



# Protecting Seniors:

A Bank Resource Guide for  
Partnering with Law Enforcement  
and Adult Protective Services



**SAFE BANKING  
FOR SENIORS**

ABA FOUNDATION

### **About the ABA Foundation**

The ABA Community Education Foundation (dba ABA Foundation) is a 501(c)3 corporation that empowers bankers to help make their communities better. Since 1925, the Foundation has helped bankers provide financial education to individuals at every age, elevate issues around affordable housing and community development, and achieve corporate social responsibility objectives to improve the well-being of their customers and their communities.

### **About the American Bankers Association**


The American Bankers Association is the united voice of America's banks—small, regional and large—that together employ more than 2 million women and men, hold nearly \$17 trillion in assets, safeguard \$13 trillion in deposits and extend more than \$10 trillion in loans. Through a broad array of information, training, staff expertise and other resources, ABA supports America's banks as they perform their critical role in energizing the economy and helping communities thrive.

### **© 2021 American Bankers Association**

This publication was paid for by ABA Foundation and its sponsors and is solely intended for use by banks. Please call 1-800-BANKERS if you have any questions about this resource or ABA membership. This publication is designed to provide accurate information on the subject addressed. It is provided with the understanding that neither the authors, contributors nor the publisher is engaged in rendering legal, accounting or other expert or professional services. If legal or other expert assistance is required, the services of a competent professional should be sought. This guide in no way intends or effectuates a restraint of trade or other illegal concerted action.

# Table of Contents

<b>Introduction</b> .....	5
<b>The State of Elder Financial Exploitation Today</b> .....	6
How large is the problem? .....	6
Who is an elderly customer? .....	6
What are the ramification of elder financial exploitation for victims? .....	7
Why is elder financial exploitation growing so fast? .....	7
Who are the perpetrators of elder financial exploitation? .....	8
What are the potential signs of elder financial exploitation? .....	8
Why is combatting elder financial exploitation important for banks? .....	9
<b>Top Scams Currently in Play</b> .....	9
What are today's most prevalent scams? .....	9
<b>What Can Be Done?</b> .....	12
Educate consumers .....	12
Banker training .....	12
Note changes in customer activity .....	12
How do we proceed when we notice something? .....	13
<b>Roles of APS and Law Enforcement</b> .....	14
Tell me more about Adult Protective Services (APS) .....	15
What principles shape APS? .....	15
Does APS operate the same everywhere? .....	15
What is the best way to work with APS in an ongoing investigation? .....	16
How can I find the APS closes to me? .....	16
How can APS handle their growing caseload? .....	16
Do APS and law enforcement work together? .....	17
How can a bank best aid local law enforcement? .....	18
What law are in place that govern reporting requirements? .....	18
What is happening at a national level? .....	19



<b>Reporting</b> .....	20
How do I report suspected elder financial exploitation? .....	20
What is the time frame to file a SAR? .....	20
Are there specific thresholds that dictate when to file a SAR? .....	21
Are banks required to file with APS if we are already filing a SAR? .....	23
What happens after a banker files a report with APS? .....	25
How can we provide information without violating our customers' privacy? .....	25
<b>How to Partner with APS and Law Enforcement?</b> .....	26
How do we begin? .....	26
Do elder fraud prevention networks exist? .....	26
What can I do if an elder fraud prevention network does not exist in my area? .....	28
What are the key things to remember about dealing with elder financial exploitation? .....	28
<b>Case Study: Bank of the Rockies</b> .....	29
<b>Appendix</b> .....	31
Top Scams .....	31
<b>Resources for Creating Partnerships</b> .....	34
<b>Additional Resources for Combating Elder Financial Exploitation</b> .....	35
Introductory Letter to Law Enforcement .....	37
Introductory Letter to Adult Protective Services .....	38
Introductory Letter # 2 to Adult Protective Services .....	39
Introductory Letter to Local Non-Profit Focused on Seniors .....	40
Introductory Letter to Senior Living Facility .....	41

# Introduction

Each year older adults lose billions of dollars to financial exploitation. Defined as the illegal or improper use of an older person's funds, property or assets, elder financial exploitation (EFE) is a devastating crime.<sup>1</sup> It not only impacts an elder's financial situation, but often takes an emotional toll as well. Victims of such abuse frequently experience intense feelings of fear, depression, anger, and humiliation.<sup>2</sup> In turn, abused elders may be at risk of poorer health outcomes and increased mortality relative to their counterparts.<sup>3</sup>

Fraudsters prey on elders because as a whole, older adults possess more financial assets than other demographics. Seniors tend to own their own homes, have accrued savings over their lifetimes, generally have better credit and tend to be more trusting of others relative to younger populations.<sup>4</sup> Consequently, criminals have engineered specific scams, such as the grandparent scam and other impostor scams, to target America's elderly.

Effectively combatting EFE requires a multifaceted approach. Protecting seniors rests in the hands of several different professions, while no single discipline can bear it all. Banks play a critical role due to the financial nature of the crime but banks cannot do it alone. Banks can connect and coordinate with federal, state, and local partners to protect our senior citizens.

This resource was designed to support banks in developing relationships with law enforcement and adult protective services (APS) to combat EFE. It is largely set up as a number of frequently asked questions to help guide the reader to understand:

- the state of elder financial exploitation today,
- the role of APS and law enforcement,
- reporting EFE, and
- cultivating partnerships with key community players.

In developing this tool, ABA Foundation consulted with government agencies, law enforcement officials, APS workers, banks, and state bankers associations. It is free to download and distribute.

---

1 [https://files.consumerfinance.gov/f/documents/cfpb\\_suspicious-activity-reports-elder-financial-exploitation\\_report.pdf](https://files.consumerfinance.gov/f/documents/cfpb_suspicious-activity-reports-elder-financial-exploitation_report.pdf)

2 Nerenberg L. (2000). Forgotten victims of financial crime and abuse: Facing the challenge. *Journal of Elder Abuse and Neglect*, 12, 49-72

3 Burnett J, Jackson SL, Sinha A, Aschenbrenner AR, Xia R, Murphy KP & Diamond PM. Differential Mortality across Five Types of Substantiated Elder Abuse. *Journal of Elder Abuse and Neglect*, 2016; 28:2, 59-7

4 <https://www.giaging.org/issues/financial-exploitation/>

**“No matter how big or small your bank is, we all need to be aware elder financial exploitation can and does happen.”**

**JENNELL HUFF**

Relationship Manager/Outreach Coordinator

Bank of the Rockies, Clyde Park, MT

## **The State of Elder Financial Exploitation Today**

### **How large is the problem?**

Published reports vary in the scale of losses, where annual estimates typically range between \$2.9 and \$36.5 billion. Data on the losses suffered by individuals also varies; a 2019 Consumer Financial Protection Bureau (CFPB) analysis of a sample of Suspicious Activity Reports (SARs) found that elders lost an average of \$34,200 from financial exploitation<sup>5</sup> while others, such as AARP, found that the average amount lost to EFE is upwards of \$120,000.<sup>6</sup>

Much of the difficulty in identifying the extent of the problem is that EFE is often underreported. An elder prevalence study from NYS found that only one in 44 cases of elder financial abuse was reported. Many seniors don't volunteer to share their experiences due to shame or potential fear of retaliation—particularly if a family member committed the crime. Consequently, banker vigilance is especially important in recognizing the signs of EFE.

### **Who is an elderly customer?**

Many banks offer “senior” banking programs to customers age 50 and older. Once customers reach the age of 62, they become a federally protected class. However, not everyone in this age range may consider themselves to be an elder. There may be generational differences between “younger elders” and “older elders.” The most vulnerable to exploitation are those who are socially isolated, have poor physical health and those who experience cognitive impairment.

<sup>5</sup> [https://files.consumerfinance.gov/f/documents/cfpb\\_suspicious-activity-reports-elder-financial-exploitation\\_report.pdf](https://files.consumerfinance.gov/f/documents/cfpb_suspicious-activity-reports-elder-financial-exploitation_report.pdf)

<sup>6</sup> <https://www.aarp.org/money/scams-fraud/info-2019/bank-tellers-prevent-financial-fraud.html>

## What are the ramifications of EFE for victims?

Financial exploitation is no simple matter. Older adults do not have the same amount of time and may not have the means to recoup a large loss experienced late in life. Such losses can impact a senior's health, wealth, and emotional well-being. EFE is an egregious crime that robs victims of their livelihoods and dignity. Exploited seniors often experience depression, shame, guilt, fear, and loss of security.<sup>7</sup> Depending on the magnitude of the loss, they may lose their homes, which in turn, can increase their risk of mortality.

## Why is elder financial exploitation growing so fast?

Part of the reason this is a fast-growing crime lies with the aging of the nation. America is experiencing a demographic shift, often referred to as the “age wave” or “silver tsunami.” Every day 10,000 baby boomers—Americans born between 1946 and 1964—are turning 65 and will continue to do so until 2030. By 2034, there will be more people ages 65 and above than children for the first time in history of the United States.<sup>8</sup>

Older demographics possess more wealth than younger populations. A 2020 Federal Reserve bulletin observed the following median net worth data by age:<sup>9</sup>

- Less than 35: \$13.9K
- 35-44: \$91.3K
- 45-54: \$168.6K
- 55-64: \$212.5K
- 65-74: \$266.4K
- 75+: \$254.8K

The three elder demographics possess higher net worth than the three younger cohorts. As a result, criminals looking to illegally acquire wealth often target those who have more of it.

7 <https://www.marketwatch.com/story/scams-are-taking-a-heavy-emotional-toll-on-senior-citizens-2020-03-05>

8 <https://www.census.gov/newsroom/press-releases/2018/cb18-41-population-projections.html>

9 <https://www.federalreserve.gov/publications/files/scf20.pdf>

## Who are the perpetrators of elder financial exploitation?

The perpetrator of these crimes can be anyone. Frequently, victims know the culprit. In a 2014 study of over 4,000 older adults, nearly 60% of those who financially abused elders were family members.<sup>10</sup> But, the perpetrators may also be completely unrelated to the victims. Often times these unknown agents are part of transnational criminal organizations seeking to exploit America's elders. These latter suspects typically engineer scams, such as those highlighted at [ftc.gov/scams](https://www.ftc.gov/scams), to con elders out of their hard earned savings.

## What are signs of potential elder financial exploitation?

1. Unusual activity in an older person's bank accounts, including large, frequent or unexplained withdrawals
2. Changing from a basic account to one that offers more complicated services the customer does not fully understand or need
3. Withdrawals from bank accounts or transfers between accounts the customer cannot explain
4. A new "best friend" accompanying an older person to the bank
5. A senior who is not allowed to speak for themselves or make decisions
6. Seniors who seem to be afraid of the person who accompanies them
7. Sudden non-sufficient fund activity or unpaid bills
8. Closing certificate of deposits (CDs) or accounts without regard to penalties
9. Uncharacteristic attempts to wire large sums of money
10. Suspicious signatures on checks, or outright forgery
11. Confusion, fear or lack of awareness on the part of an older customer
12. Checks written as "loans" or "gifts"
13. Bank statements that no longer go to the customer's home
14. New powers of attorney the older customer does not understand
15. A caretaker, relative or friend who suddenly begins conducting financial transactions on behalf of an older person without proper documentation
16. Altered wills, trusts, and other legal documentation

---

<sup>10</sup> <https://ncea.acl.gov/What-We-Do/Research/Statistics-and-Data.aspx#18>



## Why is combatting elder financial exploitation important for banks?

Older adults represent a sizable proportion of bank depositors. ABA Foundation's 2019 Older Americans Benchmarking Survey Report found that while people aged 55 and older comprise about a third of the population, they account for 70% of bank deposit balances.<sup>11</sup> Preventing financial exploitation is not only an important moral obligation, it's a sound financial practice.

## Top Scams Currently in Play

### What are today's most prevalent scams?

The table on the following page highlights some of the top financial scams perpetrated against seniors, as identified by several groups including AARP, the CFPB and the Financial Crimes Enforcement Network (FinCEN). The table also lists the agencies to contact when fraud is suspected or confirmed in addition to filing SARs with FinCEN.

Bankers should also check with their State Attorney General's Office to determine if they recommend any other reporting avenues. Be sure to also check out the FTC's resources to keep abreast of new scams at: <https://www.consumer.ftc.gov/scam-alerts>.



<sup>11</sup> <https://www.aba.com/-/media/documents/reports-and-surveys/2019-older-americans-benchmark-report.pdf?rev=219abb5495f146c99b9a0a97e3f66d84>

Scam	Description	Responsible Agency	Submit a Complaint
<b>Cemetery / Funeral</b>	Criminals read obituaries and call survivors claiming that the deceased owed them a debt to extort money from living relatives.	Federal Trade Commission	<a href="http://www.reportfraud.ftc.gov">www.reportfraud.ftc.gov</a>
<b>Charity</b>	Con artists reach out and claim to be from an organization with a carefully crafted name. They ask for a donation to obtain access to financial information, such as credit or debit card numbers. They often pop up after disasters. Others falsely state that they fundraise to support veterans.	Federal Trade Commission	<a href="http://www.reportfraud.ftc.gov">www.reportfraud.ftc.gov</a>
<b>Check Fraud</b>	Con artists send people money via check, claim they overpaid, and then ask the victim to send part of it back. But, the original check was fraudulent, so the victim ends up sending their own money to the criminal.	Federal Trade Commission U.S. Postal Inspection Service	<a href="http://www.reportfraud.ftc.gov">www.reportfraud.ftc.gov</a> <a href="http://www.uspis.gov">www.uspis.gov</a>
<b>Counterfeit Prescription Drugs</b>	When elders search for cheaper prescriptions online they may end up purchasing bogus products or drugs containing harmful substances.	Food and Drug Administration	<a href="http://www.fda.gov/safety/med-watch-fda-safety-information-and-adverse-event-reporting-program">www.fda.gov/safety/med-watch-fda-safety-information-and-adverse-event-reporting-program</a>
<b>Fraudulent Anti-aging Products</b>	There are a number of fake products on the internet and fraudsters are seeking to take advantage of people who want to look younger. Con artists develop phony companies and sell products that either do nothing or may harm you.	Food and Drug Administration Federal Trade Commission	<a href="https://www.fda.gov/safety/report-problem-fda/consumer-complaint-coordinators">https://www.fda.gov/safety/report-problem-fda/consumer-complaint-coordinators</a> <a href="http://www.reportfraud.ftc.gov">www.reportfraud.ftc.gov</a>
<b>Health Insurance / Medicare</b>	Scammers either pose as Medicare or health insurance representatives to obtain personally identifiable information from elders or provide unnecessary services at makeshift clinics and then bill Medicare to ensure they can keep the money.	Department of Health and Human Services Office of Inspector General or State Insurance Fraud Department	<a href="http://oig.hhs.gov/fraud/report-fraud">oig.hhs.gov/fraud/report-fraud</a>
<b>Homeowner / Mortgage</b>	Scammers may send fake, but professional looking letters to people on behalf of their county offering to reassess their home values for a fee to address their tax burdens.	Federal Trade Commission Federal Bureau of Investigation State Attorney General	<a href="http://www.reportfraud.ftc.gov">www.reportfraud.ftc.gov</a> <a href="http://www.fbi.gov/contact-us">www.fbi.gov/contact-us</a> <a href="http://www.naag.org/find-my-ag">www.naag.org/find-my-ag</a>

Scam	Description	Responsible Agency	Submit a Complaint
<b>Impostor</b>	<p>Fraudsters may call or send text messages impersonating government officials to manipulate elders into sharing sensitive information. Alternatively, they may pretend to be family members in an emergency situation and claim they need money right away.</p> <p>Scammers may also pose as technology support representatives to offer to fix non-existent computer issues to capture personal information and have seniors pay for useless services.</p>	Federal Trade Commission	<a href="http://www.reportfraud.ftc.gov">www.reportfraud.ftc.gov</a>
<b>Internet / Email</b>	<p>Criminals pose as romantic interests on social media platforms or dating websites to exploit older adults out of their life savings.</p> <p>Elders may receive emails asking them to update or verify their personal information from a seemingly legitimate organization, but if they click the links, they will be providing sensitive information to criminals.</p>	<p>Federal Communications Commission</p> <p>Federal Trade Commission</p> <p>Internet Crime Complaint Center IC3</p>	<p><a href="https://consumercomplaints.fcc.gov/hc/en-us">https://consumercomplaints.fcc.gov/hc/en-us</a></p> <p><a href="http://www.reportfraud.ftc.gov">www.reportfraud.ftc.gov</a></p> <p><a href="http://www.ic3.gov">www.ic3.gov</a></p>
<b>Lottery / Sweepstakes</b>	An older adult may receive a message indicating that they won a foreign or domestic prize or lottery, but are required to pay a fee to access their "winnings."	Federal Trade Commission	<a href="http://www.reportfraud.ftc.gov">www.reportfraud.ftc.gov</a>
<b>Telemarketing / Phone</b>	An elder may receive calls from fraudsters indicating that they found a large sum of money and would split it if the elder would provide or pay a smaller sum of money.	Federal Communications Commission	<a href="https://consumercomplaints.fcc.gov/hc/en-us">https://consumercomplaints.fcc.gov/hc/en-us</a>



# What Can Be Done?

## Educate consumers

Education is one of the strongest tools in preventing elder financial exploitation. An informed consumer, one who is aware of prevailing scams and how criminals seek to exploit people, is more likely to recognize frauds and therefore be less likely to fall prey to them. Through ABA Foundation's Safe Banking for Seniors program, bankers can access free turnkey materials to engage with their communities and lead in-person workshops or virtual presentations to help elders understand how to protect their financial assets and identities. The comprehensive list of resources includes presentation slides, instruction guides, traditional communications tools, social media posts, infographics, and promotional graphics to share about avoiding scams, preventing identity theft, financial caregiving, powers of attorney, executors, and more. Bankers can register for free at [www.aba.com/seniors](http://www.aba.com/seniors) to access the materials. Non-banker groups can request free presentations from participating banks using the ABA Foundation's financial education platform at [www.aba.com/FinEdLink](http://www.aba.com/FinEdLink).

## Banker training

Learning how to prevent, detect, and address EFE is critical to effectively protecting older customers. Bankers can access banker-tailored trainings about how to identify EFE, review the ways seniors are vulnerable to fraud, explain how to report EFE, and discuss the role banks can play in recognizing and combatting it. ABA's Frontline Compliance Training, free to ABA member banks, includes courses on elder financial exploitation prevention, which can be found at [www.aba.com/frontline](http://www.aba.com/frontline). Separately, AARP offers BankSafe, a program designed to help financial institutions protect their older customers' assets.<sup>12</sup> Other options may also be available through state bankers associations or offered through state governments.

## Note changes in customer activity

Banks monitor customer activity to detect anything that might be suspicious. Even if frontline employees don't notice anything, most banks have predictive software that may identify changing patterns and trigger an alert on any anomalous activity, such as increased frequency and amounts of withdrawals, deposits of checks from unknown entities out of the area, first-time requests for payments through wire transfers, money orders or cashier's checks.

---

<sup>12</sup> <https://www.aarp.org/ppi/banksafe/>

Some examples to consider: has Mr. Abuelos suddenly started withdrawing the same amount in cash on a regular basis when previously he just made deposits and wrote checks? Did Mrs. Streeter come in with a “nephew” and get a cashier’s check when you know that she was an only child without relatives? What about Ms. Glueck showing up on the nonsufficient funds (NSF) report twice in the last two weeks when she has been a customer for more than 20 years and never before overdrew her account or bounced a check?

## How do we proceed when we notice something?

The first thing we should do is assess the situation to determine if something is amiss. The bank should have procedures for handling unusual or possibly suspicious transactions, which will lay out what you should do. But, asking questions if and when you suspect financial exploitation can be a critical first step. However, inquiries must be handled carefully to not make the situation worse. Often times, an elder may be pressured into conducting a transaction without having sufficient time to think through everything, but a teller who asks the right questions may make all the difference.

In responding to suspected fraud, banks have found it helpful to:

- establish the reason for an unusual transaction. Answers that indicate a customer can’t speak about it, whether it’s a “personal” matter or one that they simply refuse to discuss may be suspicious;
- offer the customer privacy to discuss sensitive or confidential information separate from accompanied acquaintances or strangers;
- reassure the customer that you are trying to protect them. Consider mentioning that the transaction seems unusual for the customer, that it looks like a potentially fraudulent situation and that you’re trying to protect the customer;
- bring in a supervisor to review the transaction; and
- reconfirm the authorization for the transaction with the older customer.

As you work through your process, it’s important that you follow bank policy, which may require filing an internal report. The bank may decide to file a SAR and possibly even notify adult protective services or local law enforcement.

Fortunately, the federal government has published helpful guidance for filing a SAR. The guidance helps explain how best to alert authorities about possible EFE. In a 2011 advisory issued by FinCEN, a division of the United States Treasury, specifically states: “In order to assist law enforcement in its effort to target instances of financial exploitation of the elderly, FinCEN requests that financial institutions select the appropriate characterization of suspicious activity in the Suspicious Activity Information section of the SAR form and include the term “elder financial exploitation” in the narrative portion of all relevant SARs filed. The narrative should also include an explanation of why the institution knows, suspects, or has reason to suspect that the

activity is suspicious. It is important to note that the potential victim of elder financial exploitation should not be reported as the subject of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.”<sup>13</sup>

Just two years later in 2013, FinCEN introduced electronic SAR filing that included a specific category for elder financial exploitation, allowing financial institutions to unambiguously designate elder financial exploitation on SARs. Banks should document as much information about the suspected perpetrator as possible to support investigations.

Each state also may have additional requirements, so make sure to find out what is required in your state.

## Roles of APS and Law Enforcement

Addressing EFE requires partnerships and networking since it cannot rest solely on the shoulders of just financial institutions, adult protective services, or law enforcement; a truly collaborative approach between all parties is necessary. Luckily, the federal government generally agrees. On May 24, 2018, Congress passed the Senior Safe Act as part of section 303 of the Economic Growth, Regulatory Relief, and Consumer Protection Act. The statute includes a provision that offers a possible safe harbor for bankers who report suspected EFE to law enforcement or adult protective services, provided they have undergone appropriate training and the bank has met the other conditions in the statute.<sup>14</sup> Additionally, each state may have other, specific requirements that bankers should review before sharing information with APS or law enforcement.

Since reporting suspected fraud must be handled appropriately, bankers should work with the internal compliance officer or Bank Secrecy Act (BSA) officer to comply with all federal, state, and local requirements.

---

<sup>13</sup> <https://www.fincen.gov/sites/default/files/advisory/fin-2011-a003.pdf>

<sup>14</sup> <https://www.congress.gov/bill/115th-congress/senate-bill/2155/text#toc-id45B692A3CB-264F64BDE568E071AA2CFD>

# Adult Protective Services

## Tell me more about Adult Protective Services

APS is a social service program provided at the local level and governed by the state or county. APS workers serve seniors and adults with disabilities and investigate abuse, neglect and exploitation cases.<sup>15</sup> Many states have APS set up as part of the state department of human services or agency on aging, but the programs and authorities vary from state to state. APS agents are often dispersed strategically to investigate issues in person. Most state APS have toll-free numbers and websites through which to anonymously report abuse. However, if the customer is a resident of an assisted living or long-term care facility, APS may not have jurisdiction and you may need to involve the local long-term care ombudsman. More information is available at the National Center on Elder Abuse.<sup>16</sup>

## What principles shape APS?

APS workers always put the best interests of the adult they are assisting at the forefront of their investigation. They operate with practice guidelines established by their professional association, the National Adult Protective Services Association (NAPSA), that include honoring the wishes of the adult(s) involved, respecting their desires about confidentiality and making sure they receive information about their choices and options in a form they can understand.

## Does APS operate the same everywhere?

APS is controlled at the state level, so operations vary from state to state. Some states allow local control of APS, so operations might even differ from city to city or county to county. It is imperative that you find out what laws govern your local APS. Remember, however, that APS is a civil organization; they advocate for seniors and investigate claims. They do not have the power to file criminal charges, making it important to also partner with law enforcement.

---

<sup>15</sup> <http://www.napsa-now.org/get-help/how-aps-helps/>

<sup>16</sup> <https://ncea.acl.gov/What-We-Do/Practice/Intervention-Partners/LTC.aspx>

## What is the best way to work with APS in an ongoing investigation?

First, report the suspected activity in accordance with your own bank's internal procedures. This might mean notifying a supervisor or the bank's own fraud detection unit.

The bank might file a SAR, discussed in more detail later in this document, then contact law enforcement directly or refer the matter to APS. To be as efficient as possible, you need to know how your bank handles potential instances of suspicious activities.

The more details that are provided about what happened and why it was suspicious, the better the outcome. If there aren't enough details about what happened, an investigation might not be possible. The report should be as complete and accurate as possible and include the following information:

- the date, time and the location of the incident(s);
- who is making the report;
- a physical description of the suspected perpetrator(s);
- the amounts involved; and
- any other pertinent information.

Be sure to contact your local APS to familiarize yourself with the form and reporting requirements in your area.

## How can I find the APS closest to me?

To find the appropriate contact in your state, visit [www.napsa-now.org/help](http://www.napsa-now.org/help). You can also learn more about other social supports in your area by visiting the Elder Care Locator at [www.eldercare.acl.gov](http://www.eldercare.acl.gov).

It is important to remember that APS investigates more than just financial abuse cases. They are responsible for looking into reports of physical abuse and neglect, as well as cases involving all ages. While suspected financial abuse can have long range effects, reports of physical abuse and neglect will take precedence when resources are limited. The Appendix contains a sample introductory letter template you can personalize and use to reach out to your local APS contacts.

## How can APS handle their growing caseload?

As awareness of elder financial abuse has grown, so have reports of abuse, placing additional burdens on APS. Unfortunately, APS resources dedicated to investigating reports of financial abuse have not grown with the increased reporting. Since their heavy caseload might impact investigations, banks should provide clear and concise information when submitting a report to APS to help them understand and investigate



the issue. Also, bear in mind that APS workers are often social workers and they typically do not have a financial background or degrees in accounting or finance. So, being available to answer questions and providing further clarity as necessary will be imperative in resolving cases.

### **Do APS and law enforcement work together?**

APS and local law enforcement often work together. APS refers cases for prosecution. Local police and sheriff's departments may refer back to APS if they happen to uncover situations of abuse, neglect or exploitation. They also work together in Multidisciplinary Teams (MDTs) that are discussed later in this document. Remember that specificity is critical whenever providing information to APS and law enforcement.



**“Knowing what to expect when you work with law enforcement helps you be a better partner. Thinking ahead to provide what law enforcement might request, such as documentation or video surveillance, is important.”**

**LAUREL SYKES**

Executive Vice President, Chief Compliance and Risk Officer

American Riviera Bank, Goleta, CA

## Law Enforcement

### How can a bank best aid local law enforcement?

Timely and complete filing of SARs is a great first step. Law enforcement agencies rely on SARs when conducting investigations. At the same time, seniors may need to be willing to prosecute. Seniors might be unwilling to prosecute, though, because of familial relationships or fear of retaliation from a caregiver, particularly if that person is the abuser. The bank must be sensitive to their customer's interests. If the bank does determine a SAR is needed, it should follow FinCEN guidelines.

Bankers often raise concerns about privacy restrictions in the Gramm-Leach-Bliley Act when sharing customer information. However, there is an important exception in the statute that allows bankers to share limited non-public personal information in cases where financial fraud against seniors is suspected.<sup>17</sup>

When preparing to address and prevent EFE, banks should consider creating and maintaining a list of contacts at local APS and any law enforcement agencies with which the bank may need to interact. The list should include, but is not limited to: APS, local police and sheriff's departments, local/regional FBI and/or U.S. Secret Service field offices, local/regional United States Postal Inspection Service (USPIS), local prosecutors and the State Attorney General. If you can obtain contacts at other agencies involved at a state or federal level, then by all means, do so. Since many banks centralize SAR filing in one area of the bank, check to see if that department has a list available.

### What laws are in place that govern reporting requirements?

Bankers must be aware of laws in the specific states where the exploitation occurred, since reporting requirements vary by state. Some states require only reasonable suspicion to make a report, while others require certainty or proof of financial exploitation. Access ABA's Cumulative Elder Financial Abuse Statutes to review which laws apply to your state.<sup>18</sup>

<sup>17</sup> Eight federal agencies issued guidance to clarify this in October 2013; <https://www.occ.gov/news-issuances/news-releases/2013/nr-ia-2013-148a.pdf>

<sup>18</sup> <https://www.aba.com/advocacy/state-laws/comparative-state-laws#c3ad5e4848d44b7986ede3e3f-fa8e7bb>

## What is happening at a national level?

Federal agencies across the nation are partnering together to combat elder financial exploitation and fraud in all its forms. In 2019, the United States Department of Justice (DOJ) established the Transnational Elder Fraud Strike Force, a “joint law enforcement effort that brings together the resources and expertise of the Department of Justice’s Consumer Protection Branch, the U.S. Attorneys’ Office for six federal districts, the FBI, the U.S. Postal Inspection Service, and other organizations.”<sup>19</sup> Recognizing the threat that America’s elders face, particularly from international schemes, the strike force works with domestic and international agencies to investigate and prosecute criminals who target our nation’s elders.

The DOJ has also developed a dedicated website under their Elder Justice Initiative at <https://www.justice.gov/elderjustice>, to help combat the five primary subtypes of elder abuse: physical abuse, financial exploitation, caregiver neglect and abandonment, psychological abuse, and sexual abuse. The site includes a plethora of tools to address financial exploitation and supports both prosecutors and law enforcement. It also includes an Elder Justice Neighborhood Map to help people obtain the appropriate contacts for support throughout the 50 states.<sup>20</sup>

Similarly, the CFPB has dedicated a number of resources to protecting elders. Working with FinCEN, the bureau organized a study analyzing EFE SARs in 2016 that was updated in 2019. The report made a number of key findings, including:

- EFE SARs quadrupled between 2013 and 2017.
- Older adults experienced an average loss of \$34,200.
- Adults in their 70s incurred the greatest average loss at \$45,300.
- When the older adult knew the suspect, the average loss was \$50,200 versus an average of \$17,000 when the suspect was a stranger.<sup>21</sup>

Given the information gleaned from SARs and use by law enforcement, the CFPB issued an advisory in 2019 urging financial institutions to report suspected EFE to appropriate local, state and federal authorities and to file SARs.<sup>22</sup>

---

19 <https://www.justice.gov/opa/pr/justice-department-announces-new-transnational-elder-fraud-strike-force>

20 <https://www.justice.gov/elderjustice/support/resources-neighborhood>

21 [https://files.consumerfinance.gov/f/documents/cfpb\\_suspicious-activity-reports-elder-financial-exploitation\\_report.pdf](https://files.consumerfinance.gov/f/documents/cfpb_suspicious-activity-reports-elder-financial-exploitation_report.pdf)

22 <https://www.consumerfinance.gov/about-us/newsroom/bureau-recommends-financial-institutions-report-suspected-financial-exploitation-older-adults/>

**“People are more inclined to report with increased awareness.”**

**ELAINE DODD**

Executive Vice President

Oklahoma Bankers Association, Oklahoma City, OK

## Reporting

### How do I report suspected elder financial exploitation?

Banks typically report suspected EFE through filing a SAR with FinCEN. SARs help identify and stop suspected money laundering, financial crimes and terrorist financing.

Since 2013, FinCEN’s electronic filing SAR form has included a specific checkbox to designate “elder financial exploitation” as a category of suspicious activity. There’s more to the form than that though, and the narrative portion of the SAR remains critical in providing details necessary for a thorough investigation. The more detailed information that can be provided, the better law enforcement can investigate the possible criminal activity.

In many areas of the US, law enforcement agencies will convene to review SARs that apply to that area and review them for appropriate assignment and action. There may be a SAR review team in your area that evaluates cases of possible elder financial exploitation.

### What is the time frame to file a SAR?

Bankers are required to file a SAR within 30 days of the time the bank determines something suspicious has occurred. The time for reporting doesn’t necessarily start when the transaction occurs since the bank is allowed to conduct an additional investigation to determine if something was truly suspicious or whether someone was trying to hide something to prevent the bank from reporting.

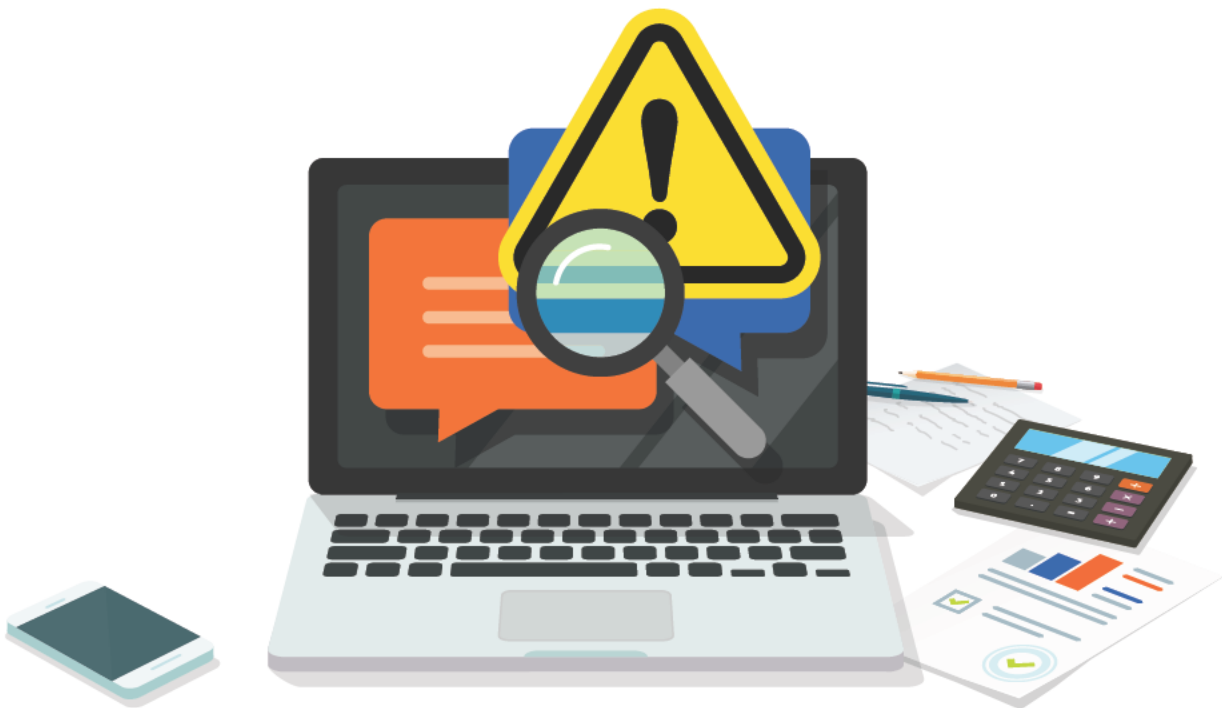
When the bank can’t identify the person suspected of perpetrating the fraud, it is allowed up to 60 days to file a report. However, the sooner a report is filed, the better the chance of recovery.

## Are there specific thresholds that dictate when to file a SAR?

There are three financial amounts to bear in mind when filing mandatory SARs. According to guidance from the federal banking agencies, banks are required to file a SAR in the following situations:

- Criminal violations involving insider abuse of any amount
- Criminal violations aggregating \$5,000 or more when a suspect can be identified
- Criminal violations aggregating \$25,000 or more regardless of potential suspect <sup>23</sup>

However, banks may file SARs voluntarily even if a transaction does not meet the aforementioned monetary thresholds.



<sup>23</sup> <https://www.fincen.gov/sites/default/files/shared/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf>

# HOW YOU FILE

## A SAR (SUSPICIOUS ACTIVITY REPORT)

Filing a SAR is done solely through FinCEN's BSA e-filing system. You should follow your bank's process for reporting suspicious activity.



### 1 The Subject

The information about the subject including all names, addresses, social security or tax IDs, birth dates, driver's license numbers, passport numbers, occupation and phone numbers of all parties involved with the activity.

### 2 The Date Range

When the activity occurred and whether it was a single transaction or a series of transactions that took place over time. In some cases a bank might need to file more than one SAR.

### 3 Information about the Financial Institution

The information about the financial institution where the activity occurred – main office, specific branch location(s).

### 4 The Contact Information

The contact information of the filing institution, usually the compliance officer.

### 5 The Narrative

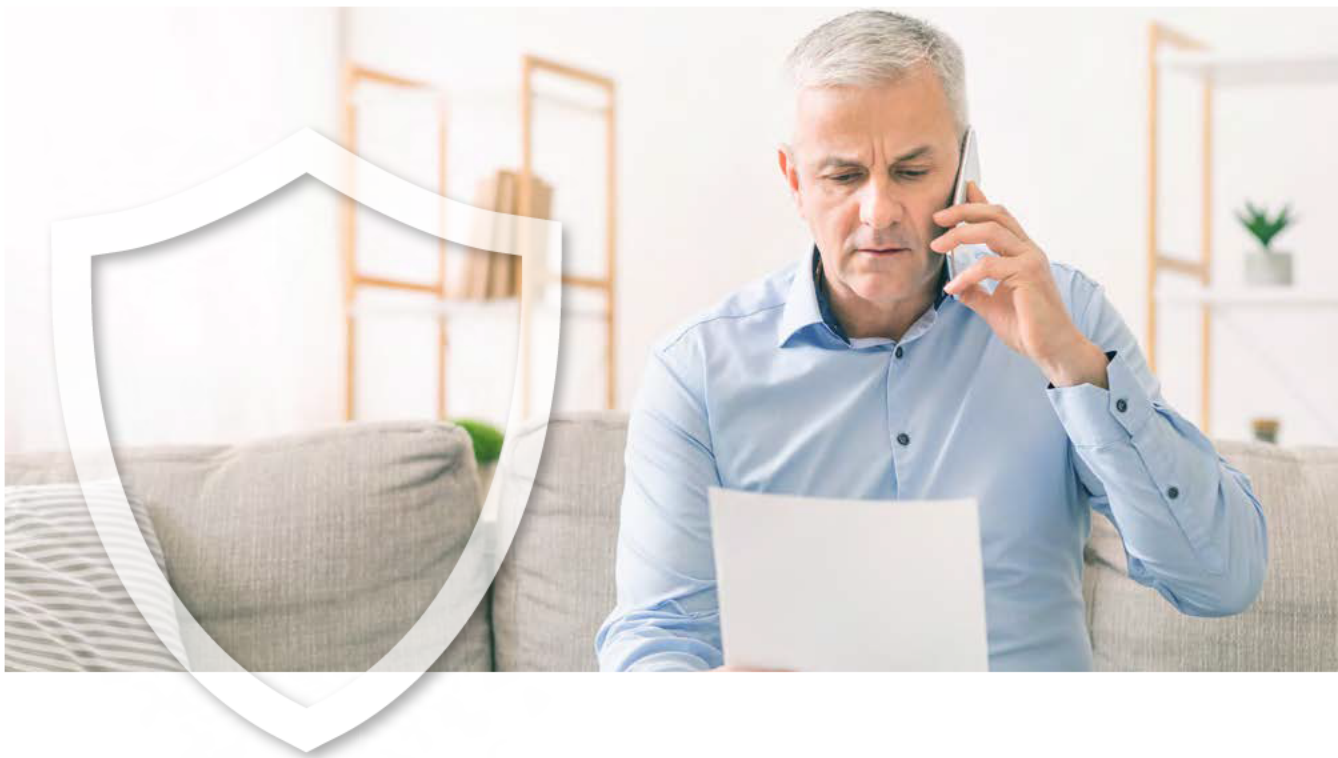
The narrative about the situation – what happened that caused the need for the report. Specificity is so important in this section. Be clear, concise and provide as many pertinent details as possible.

## Are banks required to file with APS if we are already filing a SAR?

Depending on state law, your bank also might be required to report to APS. It is critical to know your state's requirements for reporting to APS when you suspect abuse, neglect or exploitation. Some states only require certain professionals to report their suspicions. Other states require all citizens to report. More and more, banks are reporting all instances to APS regardless of the mandatory requirement.

At the same time, it is important to understand that it may be a violation of federal law to disclose to APS that a SAR has been filed. If APS is not a law enforcement agency under state law – and in most cases APS is not – sharing even the existence of a SAR with APS would violate federal law, although you can share the same information that was covered by the SAR. You should discuss this with the office in your bank responsible for filing a SAR to see if there's a separate report for APS and to make sure you don't inadvertently violate the law.

Even if it isn't required, if it is allowed by your state, sharing information quickly with APS and law enforcement upon the filing of a SAR can lead to quicker resolution and prevent the loss of large amounts of money. Your bank will already have procedures in place based on the existing requirements, so following your bank's reporting procedures is the best approach.



# HOW YOU FILE A REPORT WITH OUR LOCAL APS (ADULT PROTECTIVE SERVICES)

Below are the steps that occur when a report is filled with APS. Be sure to validate with your local APS as these may vary slightly state to state.



## 1 Report

Filed via telephone, website or in person.



## 2 Details

Details provided in the report will be screened by a trained professional to evaluate if it meets the statutory requirements for APS services in the state and/or municipality receiving the report.



## 3 Criteria

If the situation meets criteria for abuse, neglect or exploitation, an APS worker will initiate face-to-face contact with the adult needing assistance.



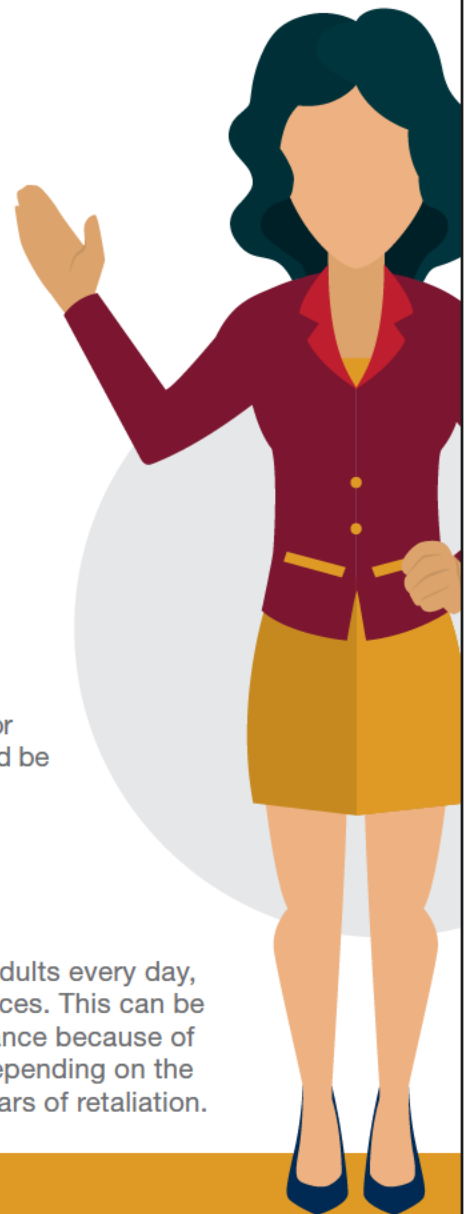
## 4 APS worker

The APS worker will assess the adult's safety, need for assistance, and determine what services, if any, would be beneficial to maintain his/her well-being and independence.



## 5 Right to Refuse Assistance

While APS workers help thousands of vulnerable adults every day, individuals generally have the right to decline services. This can be especially problematic when seniors refuse assistance because of fear. Reports can potentially remain anonymous depending on the state regulations which may help alleviate some fears of retaliation.





## What happens after a banker files a report with APS?

According to NAPSA, once a report is filed, whether in-person, on the website or by telephone:

1. The details provided in the report will be screened by a trained professional to evaluate if it meets the statutory requirements for APS services in the state and/or municipality receiving the report.
2. If the situation meets the criteria for abuse, neglect or exploitation, an APS worker will initiate face-to-face contact with the adult needing assistance.
3. The APS worker will assess the adult's safety, need for assistance, and determine what services, if any, would be beneficial to maintain his/her well-being and independence.
4. While APS workers help thousands of vulnerable adults every day, individuals generally have the right to decline services. This can be especially problematic when seniors refuse assistance due to fear. Reports can potentially remain anonymous depending on state regulations, which may help alleviate some of the fear of retaliation.

## How can we provide information without violating our customers' privacy?

Since the advent of Gramm-Leach-Bliley Act (GLBA), many bankers are not comfortable sharing customer information with law enforcement for fear of breaking the legislation's privacy provisions. In 2013, eight federal regulatory agencies (Federal Reserve, CFTC, CFPB, FDIC, FTC, NCUA, OCC & SEC) issued interagency guidance that reporting suspected elder financial abuse did not, in fact, violate the privacy provisions included in Gramm-Leach-Bliley.

Specifically, the GLBA states that, "A financial institution may disclose nonpublic personal information to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability." This exception generally allows a financial institution to disclose nonpublic personal information to appropriate authorities in order to:

- report incidents that result in taking an older adult's funds without actual consent, or
- report incidents of obtaining an older adult's consent to sign over assets through misrepresentation of the intent of the transaction.

Additionally, as previously mentioned, the Senior Safe Act adopted in May 2018 offers a possible safe harbor for bankers who report suspected elder financial exploitation of individuals ages 65 and above to law enforcement or adult protective services, when they have undergone appropriate training and met the other conditions of the statute.<sup>24</sup> The training must include:

- common signs of possible EFE,
- how to identify and report suspected EFE,
- how to report suspected exploitation to government officials or law enforcement as appropriate
- the need to protect the privacy and respect of each individual; and
- must be appropriate to the person’s individual job responsibilities.

For more information, check out ABA’s overview on the statute, which can be accessed at [www.aba.com/elderfinance](http://www.aba.com/elderfinance).

## How to Partner with APS and Law Enforcement

Strong working relationships between bankers, APS and law enforcement is helpful to effectively thwart financial abuse and prosecuting fraudsters. APS and law enforcement officials need to know that banks are willing to collaborate and combat financial exploitation.

### How do we begin?

Relationships take time to build, so start early. It’s best to begin cultivating partnerships even before a case arises so you’ll know exactly who to turn to when an issue presents itself. But, the first step will require your initiative—reach out. Check out the resources in the Appendix, which include templates that you can adapt to facilitate introductions with APS and law enforcement.

### Do elder fraud prevention networks exist?

Absolutely! Strong partnerships between banks, law enforcement agencies, senior service agencies and non-profits to protect elders and combat financial exploitation exist nationwide. They often focus on case review, community outreach and developing policy to protect older Americans. Some common examples include:

---

<sup>24</sup> <https://www.congress.gov/bill/115th-congress/senate-bill/2155/text#toc-id45B692A3CB-264F64BDE568E071AA2CFD>

- **Multidisciplinary Teams (MDT).** These are teams that meet frequently to review cases of abuse, neglect and self-neglect to determine how to appropriately address them. They typically include APS, aging services network personnel, law enforcement, prosecutors as well as victim service providers.<sup>25</sup> MDTs most often focus on elders, but may also concentrate on other populations, such as adults with disabilities. The best way to connect with an MDT is to first reach out to your local APS contact. You can determine the appropriate contact by visiting: [www.napsa-now.org/get-help/help-in-your-area/](http://www.napsa-now.org/get-help/help-in-your-area/).
  - **Financial Abuse Specialist Teams (FAST).** These are a subset of MDTs which focus on complicated financial exploitation cases. They are usually made up of public-private partnerships, which may include APS, law enforcement, lawyers, long-term care ombudsmen, bankers, real estate professionals and other volunteers.
  - **Elder Abuse Forensic Centers.** These are specialized MDTs which coordinate efforts between health care, social service, and criminal justice professionals “to review cases of abuse, assess and evaluate victims’ cognitive capacity, improve the prospects of prosecution, develop appropriate responses, and support prevention of elder abuse through awareness campaigns and professional education.”<sup>26</sup>
- **Triads.** These are designed to “promote older adult safety and to reduce the fear of crime that older adults often experience.”<sup>27</sup> They consist of a three-pronged partnership between older adults, communities, and law enforcement. Triads are organized by SALT (Seniors and Law Enforcement Together) Councils. These networks focus on crime prevention education, training volunteers, identifying community referrals for support to address fear, and uniting communities to collaboratively address community problems. Banks are welcome to join. To locate a triad in your area, visit: [www.sheriffs.org/programs/national-triad](http://www.sheriffs.org/programs/national-triad).

Bankers can and should be a part of these networks since they help you expand your network of contacts, learn from others as they simultaneously learn from you, support your bank’s reputation, and ultimately help improve your community.

25 <https://www.justice.gov/file/1284316/download>

26 [https://files.consumerfinance.gov/f/documents/bcftp\\_fighting-elder-financial-exploitation\\_community-networks\\_report.pdf](https://files.consumerfinance.gov/f/documents/bcftp_fighting-elder-financial-exploitation_community-networks_report.pdf)

27 <https://www.sheriffs.org/programs/national-triad>

## What can I do if an elder fraud prevention network does not exist in my area?

If there isn't a local network, banks can invite the appropriate local entities (law enforcement and social service/non-profit agencies) to create one. It is in the best interest of the bank to have an active network in all local areas where they have branches. The more active networks there are, the greater the chance for education and training, leading to further awareness. The CFPB has developed a number of resources to support elder fraud prevention and response networks, which can be accessed at [www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/elder-protection-networks/](http://www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/elder-protection-networks/).

## What are the key things to remember about dealing with elder financial exploitation?

- Key words to keep in mind are awareness, communication, cooperation, education, reporting and training.
- Be aware of anomalies with your older customers' accounts. Know who to reach out to when you find something suspicious. Make sure to maintain detailed records of what you found, who you talked to, when you talked to them and when the SAR and/or APS report was filed.
- Talk about potential fraud with your older customers. Let them know that it is a very real possibility that someone may attempt to perpetrate a fraud against them. Help destigmatize the situation. Educate them and your employees whenever the opportunity arises.
- Partner with agencies dealing with seniors and with senior living facilities to offer seminars and take-home information on the topic.
- Remember that you CAN share non-public personal information with law enforcement when you are trying to help prevent or prosecute a case of elder financial exploitation.

## Case Study: Bank of the Rockies

Bank of the Rockies, a community in White Sulphur Spring, Mont., began noticing an increasing trend of scams targeting elders in their footprint back in 2016. When bank tellers noted their customers were trying to wire uncharacteristic amounts of money abroad to so-called romantic interests, they realized they needed to do something quickly to combat the threat. After having an internal discussion about the need to address the growing issue, a staff member volunteered to serve as an elder champion. Jennell Huff, the bank's outreach coordinator, created an educational program, CONversations About Cons. Drawing on ABA Foundation's [Safe Banking for Seniors](#) materials, the program consists of a series of facilitated roundtable discussions with both customers and non-customers alike about cybersecurity awareness, common scams (imposter scams, lottery and sweepstakes scams, counterfeit/forged checks, and other related topics), detecting EFE, and how to respond when people suspect abuse.

The program became a focal point for connecting with their local community. Through the CONversations About Cons program, Bank of the Rockies began reaching out to experts in the field. They connected with local resources by searching the web, making calls and sending emails to bring in speakers from APS, the police department, and representatives from the state's Attorney's General Office to participate in the discussions.

But the bank also recognized that while their efforts to inform elders and other community members about EFE is important, actively engaging in a broader network is a vital step in protecting their vulnerable customers. After reviewing a CFPB report on [Fighting Elder Financial Exploitation through Community Networks](#), Mike Grove, the bank's president, encouraged Jennell to get involved.

Unfortunately, however, a network wasn't available in the area. This, however, did not hinder the bank's efforts to cultivate partnerships. Jennell and her colleagues considered their various professional relationships and recognized that they had a connection to the Montana Financial Education Coalition, a Montana Jump\$tart affiliate, which included professionals from several different disciplines. So, Jennell reached out and pitched the idea of creating an elder fraud prevention network to the group. Soon after, the Montana Elder Fraud And Exploitation Prevention Network was born.

The network comprises AARP, APS workers, bankers, credit unions, lawyers, local government officials, notaries, the Montana Bankers Association, the Montana Board of Crime Control, and senior citizens. With a shared understanding that a cooperative community response is necessary to protect elders, they work together to combat EFE. The network hosts joint community education and outreach efforts and also engages in professional cross-training. They meet at least once quarterly, but usually more frequently to regularly discuss suspected issues of abuse, collaborate, and lead educational sessions with Montana residents.

Beyond finding support for specific cases and educating community members, the network has also been helpful in ensuring a unified and powerful voice in the state.

They have been able to bring important players to the table to highlight elder concerns. Additionally, while their intent is not political, having the proper network connections ensured that the correct agencies were connected to discuss and provide a unified front in support of legislation, such as expanding the Bank Act in Montana via the Financial Institutions – Preventing Financial Exploitation addition, to safeguard seniors, which passed in 2019.

Given their positive experiences, Bank of the Rockies continues to actively participate in the elder fraud prevention network and encourages other banks to similarly engage. As Jennell states, “the first step is to make the ask.” Determine if there are established partnerships with elder justice coordinators and get involved. If one doesn’t exist, consider convening APS, law enforcement, private citizens, government officials, businesses, areas agencies on aging and others to get started. Protecting elders requires a community effort and partnering with others will only further your bank’s efforts.



# Appendix

## Top Scams

### 1. Medicare / Health Insurance Scam

Every U.S. citizen over the age of 65 automatically qualifies for Medicare, so scammers do not have to research which health insurance provider they are using. The scam artists pose as Medicare representatives and try to get seniors' personal information. They may offer services that the senior doesn't need via the telephone or a "mobile unit" then try to bill Medicare for these fake or unnecessary tests/medications/etc. Seniors may get in trouble with Medicare or even be out money for "co-pays."

### 2. Counterfeit Prescription Drugs

Mostly online scams, the FDA investigates upwards of 20 counterfeit prescription drug scams per year, up from five annually in the 1990s. Not only are seniors losing money on fraudulent prescriptions, they may also harm themselves by taking unsafe substances rather than their real medication. Cheaper is not always better.

### 3. Funeral and Cemetery Scams

Scammers scour the obituaries or funeral home websites and reach out to survivors right before, during or right after the funeral to inform the bereaved family that the deceased owes a debt that was overdue at his/her death and needs to be repaid post haste to prevent besmirching the deceased's reputation. The scammer plays on the grief of the bereaved family while seemingly being sympathetic. Another situation that can happen is that disreputable funeral homes will take advantage of grieving families who are unfamiliar with the details around funeral costs, adding on unnecessary or fraudulent extras to the bill. They play on the grief of the bereaved family by reassuring them that they want the absolute best for their loved one, including a very expensive casket for a cremation when only a cardboard box is required.

### 4. Fraudulent Anti-aging Products

In a society that stigmatizes aging, it is easy to understand why people may fall for scams that offer them the fountain of youth. Many older Americans seek out new treatments and medications to maintain a youthful appearance, putting them on scammers' radars. Whether it's the ever popular fake Botox or fraudulent "homeopathic" remedies that do absolutely nothing, there is big

money in the anti-aging business. Botox scams are particularly unsettling, because renegade labs creating versions of the real thing may still be working with the root ingredient, botulism neurotoxin, which is one of the most toxic substances known to science. A bad batch can have serious health consequences. As a result, the consumer may also have to incur unexpected medical expenses to address any adverse effects in addition to paying for the fake Botox.

## **5. Telemarketing / Phone Scams**

Since many seniors are happy to talk to anyone willing to talk to them, phone scams are highly prevalent. Seniors also are more likely to purchase items over the telephone versus the internet, As a result, there is no paper trail, making these transactions almost impossible to trace. Also, once a scammer is successful with a telemarketing scam, s/he may “share the wealth” by spreading the susceptible senior’s information. There are several types of telemarketing scams including:

- The pigeon drop – scammer tells the senior they found a large sum of money that they are willing to split if the senior will provide a “good faith” payment by withdrawing money from their bank account. Often, there is a second con artist involved who portrays a “trustworthy” participant, such as a lawyer or officer.
- Fake accident – the scammer convinces the senior that a relative or close friend has been in an accident and needs the money for treatment.
- Fake charities – scammers will call seniors soliciting donations for fake charities. Names will be similar to well-known charities to create the belief that they are legitimate. These scams are particularly popular after natural disasters.

## **6. Internet Scams**

Seniors fall victim to clicking on pop-up windows offering updated virus protection that look legitimate. In reality, they are scams that will either require a large sum to “purchase” or that upload an actual virus to the computer that grants the scammer access to personal information. The scammer may even install ransomware and demand a payment to let the senior regain control of their information. Email phishing scams are also popular. Someone pretends to be from their bank, the IRS or some other official entity that needs to verify the personal information of the senior. Seniors may also fall victim to a “Work From Home” money claim from an Internet ad or email. The offer may involve the senior needing to pay for “training” or special “equipment” in order to begin making the money.



## **7. Investment Schemes**

When they retire, seniors are often looking for ways to maximize their savings while minimizing risks. Pyramid schemes, such as investment opportunities offered by a fabled Nigerian prince, are simply too good to be true. They are designed to take advantage of people and steal their financial resources. No legitimate investment will require up front money to reap astronomical returns within unrealistic timeframes.

## **8. Homeowners / Reverse Mortgage Scams**

This encompasses two distinct scams. The first involves a con artist who poses as a tax official offering to reassess the senior's property for tax purposes. The scam is predicated on the notion that the senior's tax debt could be lowered. The con artist charges a fee for this "reassessment," which is fraudulent. The second revolves around pressuring seniors to obtain a reverse mortgage to access the equity in their home. Typically, scammers are lurking to perform "necessary home repairs" to take advantage of the windfall of cash the senior receives from the reverse mortgage. Since real estate generally encompasses a large portion of a senior's wealth, obtaining a reverse mortgage may effectively become the tool to deplete their largest asset.

## **9. Sweepstakes and Lottery Scams**

While not limited to seniors, these scams use the lure of free money to convince consumers to divulge sensitive information or send funds to a con artist. Seniors receive a communication via email, mail, phone call or sometimes even in person. They have won a prize from some contest they don't even remember entering. Before they can get the entire amount, they have to deposit a partial amount to "verify" their bank account information. They are then asked to repay that amount to the scammer before the fraudulent check has been returned. By the time the check is returned as a fraud, the scammer is long gone with money they got from the senior.

## **10. Impostor Scams**

This one seems particularly egregious because it can pull on the heartstrings of the senior involved depending on the persona adopted by the scammer. The scammer may call and pretend to be an IRS agent or from another official entity, such as the local utility company or even their bank. The scammer will then claim that the senior owes money that must be repaid immediately or charges will be filed. Alternatively, the scammer may try a more personal approach by self-identifying as the senior's favorite grandchild/niece/nephew/etc., in need of money. It may just be a "loan," to address an urgent situation like a car repair, late rent, school tuition, or something along those lines. The scammer implores

the senior not to tell mom or dad and states that s/he will pay the senior back. The scammer will then provide a Western Union or MoneyGram location to pick up the money.

### 11. Check Fraud

There are several variations of check fraud. The senior may write a check to someone, and that person alters the amount or orders checks with a new address to write fraudulent checks. Blank checks could be stolen and forged for any amount, or scammers could ask the senior for help “clearing” a check because s/he does not have a local bank account but needs the money quickly. The senior deposits the fraudulent check and writes one to the scammer. By the time the check is returned, the scammer and the money are long gone. The scammer may also write checks of larger and larger amounts with the senior until they get the amount they want, and then disappear.

## Resources for Creating Partnerships

- National Association of Triads (NATI) Triad Program Manual - [www.sheriffs.org/videos/2018\\_NATI\\_Manual.pdf](http://www.sheriffs.org/videos/2018_NATI_Manual.pdf)
- Department of Justice Guide on Developing an Elder Abuse Care Review Multidisciplinary Team in Your Community – [www.justice.gov/elderjustice/file/938921/download](http://www.justice.gov/elderjustice/file/938921/download)
- CFPB resources to build an elder fraud prevention and response network - [www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/elder-protection-networks/](http://www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/elder-protection-networks/)
- CFPB Memorandum on Financial Institution and Law Enforcement Efforts to Combat Elder Financial Exploitation - [https://files.consumerfinance.gov/f/documents/201708\\_cfpb-treasury-fincen\\_memo\\_elder-financial-exploitation.pdf](https://files.consumerfinance.gov/f/documents/201708_cfpb-treasury-fincen_memo_elder-financial-exploitation.pdf)

# Additional Resources for Combating Elder Financial Exploitation

- ABA Elder Financial Exploitation Prevention Resource Webpage – [www.aba.com/elderfinance](http://www.aba.com/elderfinance)
- ABA Foundation Toolbox on Protecting the Financial Security of Older Americans – [www.aba.com/seniors](http://www.aba.com/seniors)
  - Resource #1 – Starting a Senior Financial Education Program at Your Bank
  - Resource #2 – Planning Senior Financial Education Program Events
  - Resource #3 – Communicating Your Senior Financial Education Program
- Advisory for Financial Institutions on Preventing and Responding to Elder Financial Exploitation – [www.consumerfinance.gov](http://www.consumerfinance.gov)
- Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults – [files.consumerfinance.gov/f/201309\\_cfpb\\_elder-abuse-guidance.pdf](http://files.consumerfinance.gov/f/201309_cfpb_elder-abuse-guidance.pdf)
- FinCEN Suspicious Activity Report, supra; FinCEN Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative 13-21 – <https://www.fincen.gov/resources/statutes-regulations/guidance/sar-narrative-guidance-package>
- Money Smart for Older Adults – [www.consumerfinance.gov](http://www.consumerfinance.gov) or [www.fdic.gov](http://www.fdic.gov)
- BankSafe Initiative: A Comprehensive Approach to Better Serving and Protecting Consumers – [www.aarp.org](http://www.aarp.org)
- Final CFPB + Treasury + FinCEN Memo on Elder Financial Exploitation for ASA – [www.consumerfinance.gov](http://www.consumerfinance.gov)
- National Adult Protective Services Association – [www.napsa-now.org](http://www.napsa-now.org)
- FinCEN Advisory - FIN-2011-A003 – [www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a003](http://www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a003)
- ABA table containing state statutes on elder abuse – <https://www.aba.com/advocacy/state-laws/comparative-state-laws#c3ad5e4848d44b7986ede3e3ffa8e7bb>
- BSA Joint Memo on working with law enforcement by FinCEN, CFPB and Department of Treasury [www.fincen.gov/sites/default/files/2017-08/8-25-2017\\_FINAL\\_CFPB%2BTreasury%2BFinCEN%20Joint%20Memo.pdf](http://www.fincen.gov/sites/default/files/2017-08/8-25-2017_FINAL_CFPB%2BTreasury%2BFinCEN%20Joint%20Memo.pdf)

- Where to file with agencies based on type of case
  - Elder fraud complaints may be filed with the FTC – [www.ftccomplaintassistant.gov](http://www.ftccomplaintassistant.gov) or at 877-FTC-HELP
  - The Department of Justice provides a variety of resources relating to elder fraud victimization through its Office of Victims of Crime – [www.ovc.gov](http://www.ovc.gov)
  - Cybercrimes should be reported by banks to the FBI – [www.ic3.gov/default.aspx](http://www.ic3.gov/default.aspx)
  - Scams originating by mail should be reported to USPS at (877) 876-2455 or <https://www.uspis.gov/report>
  - Money Gram and Western Union related cases – [www.moneypak.com/security](http://www.moneypak.com/security)
- Elder fraud DOJ Fact Sheet on sweeps – [www.justice.gov/opa/press-release/file/1037946/download](http://www.justice.gov/opa/press-release/file/1037946/download)
- Interactive map on elder fraud sweeps – [www.justice.gov/opa/february-22-2018-elder-fraud-sweep/map](http://www.justice.gov/opa/february-22-2018-elder-fraud-sweep/map)

# Introductory Letter to Law Enforcement

[Date]  
[Name of Addressee]  
[Law Enforcement Agency Name]  
[Mailing Address]  
[City, ST zip code]

**RE: Elder Financial Abuse**

Dear [Courtesy Title and Last Name]:

Thank you for all your work in the elder financial exploitation arena over the last few [months, years]. I wanted to take this opportunity to introduce myself. I am the [insert position] at the [Bank/Branch] location.

As I'm sure you know, elder financial abuse is one of the fastest growing crimes in our area, and prevention is the best defense. I have been charged with putting together a series of programs for our [senior banking program] at the [neighborhood community center]. My plan is to offer a lunch-and-learn type of program on a monthly basis.

Are you available to meet and discuss topics? The input of someone on the front lines of law enforcement efforts on this topic will be invaluable to my bank's programs. I can make myself available [anytime next Tuesday or Wednesday afternoon]. If neither of those work, let me know what might. I really want to get these programs going within the next month, if possible.

Thank you, in advance, for your assistance with this project.

Sincerely,

[Your Name]  
[Title]  
[Email]  
[Phone number]

# Introductory Letter to Adult Protective Services

[Date]  
[Name of Addressee]  
Adult Protective Services  
[Mailing Address]  
[City, ST zip code]

Dear [Courtesy Title and Last Name]:

I am the [job title] at [bank/ branch] and I wanted to introduce myself. I focus on [brief information about role].

At [bank], we take the safety and wellbeing of all our customers seriously. Through my role, I am taking a particular interest in safeguarding older adults in our community. As I'm sure you know, elder financial exploitation is a complex crime, and I would like to learn more about community experts and ways we can work together to combat this egregious threat.

If you have some time to chat, I would appreciate the opportunity to connect. I am fairly open [next Thursday afternoon], are you available then? As I begin to update our elder financial exploitation prevention seminar, your input would be invaluable.

Thank you, in advance, for your assistance with this project.

Sincerely,

[Your Name]  
[Title]  
[Email]  
[Phone number]

# Introductory Letter #2 to Adult Protective Services

[Date]  
[Name of Addressee]  
Adult Protective Services  
[Mailing Address]  
[City, ST zip code]

**RE: Pending Cases [insert case numbers]**

Dear [Courtesy Title and Last Name]:

[Previous colleague] gave me your contact information as our go-to person at APS. I wanted to introduce myself. I am the new [job title] at [bank/ branch]. [Previous colleague] suggested I follow up with you on the above mentioned cases.

Since I am taking over [his/her] responsibilities, I wanted to make sure I was up to speed. I have introduced myself to the customers involved. Do you have a current status?

I would also like to stop by and introduce myself in person. I am fairly open [next Thursday afternoon], are you available then? As I begin to update our elder financial exploitation prevention seminar, your input would be invaluable.

Thank you, in advance, for your assistance with this project.

Sincerely,

[Your Name]  
[Title]  
[Email]  
[Phone number]

# Introductory Letter to Local Non-Profit Focused on Seniors

[Date]  
[Name of Addressee]  
[Local Non-Profit focused on Seniors]  
[Mailing Address]  
[City, ST zip code]

**RE: Elder Financial Exploitation**

Dear [Courtesy Title and Last Name]:

My boss told me that your organization has partnered with us on elder financial abuse prevention seminars. I wanted to take this opportunity to introduce myself. I am the [title/position] at the [Bank/Branch] location.

As I'm sure you know, elder financial abuse is one of the fastest growing crimes in our area, and prevention is the best defense. I currently run my bank's [senior banking program]. I've been asked to provide an evaluation and plan for the next fiscal year.

Are you available to meet and share your thoughts about our current programs? Your input, given your experience, will be invaluable. I can make myself available [anytime next Tuesday or Wednesday afternoon]. If neither of those work, let me know what might.

Thank you, in advance, for your assistance with this project.

Sincerely,

[Your Name]  
[Title]  
[Email]  
[Phone number]



# Introductory Letter to Senior Living Facility

[Date]  
[Name of Addressee]  
[Senior Living Facility]  
[Mailing Address]  
[City, ST zip code]

**RE: Elder Financial Exploitation**

Dear [Courtesy Title and Last Name]:

I am the [title] at the [Bank/Branch] location. [Customer Name], one of your residents is also one of our customers. [S/he] suggested I reach out to you about scheduling an Elder Financial Exploitation prevention seminar for your residents.

We have recently seen an uptick in elder financial exploitation among our senior customers. As I'm sure you know, prevention is the best way to stem the tide. I hope to get the word out to as many of our seniors as possible. At the bank, we plan to alert customers with an additional note to accompany their mailed statements. I have a presentation with handouts that takes about 45 minutes. Is it possible to plan this as an activity for your residents?

Are you be available to meet with me to discuss this further? I can make myself available anytime [next Tuesday or Wednesday afternoon]. If neither of those work, let me know what might.

Thank you, in advance, for your assistance in helping us safeguard our community.

Sincerely,

[Your Name]  
[Title]  
[Email]  
[Phone number]

# Acknowledgements

The ABA Foundation would like to especially thank the following individuals for sharing their time and expertise in developing this guide:

## **Angela Deleon**

*Master's Program Coordinator*

Peoples United Bank

## **Ed Hutchison**

*Director, Triad, Traffic, and Officer Safety*

National Sheriffs' Association

## **Elaine Dodd**

*EVP Fraud Division*

Oklahoma Bankers Association

## **Hector Ortiz**

*Senior Policy Analyst*

Consumer Financial Protection Bureau

## **Jenefer Duane**

*Senior Program Analyst for the Office for Older Americans*

Consumer Financial Protection Bureau

## **Jennell Huff**

*Relationship Manager/Outreach Coordinator*

Bank of the Rockies

## **Joe Snyder**

*Director*

Philadelphia Corporation for Aging

## **Kathleen Quinn**

*Senior Advisor*

National Adult Protective Services Association

## **Laurel Sykes**

*EVP, Chief Compliance and Risk Officer*

American Riviera Bank

## **Luis Lobo**

*EVP, Multicultural Banking Manager*

Truist Bank

## **Nan Gibson**

*Office of Nonprofit Engagement*

JPMorgan Chase

## **Regina R. Forest**

*Director, Global Financial Crimes Compliance Executive*

Bank of America

## **Stacy Canan**

*Attorney and Consultant*

In addition, we would like to thank **Bank of America, Citi, JPMorgan Chase, Truist Bank** and **Wells Fargo** for their continued support of our work and the Protecting Seniors: A Bank Resource Guide for Partnering with Law Enforcement and Adult Protective Services.





**SAFE BANKING  
FOR SENIORS**®

*ABA FOUNDATION*