FINANCIAL CRIMES ENFORCEMENT NETWORK

Financial Trend Analysis

Elder Financial Exploitation: Threat Pattern & Trend Information, June 2022 to June 2023

April 2024

Elder Financial Exploitation: Threat Pattern & Trend Information, June 2022 to June 2023

This Financial Trend Analysis focuses on patterns and trends identified in Bank Secrecy Act (BSA) data linked to Elder Financial Exploitation (EFE). The Financial Crimes Enforcement Network (FinCEN) is issuing this report pursuant to Section 6206 of the Anti-Money Laundering Act of 2020 (AMLA), which requires periodic publication of BSA-derived threat pattern and trend information.[1] FinCEN issued government-wide priorities for anti-money laundering and countering the financing of terrorism policy on 30 June 2021, which included fraud as a government-wide priority.[2] FinCEN has long understood the threat that EFE poses and issued an Advisory on Elder Financial Exploitation, FIN-2022-A002, on 15 June 2022 (June 2022 EFE Advisory). The information in this report is relevant to the public, especially the older adult population and a wide range of businesses and industries. This report also highlights the value of BSA information filed by regulated financial institutions, including responses to the June 2022 EFE Advisory.

Executive Summary: This Financial Trend Analysis provides threat pattern and trend information on Elder Financial Exploitation (EFE) incidents, based on Bank Secrecy Act (BSA) data filed with the Financial Crimes Enforcement Network (FinCEN) between 15 June 2022 and 15 June 2023 (the "review period"). During the review period, FinCEN received 155,415 EFE-related BSA reports associated with more than $27 billion in reported suspicious activity, which may include both actual and attempted transactions. EFE-related losses may affect personal savings, checking accounts, retirement savings, and investments, and can severely impact victims' well-being and financial security.

Scope and Methodology: FinCEN examined BSA reports filed during the review period that used the June 2022 EFE Advisory key term ("EFE FIN-2022-A002) and/or checked "Elder Financial Exploitation" as a suspicious activity type, as requested in the June 2022 EFE Advisory. Based on these parameters, FinCEN identified a data set consisting of 155,415 filings. References herein to EFE-Related BSA reports filed during the review period refer to this dataset, which is the basis for the analysis in this report. The BSA reports in this data set reported roughly $27 billion in EFE incidents, which may include both completed and attempted transactions.[3] [4] FinCEN identified these BSA reports based on filing date, rather

1. The AMLA was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021).
2. *See* "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities," Financial Crimes Enforcement Network, 30 June 2021, AML/CFT National Priorities.
3. The amount of suspicious activity reported may be overstated in some cases because this figure may include attempted transactions and payments that were unpaid, duplicates, counting of both inbound and outbound transactions, transfers between accounts, typos, and errors as submitted by filers. The $27 billion figure may also include continuing suspicious activity or amend earlier reporting, or reports that cover expanded networks involved in potential illicit activity.
4. Filings pertaining to June 2023 incidents that were submitted after the review period were omitted.

than the date of the underlying activity, and, as such, these reports may refer to incidents that occurred in previous months and years. FinCEN used a combination of automated and manual review of BSA reports to identify EFE-related suspicious activity and determine prominent trends and methodologies.

Overview of Key Findings: Consistent with the June 2022 EFE Advisory, FinCEN identified two predominant categories of victimization across EFE-related BSA filings: (1) elder scams, where the victim does not know the perpetrator; and (2) elder theft, where the victim knows the perpetrator.

- *Banks Filed 72 Percent of All EFE-Related BSA filings*: Two banks reported 33 percent, or 50,670 BSA filings, of the filings in the dataset. These bank filings mostly reported their customers as victims or perpetrators, but also included reports where the filer acted as a correspondent bank.[5]
- *Financial Institutions Filed More Elder Scam-Related BSA Filings than Elder Theft-Related BSA Filings*: BSA filings relating to elder scams accounted for approximately 80 percent of reported EFE-related activity. This does not necessarily indicate that scams occur more often than theft, but filers are reporting on it more frequently.
- *Account Takeover is the Most Frequently Cited EFE Typology*: The majority of elder scam-related filings also referenced account takeover activity.
- *Adult Children are the Most Frequent Elder Theft-Related Perpetrators*: BSA filers reported adult children as the perpetrators of elder theft in nearly 40 percent of cases, based on a manual review of EFE-related filings.
- *Reliance on Unsophisticated Methodologies and Avoiding Human Contact*: Perpetrators mostly rely on unsophisticated means to steal funds that minimize direct contact with financial institution employees. These include using previously compromised identifying information and/or passwords, guessing passwords, or mass spam emails that elicit replies containing sensitive information.

What is Elder Financial Exploitation

EFE is the illegal or improper use of an older adult's funds, property, or assets, according to FinCEN's June 2022 EFE Advisory and the U.S. Department of Justice Elder Justice Initiative.[6] Older adults are typically considered individuals aged 60 or older.[7] EFE consists of two primary subcategories: elder theft and elder scams.

5. Correspondent banking refers to formal agreements or relationships between banks to provide payment services for each other. It is often used to facilitate cross-border payments. See Code of Federal Regulations Title 31 CFR 1010.605, https://www.ecfr.gov/current/title-31/section-1010.605.
6. *See* "Advisory on Elder Financial Exploitation," FinCEN Advisory #FIN-2022-A002," 15 June 2022, https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2022-a002
7. *See* "Protecting Older Consumers 2021-2021," Federal Trade Commission, 18 October 2021, Protecting Older Consumers 2020-2021 (ftc.gov). Financial institutions may have included some victims under 60 years of age in EFE BSA reporting.

- Elder theft involves the theft of an older adult's assets, funds, or income by a trusted person.
- Elder scams involve the transfer of money to a stranger or imposter for a promised benefit or good that the older adult did not receive.

For purposes of this FTA, elder theft is defined as when persons known and trusted by older adults steal victim funds, while elder scams involve fraudsters with no known relationship to their victims, who are sometimes located outside the United States.[8] Elder theft is likely to be underreported and can go undetected because the perpetrators are typically individuals who are trusted by the victim.[9] FinCEN analysis of BSA information indicates that scammers mostly rely on less sophisticated scam typologies, though some are making their scams more elaborate by blending multiple scam types into one victimization, and using victims both as a source of funds and to launder illicit gains.[10] Scammers are often organized, with fraud rings ranging from small groups of individuals to organizations with hundreds of members.[11] At least two large-scale, violent criminal organizations are known to carry out fraud schemes, including EFE-related fraud, to make money.[12]

The FBI's Internet Crime Complaint Center reported that it received 88,262 complaints totaling over $3 billion from victims aged 60 or over in 2022.[13] Given that these are self-reported complaints, it is likely the $3 billion loss represents a smaller proportion of the actual amount lost to EFE each year. In June 2023, AARP issued a report estimating EFE losses at approximately $28.3 billion annually.[14]

8. *See* "Advisory on Elder Financial Exploitation," FinCEN Advisory #FIN-2022-A002," 15 June 2022, https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2022-a002.
9. *See* "Recovering from Elder Financial Exploitation, A Framework for Policy and Research," Consumer Financial Protection Bureau, September 2022, Recovering from Elder Financial Exploitation: A framework for policy and research (consumerfinance.gov)
10. *See* "Phantom Hacker Scams Target Senior Citizens and Result in Victims Losing their Life Savings," Federal Bureau of Investigations Internet Crime Complaint Center, Alert Number I-091223-PSA, 29 September 2023, "Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings (ic3.gov).
11. *See* United States Attorney's Office, Eastern District of Michigan Press Release, "Case Concludes Involving Organized Fraud Ring in Detroit," 30 March 2022, https://www.justice.gov/usao-edmi/pr/case-concludes-involving-organized-fraud-ring-detroit; Yudhijit Bhattacharjee, "Who's Making All Those Scam Calls?," The New York Times Magazine, 15 June 2023, https://www.nytimes.com/2021/01/27/magazine/scam-call-centers.html; "Hundreds Arrested and Millions Seized in Global INTERPOL Operation Against Social Engineering Scams," INTERPOL Press Release, 15 June 2022, https://www.interpol.int/en/News-and-Events/News/2022/Hundreds-arrested-and-millions-seized-in-global-INTERPOL-operation-against-social-engineering-scams.
12. *See* BBC News, "Black Axe: Leaked Documents Shine Spotlight on Secretive Nigerian Gang," 13 December 2021, https://www.bbc.com/news/world-africa-59630424; "Treasury Sanctions Fugitive, Others Linked to CJNG Timeshare Fraud Network," U.S. Department of the Treasury Press Release, 27 April 2023, https://home.treasury.gov/news/press-releases/jy1443.
13. *See* "Elder Fraud Report 2022," Federal Bureau of Investigation's Internet Crime Complaint Center, May 2022, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf.
14. *See* Jilenne Gunther, "The Scope of Elder Financial Exploitation: What it Costs Victims," AARP Public Policy Institute's BankSafe Initiative, June 2023, https://www.aarp.org/pri/topics/work-finances-retirement/fraud-consumer-protection/scope-elder-financial-exploitation.html.

Banks Filed Vast Majority of EFE-Related BSA Filings; Virtual Asset Service Providers (VASPs) Identified Most EFE-Related Activity in MSB Sector

Filers began using the key term listed in the June 2022 EFE Advisory on 15 June 2022, the date the advisory was published. A total of 4,472 financial institutions filed EFE-related BSA reports during the review period, including depository institutions, securities/futures institutions, credit unions, money services businesses (MSBs), insurance companies, credit card companies, lenders, and casinos.

- Depository institutions filed 46,888 EFE-related BSA reports from March 2023 to May 2023, accounting for nearly 30 percent of the total EFE-related reports filed in the review period. This pace appears to be continuing, as FinCEN received an average of 15,993 EFE BSA reports per month between 15 June 2023, and 15 January 2024.

Banks filed 72 percent of the total EFE-related BSA reports received in the review period. The filings from these banks consisted of transactions by their direct customers and instances when the banks identified potential EFE-related activity when acting as a correspondent bank. In total, 10 depository institutions filed over 1,000 EFE-related BSA reports each during the review period.

MSBs filed 15 percent of the total EFE-related BSA reports filed during the review period. VASPs accounted for nearly 42 percent of those MSB reports, while non-VASP MSBs filed about 58 percent of the MSB subset.[15]

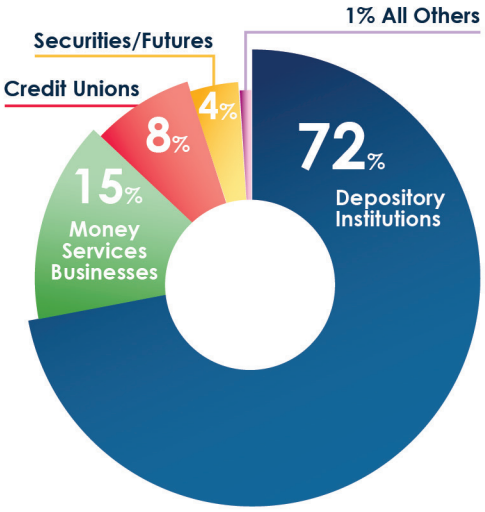
- VASPs include exchanges and convertible virtual currency (CVC) kiosks, with exchanges accounting for most of the BSA reports.[16] Exchanges or other service providers filed 5,705 BSA reports, nearly 57 percent of VASP-related reports, while CVC kiosk operators filed 4,307 BSA reports, which is the remaining 43 percent.

- CVC kiosks can have high transaction fees for senders and recipients, typically ranging from 7-20 percent, but it appears scammers are willing to accept these costs for the potential benefits that the kiosks provide such as rapid settlement of cash or fiat for crypto trades, according to BSA and open-source information.[17]

15. A VASP is a business that conducts one or more the following activities or operations for or on behalf of another natural or legal person: exchange between virtual assets and fiat currencies; exchange between one or more forms of virtual assets; transfer of virtual assets; safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset. See Financial Action Task Force, "Virtual Assets and Virtual Asset Service Providers," October 2021, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.
16. CVC kiosks (commonly called Bitcoin automated teller machines (ATMs)) are ATM-like devices or electronic terminals that allow users to exchange cash and virtual currency. See Advisory on Illicit Activity Involving Convertible Virtual Currency," FinCEN Advisory #FIN-2019-A003," 9 May 2019, https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.
17. *See* "Advisory on Illicit Activity Involving Convertible Virtual Currency," FinCEN Advisory #FIN-2019-A003," 9 May 2019, https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf; Coinme, "Bitcoin ATM Fees Explained-Bitcoin 101," https://coinme.com/blog/bitcoin/bitcoin-atm-fees-101/; Susan Tompor, "Easy-to-Find Bitcoin ATMs, QR Codes Used as Weapons by Scammers: What to Know," Detroit Free Press, 23 September 2022, https://www.freep.com/story/money/personal-finance/susan-tompor/2022/09/23/bitcoin-atm-cryptocurrency-qr-code-scam/7842125001/.

Credit unions and securities/futures institutions accounted for the largest remaining portion of the EFE-related BSA reports filed during the review period, accounting for eight and four percent of the total filings, respectively.

Filers by Financial Institution Type
(Percentage of Total EFE-Related SARs)



Increasing Trend Towards Avoiding Bank and MSB Personnel

Perpetrators of both EFE scams and theft utilize methods of siphoning funds that avoid direct contact with depository institution or MSB personnel. Such personnel would likely identify EFE activity more frequently if victims or perpetrators conducted transactions in person, and presumably not permit the requested transactions. Filers that detailed instances of elder theft where victims were brought to the financial institution often noted the likelihood of exploitation by citing interactions between the victims and perpetrators, including any nervousness or hesitancy in conducting the transactions and abnormal dialogue between perpetrators and victims. These filers sometimes noted the physical appearance of the victim, an especially important sign of possible abuse. Filers also noted that elder scam victims who conducted in person transactions often appeared nervous, struggled to maintain a consistent reason for sending their attempted transaction, and may have been on the phone with someone directing their activities throughout the interaction. Potential perpetrators likely rely on financial transactions that do not require in-person interaction with financial institution staff to minimize the likelihood of getting caught, having their transactions being stopped, or having an employee report their activity.

- Digital payment methods, peer-to-peer transfer systems, and ATMs account for a significant portion of the funds transfers in EFE-related BSA reports filed during the review period. These payment methods provide for instantaneous transfers that allow the recipient to access the funds immediately after executing the transfer. Transfers and withdrawals at ATMs also limit the amount of in-person interaction that occurs when executing fraudulent transactions.

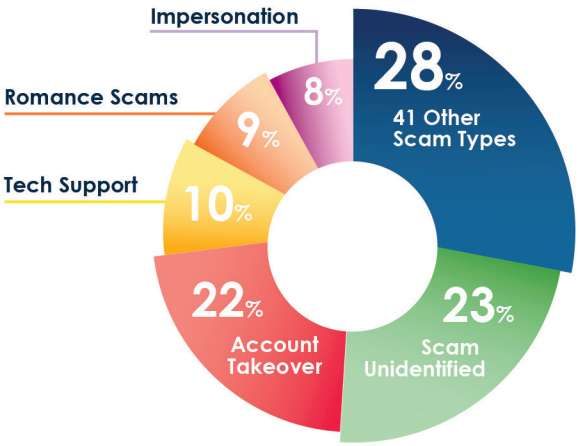
Elder Scams Account for Majority of EFE-Related BSA Reporting

The vast majority of EFE-related BSA reports filed during the review period pertained to elder scams. For elder scams, filers reported an average suspicious activity amount of $129,483, while the median amount reported for elder scams was $33,499. Compared to elder theft, financial institutions appeared to file significantly more BSA reports on elder scams, and the suspicious activity amounts tended to be higher.

Financial institutions most frequently reported account takeover in elder scam-related BSA filings.[18] In most cases, filers reported unauthorized transactions out of customer accounts and the financial institution would either close the account, provide the victim with new online banking login credentials, or give them a new debit/credit card.

- Depository institutions filed the most BSA reports detailing compromised accounts, but there were instances of other types of accounts being compromised as well, including CVC exchange accounts, credit cards, investment accounts, and mortgage accounts, among others.
- The unauthorized outgoing transactions were typically peer-to-peer transfers, bank transfers, or fraudulent checks.

Scam Types Identified in EFE Reporting, by Percentage[19]



When filers indicated a definitive scam typology, they identified tech support scams and romance scams most frequently. Tech support scams were cited most among the elder scam-related BSA reports reviewed during the review period. These scams tend to follow a pattern — victims receive a pop-up or alert on their device saying that it has a virus and they are given a phone number to contact to fix it. The victims then speak with a call center representative impersonating a known computer company, who then conducts fake "repairs" and charges the victim. Often, victims will

18. Account takeover in elder scams refers to instances where an account was taken over by a perpetrator unknown to the victim. Account takeover can occur in elder theft as well, but in those cases the victim knows or trusts the perpetrator.
19. Percentages in this table are based on manual review of EFE-related BSA reports filed during the review period.

grant the scammer remote access to their computer, which can lead to installation of malware or compromised personal identifiable information. Tech support scams can be paired with refund scams whereby victims receive an e-mail saying that they purchased antivirus software when they really did not.

Romance scams were also cited frequently among EFE-related BSA reports filed during the review period. In cases of romance scams, the most reported way scammers contacted victims was through online dating platforms. Multiple factors can play a role in romance scam victimization, including declining cognitive abilities, loneliness, grief from the recent passing of a loved one, or belief that they are marrying into wealth, according to BSA and open-source information.[20] Romance scams can follow several different patterns and can also turn into investment scams once a connection is established.[21] Other, less frequently reported scams include investment scams, retail scams, government impersonation scams, lottery scams, real estate scams, and family-in-need scams. For a list of the most frequently identified scams and their definitions, please see Appendix A.

Scams Used to Both Extract and Move Funds

Perpetrators can use scams to both extract funds from victims and move fraudulently obtained funds. Scammers may recruit other victims to move funds extracted from initial victims. These other victims are commonly referred to as money mules.[22] Money mules may be unwitting — meaning they were not aware they were moving illicit funds — or knowing participants in the scam activity. Unwitting money mules are often also scam victims. Employment scams, romance scams, lottery scams, and grant scams are common methods scammers use to recruit money mules. FinCEN identified EFE-related BSA reports filed during the review period that specifically documented schemes involving money mules.

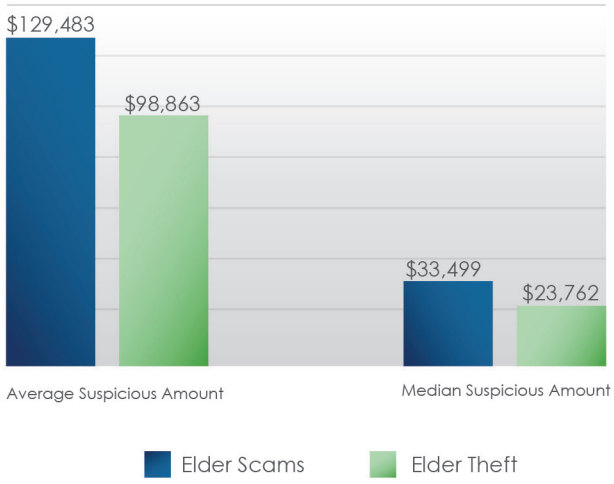
Checks and Wires are Most Frequent Methods for Transmitting Scam Funds; Majority of Payments Sent Domestically

FinCEN's analysis of the EFE-related BSA reports filed during the review period indicated that victims most frequently sent scam-related funds via check and wire transfer, though many of the check payments consisted of fraudulent or counterfeit checks. Based on review of BSA filings, fraudulent checks were typically the result of compromised accounts, as scammers either altered an intercepted check or created new checks using stolen information. While virtual currency

20. *See* Emily Schmall, "Retirees are Losing Their Life Savings to Romance Scams. Here's What to Know," The New York Times, 3 February 2023, https://www.nytimes.com/2023/02/03/business/retiree-romance-scams.html; Tom Buchanan and Monica T. Whitty, "The Online Dating Romance Scam: Causes and Consequences of Victimhood," *The University of Warwick*, 2013, https://wrap.warwick.ac.uk/83736/7/WRAP_Online%20Dating%20Romance%20Scam%20-%20causes%20and%20consequences%20of%20victimhood.pdf; Monica T. Whitty, "Do You Love Me? Psychological Characteristics of Romance Scam Victims," *Cyberpsychology, Behavior, and Social Networking*, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5806049/.
21. *See* "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as Pig Butchering," FinCEN Alert #FIN-2023-Alert005," 8 September 2023, FinCEN Alert, FIN-2023-Alert005, September 8, 2023
22. Please see Appendix A for a definition of money mules as used in this report.

is an increasingly popular transfer method, it appears that scammers still rely heavily on more traditional methods that victims are familiar with. When scam funds were sent through the mail, they were mostly sent to domestic mailing addresses.

Average and Median Reported Suspicious Amounts: Scams and Theft



EFE-Related BSA Reports Identify Fewer Instances, Lower Amounts for Elder Theft

Elder theft-related BSA reports accounted for approximately 20 percent of the EFE-related BSA reporting reviewed by FinCEN over the review period, with instances of theft averaging a reported suspicious activity amount of $98,863 (median of $23,762).[23] Both figures are significantly less than those for elder scams. This could indicate that victims tend to lose more money to scams, elder theft occurs less frequently than scams, or that financial institutions are detecting instances of elder theft less often and thus are reporting it less frequently. Additionally, it is possible that suspicious activity reporting amounts may be below BSA filing thresholds.[24] FinCEN observed that filing amounts for elder theft are lower than those reported for elder scams.

Adult Children Most Often Identified as Elder Theft Perpetrators

Adult children of older parents are the most frequently identified perpetrators of elder theft in BSA reports filed during the review period. When filers included addresses or locations of the parties in the BSA reports, the adult children tended to live near the parent they were victimizing. Even in instances where the perpetrator used a digital payment system to steal from the victim, they tended to be in close proximity. The BSA reports indicated that those closest to the victim — whether in terms of relationship or in physical proximity — were the most frequently identified perpetrators.

23. There are two outlier elder theft SARs that significantly skew the average, one for over $3 million and another for over $2 million. Without those two, the average suspicious activity amount is $70,695.
24. According to the Bank Secrecy Act, financial institutions must report any suspicious transactions if the transaction (attempted or completed) involves or aggregates at least $5,000 ($2,000 for MSBs).

Following adult children of victims, professional caregivers such as nurses, aides, rehabilitation facility workers, and in-home care providers were the next most frequently identified perpetrators of elder theft. FinCEN analysis of BSA reports filed during the review period revealed that caretakers had access to older adults' banking information, checkbooks, or other personally identifiable information in multiple instances. In a small number of instances, perpetrators included neighbors and financial advisors, though they each accounted for a comparatively negligible number of filings.

Methods of Elder Theft Vary, but Rely on Time-Tested Methodologies

The methods that perpetrators of elder theft use to steal from victims vary, but they generally appear to be relatively unsophisticated and straightforward. In most of the EFE-related BSA reports reviewed, perpetrators conducted transactions strictly for their own benefit. This often took the form of sending or withdrawing money for themselves, but also using stolen funds to make purchases or pay their own bills. These perpetrators made little or no effort to obfuscate the payments.

Unlike elder scams, perpetrators of elder theft may be less likely to be sophisticated criminals or familiar with money laundering techniques. Additionally, it often is not necessary for family members or trusted individuals to orchestrate elaborate scams to obtain access to the victim's accounts. Often the perpetrator already has access, can quickly gain access, or the victim will give them funds if the victim is adequately trusting, or conversely if the perpetrator is intimidating. In EFE-related BSA reports, filers often reported the following methods used to transfer funds:

- Funds transfers: Perpetrators either have access to victims' online banking or trick the victim into performing the transfers on their behalf. Funds are often sent directly to perpetrators, but filers also reported that perpetrators used stolen funds to pay merchants or other individuals.
- Fraudulent checks: Perpetrators with access to a victim's checkbook will write themselves checks and either have victims sign the check or forge the signature.
- Credit/debit card: Perpetrators have access to a victim's credit/debit card or credit/debit card information and make purchases for themselves.
- Cash withdrawals: Perpetrators use ATMs if they have access to a victim's debit card or they may escort the victim to the bank and conduct a teller withdrawal.
- Online bill pay: Perpetrators with access to a victim's account will pay their own bills directly.
- Wire: The least common method of transfer, but frequently associated with large, international transactions.

The information in this report is based on EFE-related information obtained from analysis of BSA data and open-source publications, as well as insights from law enforcement and other partners. FinCEN welcomes feedback on this report, particularly from financial institutions. Please submit feedback to the FinCEN Regulatory Support Section at frc@fincen.gov.

Appendix A: List of Most Prominent Scams Identified in EFE-Related BSA Reporting and Related Definitions

Account Takeover: Deliberate compromise of a victim's account to remove, steal, procure, or otherwise affect the victim's funds.[25]

Advance Fee Scam: When scammers ask victims to pay an up-front fee to close a deal or claim a prize.[26] Advanced fees are often framed as taxes, administrative fees, commissions, or incidental expenses. In reality, there is no prize or deal to close.

Check Fraud: When someone steals a victim's checks or reproduces them and is then able to cash those checks.[27] Check fraud covers both counterfeit checks using a victim's account information and when a check is intercepted and altered to be paid to a different recipient.

Employment Scam: When scammers pose as recruiters or employers offering attractive employment opportunities.[28] They may steal the names of legitimate businesses and organizations. Scams may require victim to pay an advanced fee, provide personal information, or act as an unwitting money mule.

Government/Business/Bank Impersonation: When a scammer contacts a victim and claims to work with a government agency or the victim's bank/credit union to extract money from them. Government impersonators typically tell the victim they are under investigation when they are not or that they need to pay fees to get access to a government grant. Business impersonators often claim to be from Amazon or PayPal in order to initiate contact and make fraudulent payments appear more legitimate. Bank impersonators typically tell victims that their accounts are compromised, and they need to move their funds to a secure account, typically the scammer's account, to prevent them from being stolen.

Identity Theft: Crimes where someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.[29]

Investment Scam: When criminals try to trick victims into investing money into fictitious investments.[30] Scammers may make up a fake investment opportunity or use fake information about real investments.

25. *See* "Advisory on Account Takeover Activity," FinCEN Advisory #FIN-2011-A016," 19 December 2011, https://www.fincen.gov/sites/default/files/advisory/FIN-2011-A016.pdf.
26. *See* U.S. Securities and Exchange Commission, "Advance Fee Fraud," https://www.investor.gov/protect-your-investments/fraud/types-fraud/advance-fee-fraud.
27. *See* Reyna Gobel, "What is Check Fraud?" *Experian Fraud & Identity Theft*, 14 February 2018, https://www.experian.com/blogs/ask-experian/what-is-check-fraud/.
28. *See* State of Connecticut Department of Consumer Protection, "Employment Scams," https://portal.ct.gov/DCP/Common-Elements/Common-Elements/Employment-Scams.
29. *See* United States Department of Justice, "Identity Theft," https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.
30. *See* State of Tennessee Attorney General, "What You Need to Know About Investment Scams," https://www.tn.gov/attorneygeneral/working-for-tennessee/consumer/resources/materials/investment-scams.html.

Lottery Scam: When scammers lead victims to believe they have won a lottery or sweepstakes, but the cash prizes will not be released without up-front payments.[31]

Money Mule: Someone who transfers or moves illegally acquired money on behalf of someone else.[32] Money mules can be witting or unwitting, with unwitting money mules often being scam victims themselves. The use of money mules adds layers between crime victims and the perpetrators, which makes it harder to accurately trace money trails. Money mules may receive a commission for their services.

Person in Need Scam: Also called emergency scams or grandparent scams, this is when a criminal will contact a victim pretending to be a family member or loved one in a dire emergency and in need of money.[33] These scams have become more sophisticated with implementation of artificial intelligence.

Real Estate Scam: When scammers use real estate as a cover to steal victims' money.[34] These can be manifested in many ways, including wire fraud scams, mortgage scams, real estate investment scams, rental scams, or timeshare fraud.

Refund Scam: When scammers will claim they can help a victim get money back or recover a prize that was never received, but they take a payment and never perform a service.[35] Also instances of scammers transferring money between two victim accounts and claiming that they provided too great of a refund so the victim will send back the difference, when the funds are the victim's own money.

Retail Scam: Any type of scam involving retailers or online purchases. These can take many forms, including fraudulent purchases where money is taken but no product is provided or an inferior product is provided, sellers who steal credit card information, or use malicious links to steal personal information.[36]

Romance Scam: When a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic relationship to manipulate and/or steal from the victim.[37]

31. *See* U.S. Embassy in Kingston, "Lottery Scams," U.S. Embassy in Jamaica, https://jm.usembassy.gov/lottery-scams/.
32. *See* Federal Bureau of Investigations Safety Resources, "Money Mules," https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/money-mules.
33. *See* Washington State Office of the Attorney General, "Relative in Need or 'Grandparent' Scam, https://www.atg.wa.gov/relative-need-or-grandparent-scam.
34. *See* Jamie Johnson, "How to Avoid These 7 Real Estate Scams," *Rocket Mortgage*, 22 February 2023, https://www.rocketmortgage.com/learn/real-estate-scams.
35. *See* Federal Trade Commission Consumer Advice, "Refund and Recovery Scams," https://consumer.ftc.gov/articles/refund-and-recovery-scams.
36. *See* AARP, "Online Shopping Scams," 12 July 2022, https://www.aarp.org/money/scams-fraud/info-2019/online-shopping.html.
37. *See* Federal Bureau of Investigations Safety Resources, "Romance Scams," https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/romance-scams.

Tech Support Scam: When fraudsters pose as customer or tech support representatives from reputable, well-known companies. They contact their targets and offer to resolve fabricated computer issues and either request payment or convince victims to permit remote access to their computers and ultimately, their finances.[38]

38. *See* Federal Bureau of Investigations Boston Field Office, "FBI Warns Public to Beware of Tech Support Scammers Targeting Financial Accounts Using Remote Desktop Software," https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-public-to-beware-of-tech-support-scammers-targeting-financial-accounts-using-remote-desktop-software.