 13.
12. *See* DOJ's Elder Justice Initiative, Transnational Elder Fraud Strike Force, and Money Mule Initiative. For U.S. government efforts to address romance scams, *see* Dating or Defrauding: A National Awareness Campaign. Additionally, passed in 2010, the Elder Justice Act was the first comprehensive legislation to address the abuse, neglect, and exploitation of older adults at the federal level. The law authorized a variety of programs and initiatives to better coordinate federal responses to elder abuse, promote elder justice research and innovation, support Adult Protective Services systems, and provide additional protections for residents of long-term care facilities. Further, the Elder Justice Act established the Elder Justice Coordinating Committee to coordinate activities related to elder abuse, neglect, and exploitation across the federal government. For more information about the Elder Justice Act and the associated Committee, visit the Administration for Community Living, Elder Justice Act. *See also,* the National Center on Elder Abuse (NCEA).
13. According to the National Adult Protective Services Association (NAPSA), "Adult Protective Services (APS) programs promote the safety, independence, and quality-of-life for vulnerable adults who are, or are in danger of, being abused, neglected by self or others, or financially exploited, and who are unable to protect themselves. APS is a social service program authorized by law in every state to receive and investigate reports of elder or vulnerable adult maltreatment and to intervene to protect the victims to the extent possible." *See* NCEA, NAPSA, and Keck School of Medicine of USC, "Fact Sheet: Adult Protective Services, What You Must Know;" and NCEA, Adult Protective Services; and How APS Works.

responder as well as assisting older customers who fall victim to financial exploitation.[14] The information contained in this advisory is derived from FinCEN's analysis of Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners.

Trends and Typologies of EFE and Associated Payments

EFE schemes generally involve either theft or scams.[15] Perpetrators of elder theft are often known and trusted persons of older adults, while scams, which can disproportionally affect older adults, frequently involve fraudsters, often located outside of the United States, with no known relationship to their victims.[16] Regardless of the relationship, these criminals can place older adults in financially, emotionally, and physically compromising situations, and the resulting loss of income and life-long earnings can be devastating to the financial security, dignity, and quality of life of the victims.[17]

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.

Unfortunately, perpetrators of EFE schemes often do not stop after first exploiting their victims. In both elder theft and scams, older adults are often re-victimized and subject to potentially further financial loss, isolation, and emotional or physical abuse long after the initial exploitation due to the significant illicit gains at stake.[18] Scammers may also sell victims' personally identifiable information (PII) on the black market to other criminals who continue to target the victims using new and emerging scam typologies.[19]

Elder Theft

Perpetrators of elder theft are often family members and non-family caregivers who abuse their relationship and position of trust. As identified by FinCEN in 2019 in its analysis of a statistically

14. Reporting EFE to APS, law enforcement, or other authorities is an opportunity to strengthen prevention and response. *See* CFPB, "Reporting of Suspected Elder Financial Exploitation by Financial Institutions," (July 17, 2019); "Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends," (February 2019); CFPB and FinCEN, Memorandum on EFE, *supra* Note 1; and Federal Reserve, CFTC, CFPB, FDIC, FTC, NCUA, OCC, and SEC, "Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults," (September 24, 2013).
15. *See* FinCEN Financial Trend Analysis (FTA), "Elders Face Increased Financial Threat from Domestic and Foreign Actors," (December 2019), at p. 4.
16. *Id.*
17. *See* CFPB and FinCEN, Memorandum on EFE, *supra* Note 1.
18. For additional information on re-victimization in EFE schemes, *see* FINRA Investor Education Foundation (FINRA Foundation), American Association of Retired Persons (AARP), and Heart+Mind Strategies, "Addressing the Challenge of Chronic Fraud Victimization," (March 2021).
19. *See* DOJ, "List Brokerage Firm Pleads Guilty to Facilitating Elder Fraud Schemes," (September 28, 2020).

significant, random sampling of SAR narratives, a family member was involved in the theft of assets from older adults in 46 percent of elder theft cases reported between 2013 and 2019.[20] Trusted persons who commit elder theft can also include familiar associates and acquaintances such as neighbors, friends, financial services providers, other business associates, or those in routine close proximity to the victims.

Instances of elder theft often follow a similar methodology in which trusted persons may use deception, intimidation, and coercion against older adults in order to access, control, and misuse their finances. Criminals frequently exploit victims' reliance on support and services and will take advantage of any cognitive and physical disabilities,[21] or environmental factors such as social isolation, to establish control over the victims' accounts, assets, or identity.[22] This can take many forms, including the exploitation of legal guardianships[23] and power of attorney arrangements,[24] or the use of fraudulent investments such as Ponzi schemes[25] to defraud older adults of their income and retirement savings. These relationships enable trusted persons to repeatedly abuse the victims by liquidating savings and retirement accounts, stealing Social Security benefit checks and other income, transferring property and other assets, or maxing out credit cards in the name of the victims until most of their assets are stolen.[26]

Case Study on Elder Theft

Housekeeper and Co-Conspirators Exploit Dementia-afflicted Older Adult

A woman in Charlotte, North Carolina was convicted and sentenced to 97 months in prison and two years of supervised release for conspiracy to commit wire fraud and money laundering conspiracy. Donna Graves, who was the ringleader of the criminal conspiracy, conspired to engage in a scheme to defraud a victim identified in court documents as "K.T." The victim was an elderly widow who lived alone and suffered from dementia and other physical and mental challenges. During the relevant time period, Graves and her co-conspirators (Gerald Maxwell Harrison and Elizabeth Robin Williams) exploited K.T.'s vulnerabilities and defrauded the victim through a web of forged documents, lies, and deceptions. According to evidence presented at Graves' trial, beginning in 2014, Graves and Williams provided housekeeping services for the victim through a business owned and operated by Graves. Over the course of the scheme, the co-conspirators isolated the victim from her friends and family, induced

20. *See* FinCEN FTA, *supra* Note 15, at p. 7.
21. *Id.*
22. *See* DOJ, "Associate Deputy Attorney General Paul R. Perkins Delivers Remarks at the ABA/ABA Financial Crimes Enforcement Conference," (December 9, 2020).
23. *See* DOJ, "Court-Appointed Pennsylvania Guardian and Virginia Co-Conspirators Indicted for Stealing Over $1 Million from Elderly Wards," (June 30, 2021).
24. *See* DOJ, "Franklin, Tennessee Couple Charged With Defrauding Elderly Widow of $1.7 Million," (May 12, 2021); and "Former Waterloo Medicaid Provider Sentenced to More than Five Years in Federal Prison for Defrauding Elderly Victim," (June 28, 2021).
25. *See* DOJ, "Arizona Man Sentenced for Multimillion-Dollar Nationwide Investment Fraud Scheme," (March 15, 2021).
26. *See generally*, DOJ, "Annual Report to Congress on Department of Justice Activities to Combat Elder Fraud and Abuse," (October 18, 2021).

the victim to give them power and control over her personal affairs, and fabricated a power of attorney purporting to give Graves and Williams control over the victim's financial affairs. Once they gained access and control, Graves, Williams, and Harrison moved the victim out of her residence in Indian Land, South Carolina, first to an apartment in Charlotte, and later to a rental home in Mint Hill, refusing to let the victim's friends and family know where she was living. Over the course of the scheme, Graves and her co-conspirators failed to provide the victim with proper medical care, which greatly diminished the victim's health. Furthermore, once the victim's money was depleted, the co-conspirators abandoned the victim, who was later moved to a nursing home in New York, where she passed away in large part due to the mental and physical deterioration she had suffered in the hands of Graves and her co-conspirators.[27]

Elder Scams

In elder scams, criminals defraud victims into sending payments and disclosing PII under false pretenses or for a promised benefit or good the victims will never receive. These scammers are often located outside of the United States and have no known previous relationship to the victims.[28] Elder scams often follow a similar methodology in which scammers contact older adults under a fictitious persona via phone call, robocall, text message, email, mail, in-person communication, online dating apps and websites, or social media platforms. In order to appear legitimate and establish trust with older adults, scammers commonly impersonate government officials, law enforcement agencies, technical and customer support representatives, social media connections, or family, friends, and other trusted persons. Perpetrators often create high-pressure situations by appealing to their victims' emotions and taking advantage of their trust or by instilling fear to solicit payments and PII.[29] Scammers often request victims to make payments through wire transfers at money services businesses (MSBs), but are increasingly requesting payments via prepaid access cards, gift cards, money orders, tracked delivery of cash and high-valued personal items through the U.S. Postal Service, ATM deposits, cash pick-up at the victims' houses, and convertible virtual currency (CVC).[30]

Further, elder scams are sometimes facilitated through money mules[31] who transfer or move illicit funds at the direction of the scammers. A victim of an elder scam can also serve as a money mule: the scammer convinces the victim to set up a bank account or limited liability corporation (LLC)

27. *See* DOJ, "Charlotte Woman And Her Co-Conspirator Are Sentenced To Prison For Stealing $300,000 From An Elderly, Dementia-Afflicted Victim," (May 5, 2021).
28. Nigeria, Jamaica, Ghana, India, the Philippines, and the People's Republic of China are the top foreign-located subject countries in MSB SAR Filings. *See* FinCEN FTA, *supra* Note 15, at p. 9.
29. *See generally*, FTC, Imposter Scams.
30. *See* IC3, "2021 Elder Fraud Report," (March 2022); "Scammers Defraud Victims of Millions of Dollars in New Trend in Romance Scams," (September 16, 2021); "FBI Warns of a Grandparent Fraud Scheme Using Couriers," (July 29, 2021); FTC, "New Twist to Grandparent Scam: Mail Cash," (December 3, 2018); and DOJ, "U.S. Attorney Dena J. King Announces The Successful Forfeiture And Return Of Stolen Cryptocurrency To Elderly Man Victimized By Government Imposter Scam," (March 15, 2022).
31. A money mule is a person (whether witting or unwitting) who transfers or moves illicit funds at the direction of or on behalf of another. *See* IC3, "Money Mules: A Financial Crisis," (December 3, 2021); and Federal Bureau of Investigation (FBI), Money Mules.

in the victim's own name to receive, withdraw, deposit, or transfer multiple third-party payments from other victimized older adults to accounts controlled by the scammer under the illusion of a "business opportunity." In some circumstances, victims of EFE acting as money mules may be prosecuted for this illegal activity and are liable for repaying the victims. They may also be subject to damaged credit and further victimized through their stolen PII.[32]

Common Elder Scam Typologies

- ***Government imposter scams:*** Scammers frequently target older adults by impersonating officials from U.S. government agencies that are often well-known or provide services to older adults, such as the Social Security Administration (SSA),[33] the Department of Health and Human Services/Centers for Medicare and Medicaid Services (HHS/CMS),[34] and the Internal Revenue Service (IRS),[35] among others.[36] The scammers may threaten the individuals with arrest or seizure of their bank accounts for crimes they supposedly committed, such as tax evasion. Scammers may also claim that victims' Social Security numbers are suspended due to suspicious activity and demand PII and payment to resolve the supposed matter with the government.[37]

- ***Romance scams:*** These scams (also referred to as "online dating," "confidence," or "sweetheart" scams) grew to a record level in 2021 with $547 million in reported losses.[38] Romance scams involve fraudsters creating a fictitious profile on an online dating app or website to establish a close or romantic relationship with older adults to exploit their confidence and trust.[39] Online scammers may offer to meet in person (though they almost never do) and ask victims to send money for travel expenses, a sudden "hardship" they experience such as medical costs or legal fees, or a supposed investment or business deal. The scammers often solicit payments over an extended period of time and victims may also send PII as the perpetrators gain the trust of the victims. In some cases, romance scam victims are convinced to open bank accounts and LLCs to receive and send funds as money mules so the scammers can launder their ill-gotten gains from third-party scams.[40]

32. *See* IC3, "Money Mules: A Financial Crisis," (December 3, 2021); "Cyber Actors Use Online Dating Sites To Conduct Confidence/Romance Fraud And Recruit Money Mules," (August 5, 2019); and FBI, Money Mules.
33. *See* FTC, "Growing Wave of Social Security Imposters Overtakes IRS Scam," (April 12, 2019); and Social Security Administration (SSA), Protect Yourself From Social Security Scams.
34. *See* FTC, "Protect Yourself Against Medicare Scams," (March 15, 2019).
35. *See* Internal Revenue Service (IRS), "IRS Reminds Seniors to Remain on Alert to Phone Scams during Tax Season," (March 23, 2017).
36. *See* FTC, "Government Imposter Scams Top the List of Reported Frauds," (July 1, 2019).
37. *See* FTC, "How To Avoid a Government Impersonator Scam," (May 2021); and IC3, "FBI Warns of the Impersonation of Law Enforcement and Government Officials," (March 7, 2022).
38. *See* FTC, "Reports of romance scams hit record highs in 2021," (February 10, 2022).
39. Romance scams can also be perpetrated by scammers who the older adult first meets in-person. These scammers can use romantic overtones to unduly influence an older adult and gain their trust and loyalty before perpetrating the scam.
40. *See* FBI, Romance Scams; and IC3, "Cyber Actors Use Online Dating Sites To Conduct Confidence/Romance Fraud And Recruit Money Mules," (August 5, 2019).

- ***Emergency/person-in-need scams:*** These schemes (also known as "grandparent scams") involve scammers contacting older adults and impersonating a grandchild, another relative, an attorney, emergency medical personnel, or a law enforcement official to deceive victims into believing that a loved one is in an emergency situation (e.g., a car accident, medical emergency, under arrest, or stranded in a foreign country) and needs money sent immediately to resolve the situation.[41]

- ***Lottery and sweepstakes scams:*** These scams are a type of advance-fee scheme in which scammers, typically located in jurisdictions outside of the United States, impersonate lottery or sweepstakes representatives, and lawyers claiming that the victims have won a lottery, prize, or sweepstakes. Scammers may target older adults regardless of whether the victims have previously played the lottery or entered in a sweepstakes. The scammers instruct the victims to pay for supposed shipping, taxes, or other fees in order to claim their prize or lottery winnings. Victims never receive their prize or lottery winnings and are often re-victimized with additional requests for payments throughout the scheme until they run out of money.[42]

- ***Tech and customer support scams:*** These scammers impersonate well-known companies as tech and customer support representatives to falsely claim that a virus or other malware has compromised the victims' computers. Scammers may request remote access to diagnose the alleged problem and will typically attempt to solicit payment for fraudulent software products and tech support services. They also often exploit the remote access to install malware and steal PII and credit card numbers to further defraud the victims.[43] After victims make payments, perpetrators often call back and offer refunds to the victims, claiming their tech and customer support services are no longer available. Perpetrators then will claim to send refund money to the victims' bank accounts but falsely claim that too much money was refunded. The scammers then induce victims to send payments purportedly to reimburse the tech and customer support company for its "over-refund." Victims can lose hundreds or thousands of dollars to such refund schemes. A recent evolution of the refund scheme involves perpetrators claiming to be online retailers and purporting to offer a refund for unauthorized transactions on the victims' accounts.[44]

41. *See* FTC, "Scammers Use Fake Emergencies to Steal Your Money," (May 2021).
42. *See* FTC, "Fake Prize, Sweepstakes, and Lottery Scams," (May 2021); and DOJ, Senior Scam Alert.
43. *See* CFPB, "What you should know about tech support scams," (January 12, 2021); FTC, "How to Spot, Avoid, and Report Tech Support Scams," (February 2019); "Older Adults Hardest Hit By Tech Support Scams," (March 7, 2019); and IC3, "Technical and Customer Support Fraud," (March 16, 2022).
44. *See* DOJ, Transnational Elder Fraud Strike Force; and FTC, "Amazon tops list of impersonated businesses," (October 20, 2021).

Case Study of Elder Scams

India-based Government Imposter Scam

An Indian national was sentenced to 22 years in prison for conspiracy and identity theft in connection with his operation of an overseas robocall scam that defrauded thousands of victims out of more than $10 million. The victims, many of whom are elderly, continue to endure significant financial hardship from the defendant's vast fraud enterprise. According to court documents, Shehzadkhan Pathan, 40, operated a call center in Ahmedabad, India, from which automated robocalls were made to victims in the United States. After establishing contact with victims through these automated calls, Pathan and other "closers" at his call center would coerce, cajole, and trick victims into sending bulk cash through physical shipments and electronic money transfers. Pathan and his conspirators used a variety of schemes to convince victims to send money, including impersonating law enforcement officers from the Federal Bureau of Investigation and Drug Enforcement Administration and representatives of other government agencies, such as the Social Security Administration, to threaten victims with severe legal and financial consequences. Conspirators also convinced victims to send money as initial installments for falsely promised loans. Pathan is the fourth of six defendants in this case to be sentenced for their role in the conspiracy.[45]

Behavioral and Financial Red Flags of EFE and Associated Payments

FinCEN has identified behavioral and financial red flags to help financial institutions detect, prevent, and report suspicious activity connected to EFE. These red flags build off of the red flags in FinCEN's 2011 Advisory, all of which remain relevant, and do not reflect all behavioral and financial red flags of EFE.[46] As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags, before determining if a behavior or transaction is suspicious or otherwise indicative of EFE. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional due diligence where appropriate. Financial institutions should remain alert to any suspicious activity indicating that their customers are perpetrators, facilitators, or victims of EFE.

45. *See* DOJ, "Leader of International Robocall Scam Sentenced for Defrauding Over 4,000 U.S. Victims Out of More Than $10 Million," (September 16, 2021).
46. *See* 2011 Advisory, *supra* Note 3. For more information on red flags of EFE, *see* DOJ, Red Flags of Elder Abuse; and CFPB, "Recommendations and Report for Financial Institutions on Preventing and Responding to Elder Financial Exploitation," (March, 23, 2016).

Behavioral Red Flags

Victims of EFE may have limited and irregular contact with others. For some, their only outside contact may involve visiting or communicating with their local financial institution, including at the bank branch, check-cashing counter, or MSB. Therefore, it is critical for customer-facing staff to identify and consider the behavioral red flags when conducting transactions involving their older customers, particularly suspicious behavior that also involves the financial red flags highlighted below. Such information should be incorporated into SAR filings and reported to law enforcement as appropriate. Financial institutions are reminded that behavioral red flags of EFE and the names of staff who witnessed them should be included in the SAR narrative to assist future law enforcement investigations. Behavioral red flags of EFE may include:

1. An older customer's account shows sudden and unusual changes in contact information or new connections to emails, phone numbers, or accounts that may originate overseas.
2. An older customer with known physical, emotional, and cognitive impairment has unexplainable or unusual account activity.
3. 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.
4. An older customer mentions how an online friend or romantic partner is asking them to receive and forward money to one or more individuals on their behalf or open a bank account for a "business opportunity."
5. 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.
6. 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.
7. 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.
8. 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.
9. The financial institution is unable to speak directly with the older customer, despite repeated attempts to contact him or her.
10. A new caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of an older customer without proper documentation.

11. An older customer's financial management changes suddenly, such as through a change of power of attorney, trust, or estate planning vehicles, to a different family member or a new individual, particularly if such changes appear to be done under undue influence, coercion, or forgery or the customer has diminished cognitive abilities and is unable to agree to or understand the consequences of the new arrangement.
12. An older customer lacks knowledge about his or her financial status, or shows a sudden reluctance to discuss financial matters.

Financial Red Flags

Identification of financial red flags of EFE and the associated payments are critical to detecting, preventing, and reporting suspicious activity potentially indicative of EFE. In addition to the financial red flags set out in DOJ and CFPB notices,[47] financial red flags of EFE may include:

13. Dormant accounts with large balances begin to show constant withdrawals.
14. An older customer purchases large numbers of gift cards or prepaid access cards.
15. An older customer suddenly begins discussing and buying CVC.
16. An older customer sends multiple checks or wire transfers with descriptors in the memo line such as "tech support services," "winnings," or "taxes."
17. Uncharacteristic, sudden, abnormally frequent, or significant withdrawals of cash or transfers of assets from an older customer's account.
18. An older customer receives and transfers money interstate or abroad to recipients with whom they have no in-person relationship, and the explanation seems suspicious or indicative of a scam or money mule scheme.
19. Frequent large withdrawals, including daily maximum currency withdrawals from an ATM.
20. Sudden or frequent non-sufficient fund activity.
21. Uncharacteristic nonpayment for services, which may indicate a loss of funds or of access to funds.
22. Debit transactions that are inconsistent for the older customer.
23. Uncharacteristic attempts to wire large sums of money.
24. Closing of CDs or accounts without regard to penalties.

47. *Id.*

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

Suspicious Activity Reporting
Other Relevant BSA Reporting
USA PATRIOT ACT Section 314(b) Information Sharing Authority
Additional Reporting Options

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, including EFE.[48] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[49]

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[50] Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[51] When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML/CFT program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

48. *See* 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320. All financial institutions with these SAR filing requirements also may file a SAR regardless of the amount involved (if any) or if the transaction is only attempted.
49. *See* 31 U.S.C. § 5318(g)(3).
50. *See* 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), and 1030.320(d). 31 CFR §§ 1010.330, 1010.331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.
51. *Id. See also*, FinCEN, "Suspicious Activity Report Supporting Documentation," (June 13, 2007).

SAR Filing Instructions

When filing a SAR, financial institutions should provide all pertinent available information about the activity in the SAR form and narrative. Reporting on how perpetrators of EFE communicate with and target older adults is also useful to law enforcement investigations. **FinCEN requests that financial institutions reference this advisory by including the key term below in SAR field 2 ("Filing Institution Note to FinCEN")** and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.

"EFE FIN-2022-A002"

Financial institutions that suspect EFE activity should also mark the check box for Elder Financial Exploitation (**SAR Field 38(d)**). FinCEN first added an "Elder Financial Exploitation" checkbox to the SAR Form in 2012 and encourages financial institutions to mark the box when filing an EFE-related SAR. For authorized federal, state, and local law enforcement, the checkbox makes it easier to locate and analyze BSA data related to EFE as detailed above.

Financial institutions should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.[52]

Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this advisory may call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).[53]

Filers are reminded, as stated in FinCEN's Electronic Filing Instructions, that the narrative section of the report is critical to understanding the nature and circumstances of the suspicious activity. The care with which the narrative is completed may determine whether the described activity and its possible criminal nature are clearly understood by investigators. Filers must provide a clear, complete, and concise description of the activity, including what was unusual or irregular that caused suspicion.[54] Filers are also encouraged to determine their obligations to report suspected EFE under state law and report suspected EFE to law enforcement and their state-based Adult Protective Services.

52. *See* 31 CFR §§ 1020.320(e)(1)(ii)(A)(2)(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), and 1030.320(d)(1)(ii)(A)(2).
53. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local area law enforcement officials.
54. *See* FinCEN, "SAR Electronic Filing Instructions," (October 2012).

FinCEN notes that the tips below are best practices in regard to filing a SAR for suspected EFE and are not regulatory obligations:

- 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.
- Provide details about the amounts involved and whether any amounts were refunded to the older customer (as of the submission date of the SAR).
- Reference supporting documentation, including any photos or video footage, in the narrative.
- Cross-report the circumstances leading to the filing of EFE SARs directly to local law enforcement if there is any indication that a) a crime may have been committed and/or b) the older adult may still be at risk for victimization by the suspected abuser. Filers should note that the filing of a SAR is not a substitute for any requirement in a given state to report suspected EFE to law enforcement and Adult Protective Services.
- Take advantage of the law enforcement contact field to indicate if the suspicious activity was also reported to law enforcement or Adult Protective Services, as well as the name and phone number of the contact person.
- Provide direct liaisons or points of contact at the reporting entity related to the SAR so investigators can ask questions and request additional documentation in a timely manner.
- Expedite responses to law enforcement requests for supporting documents.[55]

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons also may have other relevant BSA reporting requirements that provide information in connection with the subject of this advisory.[56] These include obligations related to the Currency Transaction Report (CTR),[57] Report of Cash

55. Elder financial exploitation investigations are often complex, time-consuming, and time-sensitive because older victims may be at risk of losing cognitive capacity or passing away before law enforcement has fully investigated the case. Therefore, expedited responses are critical to aiding any investigation.
56. BSA reporting refers to legal requirements that financial institutions and certain businesses and persons report certain financial transactions (such as large-dollar cash transactions), suspicious activity, or other information (such as information on a taxpayer's foreign bank and financial accounts) to FinCEN "that are highly useful in (A) criminal, tax, or regulatory investigations, risk assessments, or proceedings; or (B) intelligence or counterintelligence activities, including analysis, to protect against terrorism;" 31 U.S.C. § 5311(1).
57. A report of each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to the reporting financial institution which involves a transaction in currency of more than $10,000, in aggregate per business day. 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.

Payments Over $10,000 Received in a Trade or Business (Form 8300),[58] Report of Foreign Bank and Financial Accounts (FBAR),[59] Report of International Transportation of Currency or Monetary Instruments (CMIR),[60] Registration of Money Services Business (RMSB),[61] and Designation of Exempt Person (DOEP).[62] These standard reporting requirements may not have an obvious connection to illicit finance, but may ultimately prove highly useful to law enforcement.

Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this advisory, FinCEN requests that the filer select ***Box 1b*** ("suspicious transaction") and include the key term "**EFE FIN-2022-A002**" in the "**Comments**" section of the report.

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing EFE, among other illicit activity. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding activities they suspect may involve possible terrorist financing or money laundering.[63] FinCEN strongly encourages such voluntary information sharing.

Rapid Response Program

Through the Rapid Response Program (RRP), FinCEN helps victims and their financial institutions recover funds stolen as the result of certain cyber-enabled financial crime schemes, including cyber-enabled fraud against older adults. The RRP is a partnership between FinCEN; U.S. law enforcement (including the FBI, the U.S. Secret Service, Homeland Security Investigations, and the U.S. Postal Inspection Service); and foreign partner agencies that, like FinCEN, are the financial intelligence units (FIUs) of their respective jurisdictions. FinCEN

58. A report filed by any U.S. person engaged in a trade or business on the receipt of more than $10,000 in currency in one transaction or two or more related transactions involving the trade or business. Such transactions are required to be reported on joint FinCEN/IRS Form 8300 when not otherwise required to be reported under the CTR requirements. 31 CFR §§ 1010.330, 1010.331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.
59. A U.S. person that has a financial interest in or signature authority over foreign financial accounts must file an FBAR if the aggregate value of the foreign financial accounts exceeds $10,000 at any time during the calendar year, as specified in 31 CFR § 1010.350 and FinCEN Form 114.
60. Each person (i.e., an individual or legal entity), as defined in 31 CFR § 1010.100(mm), that transports, ships, or mails more than $10,000 of currency or other monetary instruments into or out of the United States must file a CMIR. 31 CFR § 1010.340.
61. Report for a business required to register with FinCEN as a money services business, as defined in 31 CFR § 1010.100(ff), or renewing the registration. 31 CFR § 1022.380.
62. Report for banks, as defined in 31 CFR § 1010.100(d), to exempt certain customers from currency transaction reporting in accordance with 31 CFR § 1010.311.
63. For further guidance related to the 314(b) Program, *see* FinCEN, "Section 314(b) Fact Sheet," (December 20, 2020).

uses its authority to share financial intelligence rapidly with counterpart FIUs and encourages foreign authorities to interdict the fraudulent transactions, freeze funds, and stop and recall payments using their authorities under their own respective legal and regulatory frameworks. A victim of a cyber-enabled crime, or the victim's financial institution, must file a complaint with federal law enforcement to initiate the RRP.

The RRP has been used to confront cyber threats involving over 80 foreign jurisdictions, and has the capacity to reach more than 160 foreign jurisdictions through FIU-to-FIU channels. Through these collaborative efforts, FinCEN has successfully assisted in the recovery of over $1.1 billion. For more information, please see FinCEN's Fact Sheet on the Rapid Response Program (RRP).

Other U.S. Government EFE Reporting Options

In addition to filing a SAR, financial institutions should refer their older customers who may be a victim of EFE to the DOJ's National Elder Fraud Hotline at 833-FRAUD-11 or 833-372-8311 for support, resources, and assistance with reporting suspected fraud to the appropriate government agencies. Filers should immediately report any imminent threat or physical danger to their local FBI office or local law enforcement. FinCEN encourages filers to collaborate with other stakeholders in their communities to enhance responses and engage in professional training opportunities, community education prevention, and awareness activities and initiatives.[64] Filers can find whether there is an existing collaboration on elder fraud prevention and response in their area by contacting Adult Protective Services or their local Area Agency on Aging.[65]

For Further Information

Questions regarding the contents of this advisory should be addressed to the FinCEN Resource Center at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

64. *See* CFPB, Elder Networks. This webpage provides additional information about collaboration in communities to prevent and respond to elder financial exploitation.
65. *See* U.S. Administration on Aging, Eldercare Locator. The website also provides a list of public services available to older adults.