NICE · ACTIMIZE

Identification and Detection of Elder Financial Exploitation

TABLE OF CONTENTS

Identification and Detection of Elder Financial Exploitation

Background

Each year, older Americans lose billions of dollars from financial fraud (James et al. 108). Though the statistics are staggering, a misconception exists about the frequency of elder abuse. Even though the general public is unaware of the immensity of this problem, elder abuse has been described by many to be an “epidemic.” Despite the fact that it often goes unreported, financial crimes against the elderly make up the vast majority of financial fraud cases. Still, many hold the misunderstanding that the chances of becoming a victim is low or null. However, with the incredible number of different kinds of ploys and scams used, it is easy to see how an older individual could fall prey to elder abuse.

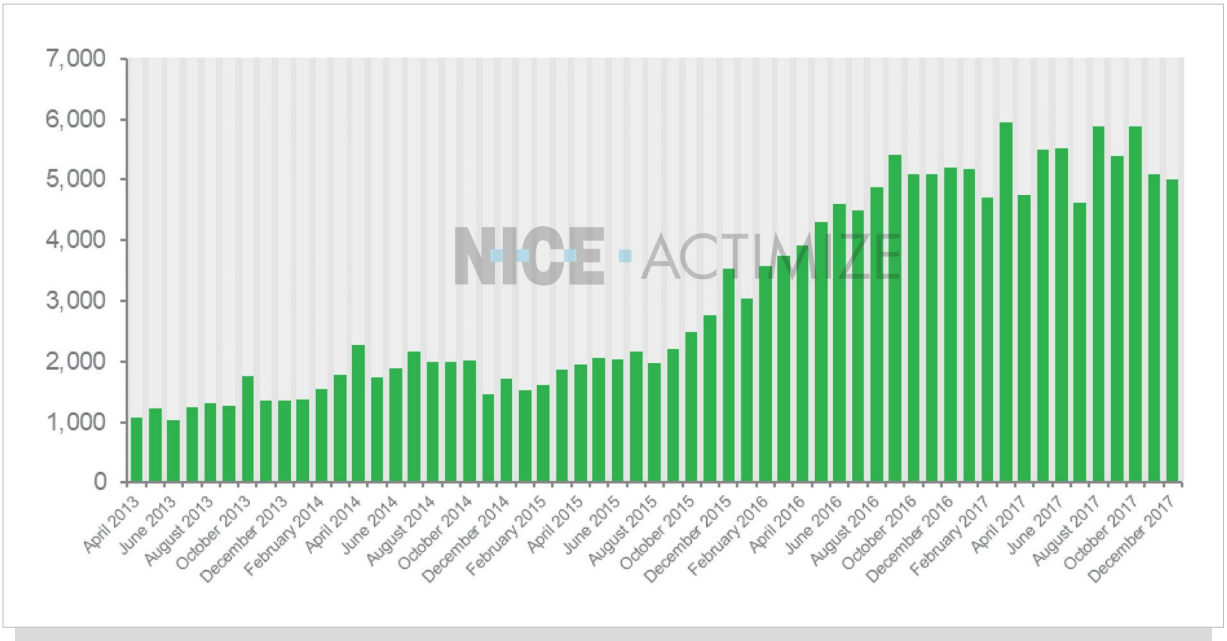
The Consumer Financial Protection Bureau (CFPB) recently published a summary of the Suspicious Activity Report (SAR) data identified as Elder Financial Exploitation from 2013 through 2017. This data reveals that Elder Abuse has continued to increase and the losses are staggering. Total dollar amounts on SARs from 2013-2017 total more than $6 billion. Authorities believe this number is vastly underreported and estimate actual losses to be anywhere between $3 billion to more than $36 billion dollars.

The study also revealed that the highest losses occurred for individuals ages 70-79. Average loss per incident for that age range was $45,300. In most of the cases, the losses were to the victim and not to the financial institution.

Interesting to note in regard to financial losses:

- One third of all reported victims are over the age of 80
- The overall average loss was $34,200
- Amounts exceeded $100,000 in 7% of the losses
- Losses to the elderly were higher (averaging $50,000) when the victim knew the abuser
- In cases involving strangers, average victim losses were $17,000
- Checking and savings accounts were most often impacted types of accounts
- Average length of time in the filings were 4 months or 120 days
- More than half of all losses involved money transfers

FIGURE 1: NUMBER OF EFE SARs BY MONTH (APRIL 2013-DECEMBER 2017)



Source: Bureau's analysis of EFE SARs filed between April 2013 and December 2017 (176,690 SARs)

Financial Institution Impacts

The reporting of EFE on the SAR forms was added in 2011. Since then, the quantity of reports has continued to grow significantly with the report number quadrupling over the 48 months noted with monthly averages at 1,300 reports in 2013 and 5,300 in 2017. The trends of where some of these filings occurred also shifted over the reporting period. From 2013 to 2015, the majority of the filings occurred in traditional financial institutions. Nearly 80% of the reports during that period were from banks and credit unions. In 2016, that trend started to change, shifting to just 35% of the reports coming from depository institutions in 2017. 58% of all reports were from MSBs in 2017 compared to just 15% in 2013.

Clearly, criminals are targeting our elders with their fraudulent schemes. So how do you start to mitigate the risk and protect elders from financial abuse? The first step is to understand the common types of schemes and who is involved in them. It is also important to note that losses tend to go underreported in both categories of exploitation. In the Stranger Scams, elders are typically embarrassed by being taken advantage of and can form emotional bonds that they feel a sense of loyalty to protect the fraudster. In the case of known abusers, the elder does not want to be responsible for an arrest or prosecution of a loved one. In all these cases, the fraud is considered "consumer authorized fraud," as the elder is manipulated into willingly transferring or allowing access to assets.

Fraud Schemes

The fraud schemes are varied but there are two broad categories identified:

Stranger Scams

Elders have been a target of scammers for many years. The various types of schemes that are identified in elder financial exploitation is growing in creativity but losses and the typologies vary, so detection becomes more challenging to manage. As previously noted, losses are typically lower than those that involve more "friendly fraud" but they are significant nonetheless. The method of loss in these

scenarios involve money transfers. (We will discuss these mechanisms in the next section) The common types of schemes currently seen are:

- **Romance scams**—Romance schemes, like most EFE scenarios, involve strong emotional ties. Fraudsters typically invest many hours in writing and sometimes calling and talking on the phone to create loyalty and trust in their victims. Preying on the elders' emotion is the common thread in these stranger scams, but fraudsters feel they have "earned" their bounty due to the investment of time in the target. The scenario unfolds like this: Victim is targeted, usually through online dating services. Commonly, the fraudster preys on the loneliness of an elder that lives alone, is recently divorced or widowed. There is typically a lucrative career that is dangled in front of the victim. The persona created by the fraudster just needs to complete one last job, visit a relative or some other activity that will "take them outside the country." Once they complete the last task, the romantic interest will be free to come and live happily ever after with the victim. Unfortunately, along the way, there are issues that come up that the romantic interest needs assistance with. They are stuck in a foreign country, don't feel safe, can't access their bank accounts, etc. and they urgently require the assistance of the victim. The victim then transfers funds to the romantic interest to get them out of a jam. Typically, there is a "mule" that is a transfer agent to receive the funds. The mule's job is to get the funds from their account to the fraudster. This helps alleviate foreign transfer issues that can be prohibitive to the victim's financial institution or even relatives.
- **Lotto/sweepstakes Scams**—Lotto scams are much quicker hitting scams. Contact occurs either through email initially or sometimes through social media mechanisms. Fraudsters will hack into a contact profile in order to direct them to a transfer agent to allow them to claim their lottery winnings, sweepstakes or "grant" funds that they are entitled to. In order to get the funds, the victim only need send in the taxes first to allow release of their funds. Once the taxes are paid, the funds can be transferred to the bank account of the victim. Usually the funds are paid through money transfer services. The fraudsters request that the victim use Western Union, MoneyGram or another transfer agent to send funds. These fraudsters are all aware of the daily limits of these services and work to structure the transfers under these limits. In many cases, there will be multiple transfer requests as additional "taxes" are discovered in order to receive the funds that of course never materialize.
- **Relative in Need**—This scam is typically known as the grandparent scam. Victims are targeted by telephone and advised that their grandchild is in some kind of trouble. Either they have been stopped by the police, arrested in a foreign country or other such malady. The victim must send money immediately to save their grandchild. No time to call anyone to confirm the grandchild's where about. Some scammers even go so far as to have the supposed grandchild on the phone to express their distress to the grandparent. The amounts of this scam vary but they are typically lower amounts than the previous two schemes. The investment of time by the scammers is also lowest as they typically just involve dialing numbers until they get a victim that will engage.
- **Mule schemes**—Because elders are typically living off a fixed income, fraudsters take advantage of this labor pool by targeting elders for "work from home" or other scams that have them accepting deposits or payments on behalf of fraud rings or scammers. These elders are typically unwitting facilitators of fraud rings or money launderers. In some cases, elders are "hired" to do things like "secret shopping" or purchasing money orders or other financial instruments or even electronics to ship. These scams can be greatly varied and typically financial losses are limited. Instead, fraudsters expose the mules to risk of law enforcement action or other risks. The leading indicators in these schemes will be deposits from new sources into the bank account of an elder.
- **IRS Tax Fraud**—Fraudsters pose as IRS agents using spoofed numbers to call the victim and explain that they owe back taxes that must be paid immediately. This form of fear is used to threaten loss of the victim's home, bank account, arrest, etc. if the debt is not paid immediately. The victim is convinced that they must pay the bill right away to

avoid prosecution and asset seizure by the IRS. The victim is then instructed to move the funds, many times to an offshore location via the use of a money transfer agent, prepaid card or other mechanism.

FIGURE 2: PERCENT OF EFE SARs WITH A LOSS TO THE OLDER ADULT AND AVERAGE MONETARY LOSS BY SUSPECT CATEGORY (APRIL 2013 – SEPTEMBER 2017)

Suspect Category	Percent of EFE SARs within a suspect category involving a loss to the older adult[a]	Average (median) loss per older adult[b]
Stranger	75%	$17,000 ($8,500)
Known person[c]	79%	$50,200 ($23,200)
Family[d]	82%	$42,700 ($24,900)
Fiduciary[e]	88%	$83,600 ($33,800)
Non-family caregiver[e]	76%	$57,800 ($21,800)

Source: Bureau's analysis of a random sample of EFE SARs (1,051 SARs)

Notes: (a) Percentages include EFE SARs with partial losses. (b) Average and median loss amounts per older adult are based on the EFE SARs where the entire amount reported is a monetary loss to the older adult, and excludes SARs with no losses, partial losses or any loss to the filer. (c) The known person category includes fiduciaries, family members, non-family caregivers and others individuals such as friends, neighbors, accountants, and contractors. (d) The fiduciary category includes family members and non-family caregivers who serve as fiduciaries. (e) The family member and non-family caregiver categories include fiduciaries.

Caregiver Fraud

This second kind of loss involves exploitation of the elder's assets by a family member, fiduciary or caregiver. This is a much more difficult fraud to detect. In many cases, the victim does not want to get their caretaker in trouble. In even more situations, the victim is not aware of the additional spending and draining of accounts and assets and sometimes even loans that occur in the victim's name. Since these types of fraud are typically perpetrated by someone that has monetary control and some degree of trust, the losses are especially devastating. As previously stated, the losses in this category can be much higher than stranger scams.

This "friendly" fraud typically involves bank accounts (checking and savings) as opposed to money transfers or MSBs and occurs over a longer period of time. As previously stated, because of the trusted relationship, easy access to funds and longer average timelines losses are much higher to the elder. The difference is typically several times that of the stranger scams, making them much more devastating to the victim.

How Can Financial Institutions Detect These Scams?

The detection of these specific typologies is more challenging to identify below is a typology matrix to help create a starting point for the various scenario detection.

Type of scheme/ Victim Relationship	Scenario	Bank products	Transfer mechanism	Detecting Dollar ranges	Number of incidents	Counterparties	Timeline	Behavior Deviation
Stranger	Romance	Savings, Checking	Predominantly transfer agents, WU, MG, etc.	Higher-typically $6,000-$9,999 each	1-5 typically	US Intermediaries, large FI accounts	1-3 months	Significant spike, fraudster works to stay under structuring limits
Stranger	Lotto	Savings, Checking	Transfer agents, prepaid cards, p2p transfers, PayPal	$600-$2,400	1-3	Third parties, strangers that have not been seen in payments prior	2-4 weeks	Drastic spike with 1-3 lower dollar transfers to a high-risk counter party
Stranger	Relative In Need	Savings, Checking	Transfer agents, prepaid cards, PayPal, p2p (pull request)	$300-$2,400	1-2	Third parties, sudden appearance of new payees	1 day	Smaller dollar spike with a payment to a new payee, usually through a transfer agent
Stranger	IRS	Savings, Checking	Prepaid cards, transfer agents	$1,300 - $9,999	1-5	IRS through intermediaries	4-6 weeks	Appearance of a new counterparty
Known Person	Caregiver Family Member Fiduciary	Savings, Checking, Loans, credit cards	Checks	Start small $100 to thousands	Many	Checks or direct transfers, also payments on behalf of the caregiver to vendors	4-6 months or longer	Gradual change in account usage patterns that escalates over time, loans suddenly taken out in the elder's name

Stranger scams - Many of the indicators of these types of fraud is similar with variations on a theme. With all these stranger scams, the dominant method of transfer is third party money transfers, typically (+70%) Money transfers are largely used, from a bank account to a transfer agent and sometimes direct. First stop for the money is domestic. Scam artists use an intermediary (mule) to transfer the funds from the victim to a US account. The mule will usually transfer the funds overseas or to another destination.

Romance Scams - Can take place over a long period as the scammer develops a relationship with the victim. They typically exploit the victim for several payments as "emergencies" come up for the romantic interest's account. Losses are typically $15,000 and involve more than one transfer of funds to the scammer.

Lotto/Sweepstakes scam – involve MSBs, money transfers or prepaid cards for transfer mechanism. Smaller dollar amounts at first with escalating payments

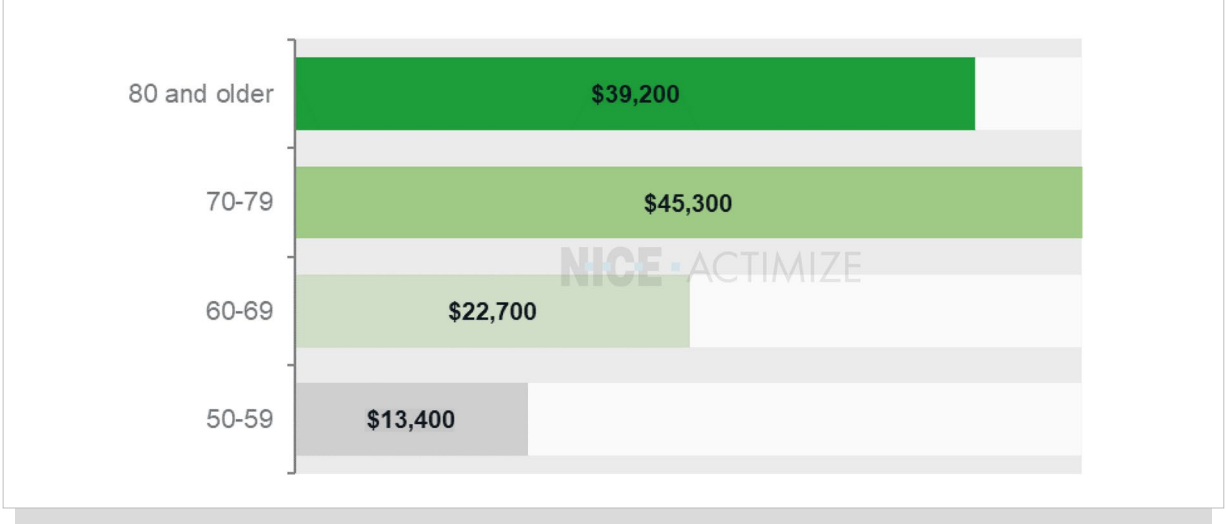
Relative in Need - Single payment typically - this will act more like burst activity with a quick, usually one-time payment. However, once scammers identify a "meal ticket," they may target the victim repeatedly.

IRS - Threats of loss of home, jail time and other scare tactics are utilized by these scammers to elicit one or multiple payments from victims.

Caregiver or Fiduciary Fraud - Fraud in this category is more difficult as it is likely to occur over a longer period of time. When a known "directly involved" person exploits an elder the losses are much higher at nearly $50K average. Most of these frauds are perpetrated on bank accounts with abusers sometimes having account access. It's important to note a change in spend pattern from earlier patterns, out of band spend patterns, as well as new payees on the account. Escalating spend patterns are hallmarks of this type of exploitation.

Other helpful detection mechanisms are to look at the age of the customer. Since one-third of all EFE victims are 80 or older, flagging these types of entities as higher risk for consumer authorized fraud and other exploitation would be a good step in helping protect elders. Those in the 70-79 age range suffer the highest loss amounts which would make this age band the highest risk for exploitation.

FIGURE 3: AVERAGE MONETARY LOSS BY AGE OF THE TARGETED OLDER ADULT (APRIL 2013 – SEPTEMBER 2017)



Source: Bureau's analysis of a random sample of EFE SARs (324 SARs)

Note: Based on EFE SARs where the age of the targeted adult(s) is stated. Excludes EFE SARs showing no loss or a partial loss to the older adult or any loss to the filer.

Looking at the transaction risk and the various indicators of fraud with this kind of abuse can help you start to identify the potential risk to our elders. Creating a risk score that looks at the factors of risk can assist you in escalation of the appropriate scenarios. Understanding how EFE cases represent themselves at your institution can also assist you in creating a very specific typology for your organization. Since elders are typically creatures of habit, changing spend patterns can create opportunities for staff to interact with the customer, identify risk of the transactions and inform how to investigate any alerts from the system as well as understand when to escalate an alert to a case.

Investigating the Alerts and Cases

The investigation and methods utilized for the alerts that can appear around EFE can be a more sensitive and difficult process. In the case of stranger fraud, remember that each of the scenarios outlined have various degrees of emotional investment. The higher the emotional investment of the victim, the higher the losses. When investigating these situations, be sensitive to the potential embarrassment and emotion of the victim. If you do reach out to the victim, they are typically moving money to these schemes willingly. To understand the manipulation of each scheme, try to keep any questions factual in nature. Ask about how the victim met the person, how long they had conversations, did they speak directly to the person, what was the reason given that the person needed the money. At the same time, understand there may be a second victim that is being utilized as a mule.

When reviewing preliminary alerts, there may be dollar thresholds that your organization uses as the determining factor of proceeding. Look at the typical spend patterns of the elder and if the amounts are outside the bounds of normal without a reasonable explanation (medical, large asset purchase, etc.) or if it involves frequent money transfers or any international funds movement, escalate the case for further review. In addition, research all that you can about the counterparty in the case. One romance scheme example utilized a stock or artificial intelligence (AI) generated photo and the name of the romantic interest was vanilla and very common. The story communicated to the victim was inconsistent and the email communications with the victim indicated that English may not have been their first language. Some of the transfers that were done were to mules first and second to entities outside the US.

In the event of alerts that look to be more focused on a caregiver fraud, this is an even more volatile situation. It can involve physical abuse, mental abuse and manipulation. At the alert phase, look to the change in pattern of the spend of the original account holder. If the addition of the co-signer to the account sees major changes in *who* is being paid and how frequently, the case should be escalated. Are there new payees that have been added that are outside the norm for the client? Frequent cash withdrawals, payments to completely new payees, even payments to the caregiver themselves will likely start out small. If those outflows of funds start to increase, the issue should be quickly escalated. Be sensitive again to the fact that the person perpetrating the fraud may be a family member, loved one or other trusted person to the victim. If you speak to the victim, again stick to the facts, the mechanics of the account activity. Questions may feel very invasive and personal to the victim, which will limit their cooperation. Since these are complicated and sensitive frauds, there are two main objectives: first to limit the additional drain of the accounts and second to involve resources to assist the victim. The reporting section outlines these types of reporting activity, but these reports can be critical to helping the victim preserve their independence.

Reporting

Even though the issues that many organizations are seeing with EFE are being reported to FinCEN, the one issue noted in the CFPBs review of Elder Financial Exploitation was the lack of reporting outside of FinCEN. Adding a report to local law enforcement or to a local Adult Protection Agency can help further protect our seniors from ongoing abuse and get them a resource to help them address their situation in a more timely manner. That additional step could make a significant difference in dealing with and stopping significant financial abuse. This is a discussion that each bank should consider adding to their internal procedures to assist in protecting their valued customers or members. You can find out how to reach your APS office from the Eldercare locator at eldercare.aci.gov or by calling 1.800.677.1116.

Conclusion

In conclusion, Elder Financial Exploitation is a threat to the independence and mental and physical health of our elderly population. Even though this piece addresses the financial, the financial health of our elders has a direct impact on their overall well-being. In addition, in caregiver/known person fraud, the is also a correlation between financial and physical. Sometimes physical threats, abuse and harm that can go hand-in-hand with the EFE by known persons. Identifying and reporting the potential abuse starts with stopping financial exploitation but can also create a spotlight on other types of abuse and can create a lifeline for those seniors who are unsure where to turn or how to make the abuse stop.

In order to make the detection and identification of these issues a more robust part of your operations, create typologies to identify transaction risks and patterns of behavior. Using the foundation laid out above and potential “risk” additions based on age ranges and key indicators, we can better detect the changes in the spending patterns of elders. Compare your organization’s typologies by doing case reviews on known EFE case types.

Understand the first leading indicator may be a small change in spend behavior. Understanding the AML function can also be very beneficial. Changes in the flow through of funds in an account, structuring thresholds by different sources and other such behavior by the perpetrators can also give you alerts of changes in an account. Such threshold evasion can be clear signs that foul play may be involved in the account activity.

Train your investigations staff to recognize the various scenarios and know when, and how, to escalate and consider reporting to additional agencies. These kinds of adjustments to your operations could make all the difference to your customer or member in protecting their financial security.

How we can help?

NICE Actimize provides solutions that are dedicated to protecting banks' customers from fraud threats like Elder Financial Exploitation. Our solutions apply machine learning analytics to detect Elder Abuse and related scenarios. These detection analytics have been optimized and trained by our expert fraud data scientists based on years of experience and a large database of big and small Financial Service Organizations (FSOs). The detection models can be further optimized by the specific FSO data and are monitored overtime to ensure continuous high performance.

With a robust alert and case manager, and special workflow to support the alert resolution, investigation, quality and audit and reporting of EFE cases, our solutions provide a single platform to allow central management of solutions, operations and cases.

ABOUT NICE ACTIMIZE

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

Stay current with NICE Actimize webinars at actimize.nice.com/events

info@niceactimize.com | niceactimize.com/blog | @NICE_actimize | /company/actimize | NICEactimize

NICE · ACTIMIZE