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.

Developed in collaboration with OrgWide Services, LLC
Orgwide.com | (901) 850-8190

Table of Contents

Introduction **5**

The State of Elder Financial Exploitation Today **6**

How big is the problem? 6
Who is an elderly customer? 6
Why is elder financial exploitation growing so fast? 6
Why are banks so pivotal in helping to combat elder financial fraud? 7
What are the ramifications for our elder customers affects by fraud? 8

Top Scams Currently in Play **8**

What are today's most prevalent forms of scams? 8

What can be done? **10**

Note changes in customer activity 10
How do we proceed when we notice something? 10

The Roles of APS and Law Enforcement **11**

Tell me more about Adult Protective Services (APS) 11
What principles shape APS? 11
Does APS operate the same everywhere? 11
What is the best way to work with APS in an ongoing investigation? 12
How can I find the APS closest to me? 12
How can APS handle their growing caseload? 12
Do APS and law enforcement work together? 12
How can a bank best aid local law enforcement? 13
What laws are in place that govern reporting requirements? 14
What is happening at a national level? 14

Table of Contents (continued)

Reporting **15**

How do I report suspected elder financial fraud? 15

What is the time frame to file a SAR? 15

How do you file a SAR? 17

Are banks required to file with APS if we are already filing a SAR? 17

What steps are typically involved once a banker files a report with APS? ... 19

How can we provide information without violating our customers' privacy? . 19

How to Partner with APS and Law Enforcement **20**

How can we best leverage the work being done by others? 20

Tell me more about partnerships that are working together to combat elder financial fraud 20

Are bankers allowed to join? 21

How do bankers benefit by participating in these partnerships? 21

How do we develop a local network? 22

What are the key things to remember about dealing with elder financial fraud? 22

Key Takeaway Questions **23**

Appendix **24**

Top 11 Scams 24

Resources for Creating Partnerships 27

Additional Resources for Combating Elder Financial Exploitation 27

Introduction Letter to Law Enforcement 29

Introduction Letter to Adult Protective Services 30

Introduction Letter to Local Non-Profit Focused on Seniors 31

Introduction Letter to Senior Living Facility 32

Introduction

Financial abuse of seniors is a devastating crime that banks are uniquely positioned to help address and prevent. Financial abuse against seniors refers to the "theft or embezzlement of money or any other property from an elder. It can be as simple as taking money from a wallet or as complex as manipulating a victim into turning over property to an abuser."[1] Abuse may also involve the improper use of senior funds, identity, property or assets.

Socially isolated seniors and those with cognitive impairments are particularly vulnerable to abuse. Additionally, many seniors are more financially secure relative to younger populations as they tend to own their own homes, have accrued savings over their lifetimes, typically have good credit and are generally more trusting of others.[2] Unfortunately, fraudsters and scammers are well aware of these characteristics and specifically target seniors to exploit their financial resources.

Only one in 44 financial elder abuse cases are ever reported.[3] However, banks can play a critical role in improving the statistic. Seventy percent of all deposits are made by customers aged 50 and older.[4] Bankers see their older customers in branches more than any other age group, and seniors often perceive bankers as trusted advisors. Consequently, bankers are in the best position to spot irregularities quickly.

ABA's *2017 Older Americans Benchmarking Report* indicates that in two-thirds of cases where banks suspected elder abuse or fraud, the banks turned to local law enforcement or Adult Protective Services (APS) for assistance.[5] Partnerships with law enforcement and APS can provide resources to educate bankers and their customers about elder abuse. Furthermore, strong partnerships can help prevent devastating financial losses for elderly customers.

This document was designed as a resource guide to support banks in developing relationships with APS and law enforcement officials to proactively combat elder financial abuse and exploitation.

This guide contains information on:

- the state of elder financial exploitation today;
- the role of APS and law enforcement;
- reporting; and
- how to create partnerships with key players, including customizable letters to reach out to law enforcement agencies, APS and non-profit organizations.

In developing this guide, ABA Foundation and OrgWide Services consulted with government agencies, law enforcement agencies, banks of all sizes, as well as banking associations.

1 http://www.fsroundtable.org/wp-content/uploads/2014/06/Webster-Blog-on-Elder-Abuse-The-Golden-Years.pdf
2 https://www.giaging.org/issues/financial-exploitation/
3 http://www.napsa-now.org/policy-advocacy/exploitation/
4 https://www.aba.com/Engagement/Documents/2017-Older-Americans-Benchmark-Report.pdf
5 ibid.

> **"No matter how big or small your bank is, we all need to be aware elder financial exploitation can and does happen."**
>
> JENNELL HUFF
> CUSTOMER SERVICE REP/MAINTENANCE SPECIALIST
> BANK OF THE ROCKIES, LEWISTOWN, MONT.

The State of Elder Financial Exploitation Today

How big is the problem?

According to a MetLife Mature Market Institute report, *MetLife Study of Elder Financial Abuse: Crimes of Occasion, Desperation, and Predation Against America's Elders*, seniors lose $2.9 billion annually due to financial abuse.[6] As the United States population continues to age, with the median age rising from 29.5 in 1960 to nearly 40 as of 2016,[7] the potential pool of victims only increases. Consequently, ABA strongly recommends that bankers focus on building and strengthening partnerships with APS and law enforcement officials to combat the problem on multiple fronts.

Who is an elderly customer?

Most banks offer "senior" banking programs to customers age 50 and older. Once customers reach the age of 62, they become a federally protected class. Among the most vulnerable consumers are those who are socially isolated, have poor physical health, and experience cognitive impairment.[8]

Why is elder financial exploitation growing so fast?

Baby Boomers, Americans born between 1946 and 1964, represent the largest portion of the population and continue to reach senior status in record numbers due, in part, to increased life expectancy. The U.S. Census Bureau estimates that one out of every five Americans will be 65 or older by 2030.[9] So, as a larger percentage of the population ages, more wealth tends to be concentrated among seniors.

6 http://www.canhr.org/reports/TheSentinelNov2011_HBABCs_fin_exploitation.pdf
7 https://www.statista.com/statistics/241494/median-age-of-the-us-population/
8 https://www.forbes.com/sites/johnwasik/2017/02/12/4-risk-factors-for-elder-financial-abuse/#19a737b55f93
9 https://www.census.gov/newsroom/press-releases/2018/cb18-41-population-projections.html

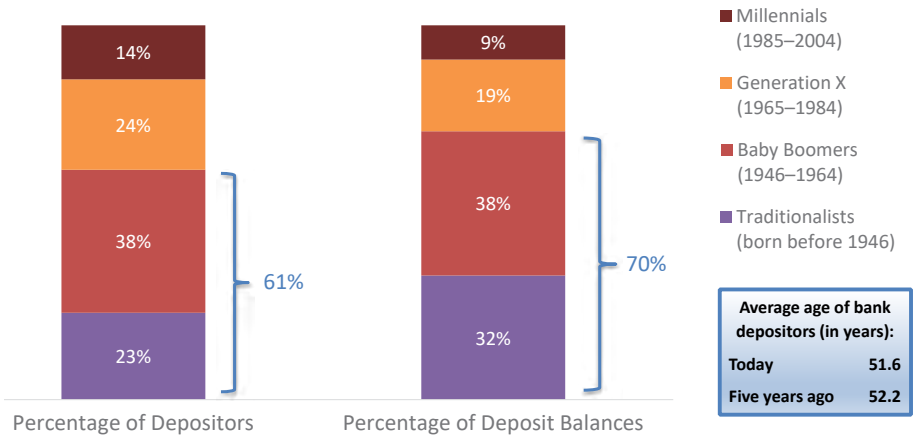
Why are banks so pivotal in helping to combat elder financial fraud?

Bankers should continue to be vigilant and educate their customers about potential fraud. In 2017, the Financial Industry Regulatory Authority (FINRA) issued new rules to guide financial advisors' conversations with older customers about cognitive decline.[10] These conversations happen between the financial advisor/banker and the customer, their family, trusted contacts and designees throughout the relationship, from account opening to intergenerational transfer of assets.

Intergenerational wealth transfer is happening now from the Greatest Generation (those born between 1910 and 1924) to Baby Boomers. According to an Accenture 2012 report titled, *The "Greater" Wealth Transfer: Capitalizing on the Intergenerational Shift in Wealth*, an estimated $12 trillion is currently transferring between generations. Accenture anticipates an even greater wealth transfer between Baby Boomers and their children over the next 30 – 40 years, with estimates in excess of $30 trillion.

With the stakes as high as predicted, it is more important than ever for bankers to leverage the engendered trust of their older customers. Bankers are in a prime position to help protect their customers from financial exploitation, since they can spot fraud at the onset and can also help prevent it.

ABA's 2017 *Older Americans Benchmarking Report* shows that people over the age of 50 make up about one-third of the population while accounting for 61% of bank accounts and 70% of bank deposits, as indicated in the chart below.[11]



10 http://www.finra.org/sites/default/files/Regulatory-Notice-17-11.pdf
11 https://www.aba.com/Engagement/Documents/2017-Older-Americans-Benchmark-Report.pdf

What are the ramifications for our elder customers affected by fraud?

Everyone can be affected by financial scams, but seniors are particularly susceptible. According to the Association of Certified Fraud Examiners (ACFE), "fraudsters target the elderly, as they may be lonely, willing to listen and are more trusting than younger individuals."[12] Typically, seniors accumulate their wealth during their careers and use it for their retirement. After the global economic crisis of 2008, many seniors found their nest eggs broken or at least severely cracked since much of their wealth was held in pensions, IRAs and real estate. Unfortunately, most of our senior customers do not have the time or the means to recoup large losses of their wealth experienced late in life. As a result, financially vulnerable seniors hoping to rebuild their savings may be susceptible to lottery, reverse mortgage or work-from-home scams. Beyond the obvious financial losses associated with financial abuse, exploited seniors experience depression, shame, guilt, fear, loss of security, and may even lose their homes.[13]

Top Scams Currently in Play

What are today's most prevalent forms of scams?

The table on the following page shows the top financial scams perpetrated against seniors, as identified by several of our partner agencies including AARP, the Consumer Financial Protection Bureau (CFPB) and the Financial Crimes Enforcement Network (FinCEN). The table also lists the agencies that you or the senior customer's family should contact when fraud is suspected or confirmed.

ABA recommends that you also check with your State Attorney General's office to determine if they recommend any other reporting avenues. More details about the scams can be found in the Appendix of this guide.

12 http://www.acfe.com/fraud-examiner.aspx?id=4294997223
13 http://www.napsa-now.org/policy-advocacy/exploitation/

Scam	Responsible Agency	Website
Medicare/Health Insurance	Dept. of Health and Human Services Inspector General, state insurance fraud department	https://oig.hhs.gov/fraud/report-fraud
Counterfeit Prescription Drugs	Food and Drug Administration (FDA)	https://www.fda.gov/Safety/MedWatch/default.htm
Funeral/Cemetery	Federal Trade Commission (FTC)	https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc
Fraudulent Anti-aging Products	FDA/FTC	FDA: https://www.fda.gov/Safety/ReportaProblem/ucm059044.htm FTC: https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc
Telemarketing/Phone	Federal Communication Commission (FCC)	https://consumercomplaints.fcc.gov/hc/en-us/
Internet/Email/Work From Home/Clickbait	FCC	https://consumercomplaints.fcc.gov/hc/en-us/
Homeowner/Mortgage	State Attorney General/ FBI/FTC	State Attorneys: http://www.naag.org/naag/attorneys-general/whos-my-ag.php FBI: https://www.fbi.gov/contact-us FTC: https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc
Sweepstakes/Lottery	FTC	https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc
Imposter (including Grandparent, IRS and Romance)	FTC	https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc
Check Fraud	FTC U.S. Postal Inspection Service	FTC: https://www.ftccomplaintassistant.gov/#crnt&panel1-1 USPIS: https://postalinspectors.uspis.gov

What Can Be Done?

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 to notify of 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.

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 non-sufficient 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.

Depending on the circumstances, banks may consider contacting the customer in the event something isn't right. This will require you to follow bank policy, which may require filing an internal report. The bank may decide to file a Suspicious Activity Report (SAR) and possibly even notify APS 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 elder financial abuse. The Financial Crimes Enforcement Network, a division of the United States Treasury, issued FinCEN Advisory FIN-2011-A003 which 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."

Separately from the FinCEN advisory, FINRA (broker/dealer regulator) issued guidelines in February 2018 that apply to securities brokers/dealers. FINRA Rule 2165 allows a broker/dealer to place a temporary hold on funds if they have a reasonable belief that fraud is occurring. In addition, Rule 4512 asks broker/dealer members to ask for a trusted contact.

Remember that each state may have different requirements, so make sure to find out what is required in your state.

The Roles of APS and Law Enforcement

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.[14] 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. If the customer is a resident of an assisted living or long-term care facility, APS may not have jurisdiction. You would need to involve the local long-term care ombudsman. More information is available at the National Center on Elder Abuse. [15]

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 could 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. The Appendix includes a chart provided by NAPSA that provides basic information on how APS operates in all 50 states.

14 http://www.napsa-now.org/get-help/how-aps-helps/
15 https://ncea.acl.gov/whatwedo/policy/state.html

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 Suspicious Activity Report (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.

How can I find the APS closest to me?

Your bank should have procedures in place to determine if and when the bank will contact APS, but you can also visit **www.eldercare.gov** or call (800) 677-1116. 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 you can personalize and use to reach out to a local APS.

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.

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 Multi-Disciplinary Teams (MDTs) that are discussed later in this document. Remember that specificity is critical for both APS and law enforcement.

> **"Knowing what to expect when you work with law enforcement helps you be a better partner by providing the documentation they need and thinking ahead to ensure video surveillance is archived for their use."**
>
> LAUREL SYKES
> SVP AND CHIEF RISK OFFICER
> MONTECITO BANK & TRUST, SANTA BARBARA, CALIF

LAW ENFORCEMENT

How can a bank best aid local law enforcement?

Timely and complete filing of SARs is a great first step. Law enforcement rely on SARs in order to be effective, but it's important to note that seniors may need to be willing to prosecute. Seniors might be unwilling to do so because of familial relationships or fear of retaliation from a caregiver, particularly if they are 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 for submitting the report.

Also, be aware of the provisions in the Gramm-Leach-Bliley Act that allow bankers to share limited non-public personal information in cases where financial fraud against seniors is suspected. You are sharing information for the benefit of your customer, not the bank or the law enforcement agency.

In preparing to address and prevent financial exploitation, it can help if the bank creates and maintains a list of contacts at local APS and all of the law enforcement agencies with whom 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 Statues to review which laws apply to your state.[16]

What is happening at a national level?

In February 2018, the FBI announced that a coordinated effort with federal agencies, such as the United States Postal Inspection Service (USPIS) and the Federal Trade Commission (FTC), resulted in 250 arrests of alleged perpetrators of financial fraud against more than 1,000,000 seniors. Criminals caught in the nationwide sweep caused more than a half a billion dollars in losses.

Another case in 2016 involving the U.S. Department of Justice, the Department of the Treasury's Office of Foreign Assets Control (OFAC) and the USPIS, among others, brought charges against foreign and domestic entities involved in massive fraud against seniors and other vulnerable people.

A critical piece that these two investigations have in common is that they began when bankers filed SARs. Without the vigilance and follow-through by bankers, the charges would never have been filed.

16 https://www.aba.com/Consumers/Documents/CumulativeElderFinancialAbuseStatutes.pdf

> **"People are more inclined to report with increased awareness."**
>
> ELAINE DODD
> EXECUTIVE VICE PRESIDENT
> OKLAHOMA BANKERS ASSOCIATION

Reporting

How do I report suspected elder financial fraud?

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

Since 2011, the 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 to provide 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 truly was 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.

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.

ABA FOUNDATION

How do you file a SAR?

SARs are filed through FinCEN's BSA e-filing system. You should follow your bank's process for reporting suspicious activity. Be sure to include the following information:

1. The information about the subject including all names, addresses, Social Security numbers (SSNs) or Taxpayer Identification Numbers (TINs), birth dates, driver's license numbers, passport numbers, occupation and phone numbers of all parties involved with the activity.
2. 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. The information about the financial institution where the activity occurred – main office, specific branch location(s), etc.
4. The contact information of the filing institution, which usually includes the compliance officer's information.
5. 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 might be required to also report to APS. However, it is important to note 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, sharing a SAR with APS would violate federal law. 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.

It is critical to know your state's requirements for reporting to APS when abuse, neglect or exploitation is suspected. 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. The more cooperation among entities working to combat this problem, the better.

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.
ABA FOUNDATION

What steps are typically involved once a banker files a report with APS?

According to NAPSA, once a report is filed in-person, on the website or via 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 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 because of fear. Reports can potentially remain anonymous depending on state regulations, which may help alleviate some fears 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 (Fed. 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.

Specific language from the GLBA states:

> *A financial institution may disclose nonpublic personal information to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability. (15 U.S.C. 6802(e) (3) (B) and implementing regulations at ___.15 (a) (2) (ii)).*

This exception generally would allow a financial institution to disclose to appropriate authorities nonpublic personal information 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.

As always, be sure to confirm what is allowed in the state where the fraud occurred.

How to Partner with APS and Law Enforcement

Strong working relationships between bankers, APS and law enforcement officials is critical in preventing and investigating financial abuse as well as the potential prosecution of fraudsters. Law enforcement officials need to know that banks are willing to collaborate and share permissible information to combat financial elder abuse. Reaching out to local law enforcement offices is a great way to get the conversation started. The Appendix contains a sample introductory letter you can personalize.

How can we best leverage the work being done by others?

Prevention is the best way to stem the massive losses from financial fraud against seniors. Communication and education – increasing awareness – are key to preventing or at least reducing this type of fraud.

Check fraud could involve the Federal Reserve, OCC or NCUA in addition to your bank's fraud department and local law enforcement. Local law enforcement should, at least always be informed, if not involved if the crime took place in their jurisdiction. You should also inform the State Attorney General's office, who can guide you on which contacts at the local, state and federal level need to be involved.

One of the advantages to filing a SAR is that the information is entered into a database available to many law enforcement agencies. However since it can take time to work its way through the system, when timing is critical, it also might make sense for the bank to contact law enforcement once the SAR has been filed.

Leveraging the research and resources provided by APS and various law enforcement and government agencies can help banks provide training and communication to seniors and groups involved with seniors on a continuous basis. A list of those resources is available in the Appendix. Also, be sure to check out ABA's Safe Banking for Seniors resources.[17]

Several banks interviewed in developing this guide indicated that they frequently ask law enforcement to participate in their community events to share stories about cases in which they were involved and how to identify red flags to stop this type of fraud in its tracks.

Tell me more about partnerships that are working together to combat elder financial fraud.

Strong partnerships between banks, law enforcement agencies, senior service agencies and non-profits, as they relate to financial exploitation of seniors, exist nationwide. At a local level, remember to develop and maintain contacts with all appropriate groups. For an overview of the various Federal law enforcement agencies and their areas of investigative expertise, visit the ABA's Law Enforcement Agencies page.[18]

17 https://www.aba.com/Engagement/Pages/safe-banking-for-seniors.aspx
18 https://www.aba.com/Tools/Function/Cyber/Pages/LawEnforcementContactsandResources.aspx

According to the CFPB, 54 existing networks have been identified that exist to help protect seniors. These networks typically take one of two forms – Multi Disciplinary Teams (MDTs) and Triads. MDTs include Forensic Centers (FCs) and Financial Abuse Specialist Teams (FASTs) that specialize in investigating financial abuse. The following table contains more details of these groups.

Category	Triads	MDTs	Other Networks
Primary Activities	Awareness, education and training	Case review	Advocacy, awareness, education, system change and training
Focus Areas	Safety and crime prevention	Elder abuse including financial exploitation	Depends
Strengths	Presence in 30 states, direct involvement with consumers	Direct support to victims; multidisciplinary expertise	Policy changes; stakeholder engagement
Usual Members	Law enforcement and senior services organizations	APS, area agencies on aging, law enforcement	Area agencies on aging, community and advocacy groups, senior services organizations
Geographic Coverage	City, county, town	City and county	All levels including statewide

Are bankers allowed to join?

Bankers can and should be a part of these networks. It may be that specific institutions cannot serve as standing members. Nevertheless, ABA recommends that banks learn about the networks and proactively keep abreast of network activities. Banks should offer support to triads, networks and all law enforcement agencies by sharing trend information and inviting them to participate in awareness, education and training events.

How do bankers benefit by participating in these partnerships?

MDTs, especially FASTs and FCs, should be on bank speed dials in areas where they are available. Working with these specialists can help expedite resolution of financial exploitation investigations and expand banker knowledge of what happens once the reports are made.

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. Additionally, if the the network is an MDT, then more cases can be investigated in a timelier manner. Remember, if prevention doesn't work, speed is imperative in a fraud investigation.

How do we develop a local network?

Expressing the desire to form a network is the first step. Connect with key local law enforcement, APS and any non-profits or other groups focused on helping our seniors. Use the resources provided by the National Sheriff's Association about how to form a network by visiting their website.[19] Reach out to current networks to gather best practices. While it doesn't take a lot of money, there is no central source of funding currently available and funding is up to the local networks. Some networks have formed on a volunteer basis, so no funding is needed. Please refer to the links in the Appendix for more information.

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

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 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.

19 https://www.sheriffs.org/programs/starting-triad

Key Takeaway Questions

1. What is the biggest source of elder financial exploitation in my community?
2. What types of fraud have my elder customers experienced?
3. What programs are in place to help educate me and my colleagues?
4. What programs are in place to help educate my customers?
5. What programs are in place to identify fraud or potential fraud?
6. What is my bank's current relationship with our local APS?
7. How can we build or strengthen our relationship with our local APS?
8. What is my bank's current relationship with our local law enforcement?
9. How can we build or strengthen our relationship with local law enforcement?
10. Is there a triad or official team in my area?

Appendix

Top 11 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, so 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:

a. 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.

b. Fake accident – the scammer convinces the senior that a relative or close friend has been in an accident and needs the money for treatment.

c. 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 upload an actual virus to the computer that grants the scammer access to personal information. The scammer may even install ransomware and request a payment to 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 would 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 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. Imposter Scam

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**)
- A Resource Guide Elder Financial Exploitation Prevention and Response Networks (**www.consumerfinance.gov**)
- Memorandum on Financial Institution and Law Enforcement Efforts to Combat Elder Financial Exploitation (**www.consumerfinance.gov**)

Additional Resources for Combating Elder Financial Exploitation

- ABA Foundation Toolbox on Protecting the Financial Security of Older Americans (**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**)
- Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults (**https://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/news_room/rp/files/sar_guidance_narrative.pdf**)
- Money Smart for Older Adults (**www.consumerfinance.gov** or **www.fdic.gov**)
- BankSafe Initiative: A Comprehensive Approach to Better Serving and Protecting Consumers (**www.aarp.org**)
- Snapshots: Banks Empowering Customers and Fighting Exploitation – part of BankSafe (**www.aarp.org**)
- Locate closest APS office (**www.eldercare.gov**)
- Final CFPB + Treasury + FinCEN Memo on Elder Financial Exploitation for ASA (**www.consumerfinance.gov**)
- National Adult Protective Services Association (**www.napsa.org**)
- FinCEN Advisory - FIN-2011-A003 (**https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a003**)

- CFPB Advisory to Financial Institutions on Elder Financial Exploitation (**http://files.consumerfinance.gov/f/201603_cfpb_advisory-for-financial-institutions-on-preventing-and-responding-to-elder-financial-exploitation.pdf**)

  The Report and Recommendations (**http://files.consumerfinance.gov/f/201603_cfpb_recommendations-and-report-for-financial-institutions-on-preventing-and-responding-to-elder-financial-exploitation.pdf**)
- ABA table containing state statutes on elder abuse (**https://www.aba.com/Consumers/Documents/CumulativeElderFinancialAbuseStatutes.pdf**)
- Long-Term Care rules (**https://ncea.acl.gov/whatwedo/policy/state.html**)
- BSA Joint Memo on working with law enforcement by FinCEN, CFPB and Department of Treasury (**https://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**) 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**)
  - Cybercrimes should be reported by banks to the FBI (**http://www.ic3.gov/default.aspx**.)

    Reference on MoneyPak (**https://www.fbi.gov/contact-us/field-offices/sandiego/news/press-releases/fraudulent-websites-posing-as-green-dot-moneypak-customer-support**)
  - Scams originating by mail should be reported to USPS at (877) 876-2455 (**https://postalinspectors.uspis.gov/pressroom/schemealerts.aspx**)
  - What about Money Gram and Western Union, etc.? (**https://www.moneypak.com/security**)
  - Report/file to get refunds – see the FBI article for info. (**https://archives.fbi.gov/archives/atlanta/press-releases/2013/fbi-atlanta-warns-consumers-of-green-dot-moneypak-scam**)
- Elder fraud DOJ Fact Sheet on sweeps (**https://www.justice.gov/opa/press-release/file/1037946/download**)
- Interactive map on elder fraud sweeps (**https://www.justice.gov/opa/february-22-2018-elder-fraud-sweep/map**)

Introduction 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 new [branch manager] 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]

Introduction Letter 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]

Introduction 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 new [branch manager] 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]

Introduction 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]:

[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. I am the new [branch manager] at the [Bank/Branch] location.

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 with this project.

Sincerely,

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

Notes

Notes

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: Traffic, Triad, and Officer Safety, National Sheriffs' Association
- **Elaine Dodd**, EVP Fraud Division, Oklahoma Bankers Association
- **Hector Ortiz**, Policy Analyst, Consumer Financial Protection Bureau
- **Jenefer Duane**, Senior Program Analyst for the Office for Older Americans, Consumer Financial Protection Bureau
- **Jennell Huff**, Customer Service Rep/Maintenance Specialist, Bank of the Rockies (MT)
- **Joe Snyder**, Director Philadelphia Corporation for Aging
- **Kathleen Quinn**, Senior Advisor, National Adult Protective Services Association
- **Laurel Sykes**, SVP, Chief Risk Officer, Montecito Bank & Trust (CA)
- **Luis Lobo**, EVP Multicultural Banking Manager, BB&T
- **Nan Gibson**, Office of Nonprofit Engagement, JP Morgan Chase
- **Regina R. Forest**, Director, Global Financial Crimes Compliance Exec, Global Financial Crimes Compliance- Financial Crimes Investigations, Bank of America
- **Stacy Canan**, Assistant Director for the Office for Older Americans, Consumer Financial Protection Bureau

In addition, we would like to thank **Bank of America, BB&T, JP Morgan Chase** 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®

1120 Connecticut Avenue, NW | Washington, DC 20036 | aba.com/seniors | 1-800-BANKERS