MARYLAND'S

PROJECT SAFE

STOP ADULT FINANCIAL EXPLOITATION

MODEL REFERENCE MANUAL
FOR FINANCIAL INSTITUTION EMPLOYEES

Second Edition

Revised September 10, 2012

Martin O'Malley
Governor

Anthony G. Brown
Lieutenant Governor

A Public/Private Partnership of

Commissioner of
Financial Regulation

**Maryland
Triad/SALT
Network**

ACKNOWLEDGMENTS

This Model Reference Manual and the companion video are major components of Project SAFE's training materials. The training video can be found at https://youtu.be/9NtlvwiIm8A . Project SAFE is deeply indebted to the states of Massachusetts and Oregon. Our Model Manual is adapted from Massachusetts' "Employee Training Manual." Our training video is an edited version of Oregon's training video for front-line, financial institution employees. Both were very gracious in allowing Project SAFE to use the copyrighted materials that they had created.

This project was supported by Byrne Grant 1999-1005, awarded by the United States Department of Justice. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the United States Department of Justice.

The case studies in this Model Manual are based on actual cases, although names and other identifying information have been changed to preserve confidentiality. Not all the cases have happy endings.

Project SAFE hopes to identify cases more promptly, before the vulnerable adult's assets are completely depleted. An additional Project SAFE goal is to educate financial institution employees and customers about ways to prevent financial exploitation.

DOUGLAS F. GANSLER
Attorney General

KATHERINE WINFREE
Chief Deputy Attorney General

JOHN B. HOWARD, JR.
Deputy Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

June 6, 2012

Dear Members of the Financial Community:

Financial exploitation robs victims of their hard earned savings all too often. Early detection of this crime, however, can help minimize the damage. With the passage of House Bill 1257/Senate Bill 941, the 2012 Maryland legislature established a new type of protection for elder adults living in Maryland. Now you, the employees of financial institutions, are required to play a pivotal role in the process of detecting and reporting possible financial exploitation of elder adults. This requirement is a new one and builds on a 2000 law that allowed financial institutions to voluntarily report suspected exploitation of vulnerable adults.

The Project S.A.F.E. (Stop Adult Financial Exploitation) public/private partnership first developed this manual in 2000. We recently revised it to offer guidance on this new responsibility. The manual is a valuable tool to help you understand financial exploitation and the role you can play in preventing it. As part of this training, you will learn how to recognize the warning signs of financial exploitation and how you must respond to help protect elder adults from possible exploitation.

This new legislation requires a number of different entities in the private and public sectors to work together in the important effort of fighting financial exploitation of elder adults in Maryland. All of us are committed to this goal and to working together for the benefit of our customers and citizens, be they vulnerable or elderly. Use this manual to learn about the key role you and your financial institution will now play in the process of keeping vulnerable adults and Maryland's elder adults safe from those who seek to exploit them.

Sincerely,

Douglas F. Gansler
Attorney General
State of Maryland

Gloria G. Lawlah
Secretary
Maryland Department of Aging

Theodore Dallas
Secretary
Maryland Department of Human Resources

Kathleen M. Murphy
President & CEO
Maryland Bankers Association

Robert C. Hyde
President
Maryland Association for Bank Security

Mark A. Kaufman
Commissioner
Maryland Department of Financial Regulation

Hank Greenberg
State Director
AARP Maryland

Barbara Korenblit/Lynn McCamie
Co-Coordinators
BC-REST
(Baltimore County-Restoring Elder Safety Today)

Merry O'Brien
Coalition Coordinator
P.E.A.C.E Coalition
(Protecting Elders Against Crime & Exploitation)

TABLE OF CONTENTS

KEY TERMS USED IN THIS MANUAL

- **ABUSE REFERRAL LINE: (1-800-91-PREVENT)**

This customer service number transfers callers to the appropriate local APS unit from 8:00 a.m. to 5:00 p.m., Monday through Friday. It will route reports of abuse, neglect, or exploitation of vulnerable adults to the local APS.

- **ADULT PROTECTIVE SERVICES (APS):**

Local Department of Social Services program that receives and investigates reports of abuse, neglect, self-neglect, and exploitation of vulnerable adults. See Section IV.

- **ATTORNEY GENERAL'S CONSUMER LINE (1-410-528-8662 or Toll-free 1-888-743-0023)**

To file a complaint via the web go to www.oag.state.md.us/consumer/

- **ELDER ADULT:**

A person believed to be residing in Maryland and 65 or older.

- **FIDUCIARY:**

An individual appointed (1) guardian by a court of another person's property or (2) to act on behalf of another person, by that person, in a legal document known as a Power of Attorney.

- **FINANCIAL ABUSE OR EXPLOITATION:**

Any action which involves the misuse of a vulnerable or elder adult's funds or property.

- **FINANCIAL INSTITUTION EMPLOYEE:**

Anyone with a full or part-time job, other than security, who may come in contact with a customer or a customer's financial records. Includes tellers, customer services representatives, managers, computer operators, or other staff.

- **FINANCIAL INSTITUTION OR INSTITUTION**

Includes banks, credit unions, and savings and loan associations that are either maintain a branch in Maryland or are organized under Maryland law.

- **OMBUDSMAN PROGRAM:**

Department of Aging program that investigates complaints concerning nursing home and assisted living residents and advocates on behalf of the residents. See Section V.

- **SECURITY/MANAGEMENT:**

Any designated department or individual with full or part-time responsibility for investigating and reporting possible instances of financial exploitation to outside authorities.

- **VULNERABLE ADULT:**

An adult who lacks the physical or mental capacity to provide for his or her daily needs.

SECTION I

OVERVIEW

Mr. J. was a regular customer at his financial institution. He went in once a week to cash a check for a small amount. One week a teller noticed he came in three different times. He was accompanied by a woman the teller had not seen before. On each occasion Mr. J. cashed increasingly large checks. The final check cleaned out his account.

The following week, he came into the institution to cash his usual small check, and she had to tell him that his account was empty. Mr. J. did not seem to remember the transactions he had made the previous week. When he discovered he had no money, he stood in the lobby and cried.

The teller called Protective Services in great distress. She asked if Mr. J. could be helped. The teller said that she had felt that there was something wrong, but had not known what to do. Had she been aware of the warning signs of financial exploitation, the appropriate employee response to these situations, and the protocol for reporting suspicions, this exploitation might have been prevented.

Project SAFE is a collaborative effort to combat financial exploitation. Through participation in Project SAFE, financial institutions and their employees can help to prevent financial exploitation. Any financial institution may adopt and adapt this Model Manual as it sees fit as long as it provides proper attribution to Project SAFE. It can be used in conjunction with SAFE's training video, which can be found at https://youtu.be/9NtlvwiIm8A .

Financial abuse or exploitation is the improper use of a vulnerable or elder adult's funds or property. A vulnerable adult is someone who lacks the physical or mental capacity to provide for his or her daily needs. An elder adult is defined as an individual who is believed to be at least 65 years old and residing in the State.

People over sixty are the most rapidly growing segment of our population. Older people may be very vulnerable to abuse, and unscrupulous people increasingly target them as victims. One of the most devastating forms of abuse is financial exploitation. Adult Protective Services programs throughout the country find that over 20 percent of their substantiated cases of mistreatment involve financial exploitation. The Attorney General's Office also sees an increasing number of con artist scams against elders. Many cases go unreported or are not discovered until the victim has been stripped of all of his or her assets.

This Model Manual is a quick reference guide developed especially for employees of financial institutions. It describes common symptoms of exploitation that will help identify appropriate cases for reporting. The Manual also sets forth a model reporting protocol.

Financial institution employees understand exploitation is a real problem. They are in a unique position to have early knowledge of financial abuse. Financial institution employees with customer contact often see situations develop where they believe that the customer is at risk. It is vitally important that they know how to report these cases to public authorities while appropriately safeguarding customer confidentiality.

Other resources for elders. While the focus is on preventing financial exploitation, through the Project, employees can become aware of services that neither they nor their customers knew existed. People can become vulnerable to exploiters simply because they need practical help with a day-to-day need. When no trusted family member is available, it can be helpful to arrange services through a reliable provider, including transportation to the bank or credit union, homemaker services, grocery deliveries, and help with financial management. These and many other services make a person, especially an elder adult, less dependent on and vulnerable to exploitation or abuse by others. All of these services or referrals may be available through the local Department of Social Services or local aging agency. See this website: www.marylandaccesspoint.info/

Miss G., age 92, had been hospitalized for a year due to a fractured hip and bedsores. A neighbor, who had been handling her finances during this time, died.

Miss G. agreed to have the neighbor's 23 year old daughter, Loren, named on her accounts. Loren was paid $50 a month for her help. When Miss G. discovered Loren had been writing checks for her own purchases, she called Adult Protective Services. She wanted to press charges for the theft of $3,000, and to have her money returned.

Miss G.'s financial institution, with her consent, helped with the investigation by providing copies of missing statements and 29 cancelled checks showing personal use of Miss G.'s money by Loren. As the money had been withdrawn by a signatory of a joint account, the bank manager stated the bank could not refund the money. The local prosecutor would not prosecute for the same reason. A private attorney believed that the cost of a small claims suit would exceed the amount of the original loss.

The Adult Protective Services caseworker met with Miss G, Loren, and her father. Loren's family agreed to repay the money in return for a written statement from Miss G. stating that she would not pursue legal action. Miss G.'s nephew is now helping her with paying her bills.

SECTION II

RECOGNIZING FINANCIAL EXPLOITATION

When her credit union notified Mrs. C. that her savings account was overdrawn because of her frequent use of an ATM card, Mrs. C. said that she did not know what an ATM card was. Mrs. C. had rarely left her house and had not visited the credit union for several years due to her increasingly frail health. A visiting nurse reported the case to Adult Protective Services. The credit union was contacted during the investigation. Adult Protective Services and credit union security discovered that Mrs. C. was being exploited by a young man, Alan, a neighbor's son.

Alan had asked Mrs. C. to sign an ATM card application when she was intoxicated. He took the signed application to the credit union, claiming to be acting for her. No one questioned this claim or called Mrs. C. to verify her wishes. Alan retrieved the ATM card from the mail, made up a PIN number, and began making almost daily withdrawals of $100 to $300. In three months he had depleted her life savings. Mrs. C. was no longer able to pay her medical bills.

Adult Protective Services and her credit union helped Mrs. C. to cancel the ATM card. A report of theft was filed with the local prosecutor, and a warrant was put out for Alan's arrest.

A. DEFINING FINANCIAL EXPLOITATION

1. WHAT IS FINANCIAL ABUSE OR EXPLOITATION?

Financial abuse or exploitation occurs when a person misuses a vulnerable or elder adult's funds or property.

2. WHO IS A VULNERABLE ADULT?

A vulnerable adult is a person who is eighteen or older and who lacks the physical or mental capacity to provide for his or her daily needs.

3. WHO IS AN ELDER ADULT?

An elder adult is an individual who is believed to be both 65 or older and residing in the State. A person can be both a vulnerable adult and elder adult, e.g., a 67 year old Maryland resident who lacks the capacity to provide for his daily needs would be both an elder adult and vulnerable adult. It is important to remember the distinctions and overlaps between vulnerable and elder adults because there are different reporting requirements and resources for the two groups.

4. CONSENT AND COMPETENCY

Financial exploitation can happen in three ways:

(a) ***Without*** the victim's ***consent***, or

(b) if the victim is ***tricked, intimidated,*** or ***forced into*** giving ***consent***, or

(c) if the victim is ***too confused to be able to give valid consent.***

People must be fully informed of and authorize any transactions made in their names. Consent must be freely given. Tricking, forcing, or coercing vulnerable or elder adults into giving consent, does not create valid consent.

Moreover, a person must be able to understand the situation, and the implications, and consequences of any choice. In other words, a person must be "competent" to give valid consent to a transaction. When contested, competency is a legal issue decided by a court of law. For your day-to-day purposes consider "competency" to be a person's sufficient ability to understand, make, and communicate responsible decisions concerning his or her person, including provisions for health care, food, clothing, shelter, and financial affairs.

Financial institution employees should presume older customers to be competent and responsible for making decisions about their own finances. Older customers who appear very confused or disoriented may need help, however. Even if you do not suspect financial exploitation, you may report your concerns to security/management. Security/management can suggest to customers that they contact the local area aging agency for assistance.

5. THE RIGHT TO CHOOSE

It is not financial exploitation if a competent adult willingly consents to a transaction, even if it appears to be a bad deal to you. Mrs. A., for example, who hardly has any money, willingly gives her reckless grandson several thousand dollars as a wedding present.

Sometimes the onlooker may think that a vulnerable or elder adult is making a poor choice. Mrs. D., for example, a seventy-year-old woman with a low income, repeatedly bails out her cocaine addicted granddaughter who neglects her. To some this may appear to be a bad idea. However, if she is competent, Mrs. D has every right to spend her money this way. She has the right because ***competent adults of all ages have the right to make their own decisions, even if those decisions are ones that most people would not make.***

B. TYPES OF FINANCIAL EXPLOITATION

1. THE TWO MAIN CATEGORIES OF EXPLOITERS

There are two main categories of financial exploiters:

(a) Exploitation of people *known* to the victim (family members, friends, caregivers, or fiduciaries).

(b) Exploitation by *strangers* (scam artists).

Family members, acquaintances and fiduciaries, who have ongoing relationships with the victim, will typically use different exploitation methods than the scam artist, who is a stranger. Exploitation, regardless of the type of exploiter, may be reported. See Section III.B below.

2. FAMILY, ACQUAINTANCE, AND/OR FIDUCIARY EXPLOITATION (PERSONAL RELATIONSHIP EXPLOITATION)

Most family members and friends provide vital assistance to frail elders and younger adults with disabilities. Without this help, many elder adults and vulnerable adults would not be able to remain safely at home. Obviously, financial institution employees should continue to encourage elder adults and vulnerable adults to use trusted friends and family members to help them with financial matters when necessary.

However, do not be blind to the fact that some family members and friends exploit vulnerable adults and elders. They are particularly susceptible to exploitation from someone they know, trust, and love. When exploited by family members and friends, they may also be physically or emotionally abused. Often their needs are neglected when their money is spent by the exploiter. Fiduciaries, people with powers of attorney and court appointed guardians, can also exploit vulnerable and elder adults.

People who exploit their family members often do so because of: an addiction or gambling problem, exorbitant debt or other financial needs, fear that a potential inheritance will be lost or dissipated, familial dysfunction with siblings or a parent, etc.

Victims may be reluctant to admit they are being exploited, especially if the exploiter is someone they know. They may feel embarrassed or ashamed that a family member is abusing them. They may fear retaliation, be dependent on the abuser for care, or worry that they will be placed in a nursing home if they admit to being abused and the caregiver is removed. Some victims may also be confused or have dementia and be unable to care for themselves. These victims may be unaware that they are being exploited and abused and may be unable to find help due to their condition.

Family members, friends, and fiduciaries who exploit vulnerable and elder adults frequently use the following methods.

(a) Signing Checks or Documents Without the Victim's Consent

An exploiter may forge or alter checks or withdrawal slips to obtain money from the victim's checking or saving account. For example, the victim signs a blank savings withdrawal slip and the perpetrator later fills in a large amount. The suspect may also forge the victim's name on ATM card applications, credit card applications, or deeds to gain control of the victim's assets. For instance, a neighbor "helping" an elderly woman with her banking transactions forged her signature on an ATM card application and made up a PIN number. He withdrew approximately $250 a day until her savings of $6,000 were depleted.

(b) Charging Excessive Fees for Rent or Caregiver Services

Vulnerable adults may be charged excessive fees for rent, transportation, meals, laundry, personal care, or other services provided by relatives, "friends," or neighbors. For example, an elderly woman moved in with her daughter and was charged $2,500 for rent per month for a single room and shared living space, where she felt unwelcome. In another case, an elderly person was charged an exorbitant amount of money each week by a neighbor just to pick up a single small bag of groceries.

(c) Theft of Money or Property

Money or property taken without the victim's prior knowledge and consent is exploitation regardless of the amount taken. A son taking $50 of his mother's cashed Social Security check each month from her bureau or dresser drawer without her consent is financially exploiting her by stealing. This "small" amount causes a substantial loss because of her limited income.

(d) Obtaining Money or Property by Undue Influence, Coercion, Misrepresentation, or Fraud

Although a victim may "give" the perpetrator money or property, it is exploitation if the "gift" was motivated by fear or deception.

Undue influence is not a principle that only involves disputed wills. A gift made by a person who is still living can be set aside on the grounds of undue influence, if the recipient of the gift had a confidential relationship with the gift giver and the recipient cannot show that the gift was voluntary, fair, proper, and reasonable under the circumstances.

Coercion does not require physical violence. It can include withholding food or medication; isolating the victim from friends, relatives, or services; confining the victim; depriving him or her of the company of loved ones; etc. A daughter, for example, threatened to have her mother put in a nursing home against her will and not allow visits with her grandchildren unless she was given access to her mother's life savings.

Misrepresentation or fraud occurs when the suspect seeks to obtain the consent of the victim to give or sign over assets by misrepresenting the intent of the transaction. An elderly woman, for example, signed the deed to her house over to a friend. The victim believed that she would be able to remain in her own home until she died. Her friend promised to care for her there and, in return, have the house after she died. The "friend" sold the house almost immediately after the deed was signed over to her. The victim had to move to a nursing home because she had nowhere else to live. Caretakers may also tell their clients that they need to write checks for food and/or medical treatment when the caretaker is using the money for his or her own benefit. Often, if the caregiver is a substance abuser, the victim's money is used to finance the caregiver's addiction.

3. SCAM ARTIST EXPLOITATION

There are also numerous situations in which elder and vulnerable adults are the victims of scams by strangers or people who have befriended them solely for the purpose of fleecing them. The victimization rate for fraud is very high among older people. Con artists often target the vulnerable or elderly because they can be more trusting or lonely. Some have time to listen to the "pitch" of the con artist and may be more susceptible to being misled by fast or double talk.

Many older people also have saved up significant assets over the years and have relatively easy access to those savings, whereas many younger people have committed their money to raising families, educating children, or paying for their homes. Some con artists keep records and lists of those they have previously conned. Because the people on these lists have been successfully swindled in the past, they are considered "leads" or "marks" for future swindles.

No one is immune from a con artist. People of all ages, abilities, and backgrounds have been swindled. Con artists are successful for several reasons. Many con artists have the abilities of professional actors and can convincingly present themselves as trustworthy to their potential victims. Also, most people believe they are too clever to be swindled. Con games can be very difficult to detect. There are two reasons for this. First, frauds are committed without violence. People (even police**)** in the vicinity will normally be unaware that a fraud is being committed. Second, frauds are seldom reported to authorities. There are several reasons for low reporting. Many victims are embarrassed to report that they have been swindled; some are not aware that they have been conned; and others may conclude that there is nothing the police can do to recover their money or other assets.

Con games are very difficult to investigate and prosecute. People who swindle others cannot easily be traced. That is why it is so critical for financial institution employees and security/management to intercept cons as quickly as possible.

Financial institution employees can help defeat fraud by educating themselves and their customers in advance about common scams. Scams fall into four basic categories: (1) person-to-person confidence scams, (2) mail fraud, (3) telemarketing fraud or telefraud, and (4) internet scams.

In the subsections that follow are descriptions of some of the classic scams in each category. However, new scams are developed daily. While common themes may run through various incarnations of scams, listing all the scams is impossible. Thieves are often highly skilled in transforming an old scam anew to stay two steps ahead of law enforcement professionals. To stay abreast of the latest scams, sign up for email alerts by visiting the Better Business Bureau's Scam Source page found here: www.bbb.org/us/scam-source.

(a) Person-to-Person Confidence Scams

Confidence scams are constantly evolving (although perhaps "devolving" is the more appropriate word). Some of the most popular and successful are "the bank examiner," "the pigeon drop," "the home repairman," and the "fake accident ploy." All these require person-to-person contact with the victim (although initial contact may be made by a phone call). All have variations, but usually the victim is conned into believing he or she is doing a good deed or being offered a great deal or both.

The Bank Examiner scam entails the con artist convincing the victim that he is an official of some kind. The con artist/"examiner" then tells the victim that he is trying to trap a dishonest bank employee and asks the victim to withdraw a large amount of money and give it to him so that he can check that the notes are genuine. The con artist/"examiner" will tell the victim that the money will be redeposited immediately, or will hand back an envelope that supposedly contains the money. Of course, the money is never redeposited, or the envelope is full of useless paper.

The Pigeon Drop is usually run by females. One con approaches the intended victim with a "found package" containing a large sum of money and a note. The note gives the impression that the money represents the proceeds from illegal activities and is unlikely to be claimed. The con asks for advice on what to do.

Typically, her accomplice then appears and claims that she works for an attorney. She announces that they can split the money three ways after a waiting period of 30 days. The accomplice suggests that they all make a "good faith" payment to prove that they won't be tempted to spend the money before the waiting period expires. The cons place what appears to be $2,000 or more of their own money in the "found package." They take the victim to his or her financial institution for a withdrawal that goes into the package as well.

The accomplice then drives the victim to the "attorney's office" to deposit the cash for safekeeping. Once inside, the con suddenly has to make a phone call or use the bathroom. To avoid any suspicion she gives the victim the "found package" to hold. When the con fails to return, the victim discovers that he or she is holding a package containing nothing but blank paper.

The Home Repairman arrives at the victim's door and tells her that her roof, gutters, and/or driveway are in a bad, if not dangerous condition. He explains that he can do the job very

cheaply as he has material left over from another job nearby. If the work is done, it is done badly. For example, the cons put black oil on a driveway so that it looks good for a while and leaves with the payment. Usually no repairs were even needed.

(b) Mail Fraud

This includes phony contests or sweepstakes; selling nonexistent or misrepresented investments in annuities, stocks, securities, precious metals, or real estate; touting worthless or dangerous medical cures; soliciting money for phony charities; promoting participation in fraudulent work-at-home schemes; and selling "dream vacation" packages that turn into nightmares. This list is not all-inclusive, but it represents the variety of mail frauds that can victimize elders and younger people as well.

In some instances of mail fraud the victim is asked to place a phone call to confirm their winnings. The victim may then be asked for financial information, for example, account or credit card numbers, to "check that we are talking to the right prizewinner." Charges can then be made to the victim's account without their knowledge.

(c) Telemarketing Fraud and 1-900 Numbers

Telefraud operations employ callers who use rehearsed, high-pressure sales pitches over the telephone. They convince people to buy products that are never delivered, invest in fictitious enterprises, participate in contests to win worthless prizes, or contribute to phony charities. Telefraud operators can also use many of the same scams as the mail fraud operators, e.g., phony sweep stakes.

Often elderly people are enticed to call the telefraud organization by advertisements for services placed in magazines or newspapers. Sometimes 800 or 900 numbers are given to victims to call. When the victim places the call they get a hard sell or are asked to call another number for confirmation. That second number may be a 900 number. Any 1-900 number call is a pay-per-call service. The caller has to pay after the call. The charges show up on the next telephone bill. While the caller is supposed to be told of the charge rate, frequently this does not happen. In 900 frauds the victim is tricked into staying on the phone for long periods to run up the charges.

(d) Internet Fraud

With the growth of the Internet, scams that had previously been limited to telephone or mail are now being perpetrated via the computer. There are now variants of the fake contest, debt consolidation, business opportunity, miracle cures, and charity scams that are committed with false or misleading websites, or through e-mail solicitations.

As older adults begin to make up a more sizeable portion of internet users, they are becoming increasingly vulnerable to this type of fraud. The Internet Crime Complaint Center reports that individuals over age 60 account for the most dramatic rise in internet crime complaints over the last ten years.

In addition to the Internet variations of telephone and mail scams, there are new scams that have appeared recently appeared that are unique to the world of computers. While it is impossible to document all of these scams, these are some of the most common:

Non-delivery of Merchandise or Payment was the most widely reported type of fraud in 2010. This is when a purchaser does not receive the items purchased over the Internet or telephone, or when a seller does not receive payment for items sold. Sometimes, this crime occurs in the context of an online auction site.

Phishing is the sending of a false e-mail that claims to be from a legitimate business or government agency. Often times the e-mail claims to be from a financial institution, the Social Security Administration, or the FBI. Often the e-mail claims that billing or account information needs to be updated, or that the victim's help is needed to catch a dishonest employee (similar to the "bank examiner" scam). Sometimes there is a claim that the individual's account will be frozen or liquidated, if information is not provided. This fraud attempts to get the recipient to reveal personal information, passwords, credit card numbers, or account information. Once this information is obtained, identity theft occurs and the thief uses the information to perpetrate other crimes without the knowledge of the victim.

The Stranded Victim occurs when the criminal hacks into an individual's e-mail address book. The criminal then sends an e-mail to contacts in the address book claiming to be stranded in a foreign country and in desperate need of help. The e-mail appears to be from a friend because it comes from his or her e-mail account. The criminal asks for money to be wired to help them out of their bad situation, but it is actually a fictitious story.

Overpayment Fraud can occur over the Internet or by mail or phone when the victim receives a payment which is significantly larger than the original sum agreed upon for a product or service. Often this is used when the victim is advertising an apartment rental or the purchase of a vehicle. The victim is then asked to deposit the payment into his or her account and pay back the difference. In actuality, the original payment is counterfeit and the individual is being scammed.

Internet Dating Scams begin with a man or a woman registering on a dating website. Often the website itself may be legitimate, but in due time a scammer, using an assumed name contacts the victim. The scammer generally claims to live outside the United States. While the correspondence begins on the dating website, it often moves into personal e-mail or even phone calls with the victim. As the trust of the victim is gained, the scammer professes romance and often marriage intentions toward the victim. Ultimately, however, the scammer will begin to ask for money from the victim for various fictitious scenarios. Some of these scenarios include: travel expenses, visas, help getting out of a difficult situation, medical emergencies, or help for a needy relative.

Advance Fee Schemes occur when the victim pays money to someone in anticipation of receiving something of greater value — such as a loan, contract, investment, lottery winnings, "found money" or gift — and then receives little or nothing in return. In some cases, thieves will

offer to find financing arrangements for their clients who pay an advanced "finder's fee." They require their clients to sign contracts in which they agree to pay the fee when they are introduced to the financing source. Victims often learn that they are ineligible for financing only after they have paid the "finder" according to the contract.

4. ELECTRONIC BANKING SERVICES - Automated Clearing House (ACH) Debits, Remote Created Checks, Online Banking, etc.

An exploiter may be savvy enough to realize that current financial products and services offer non-face to face transactions via electronic banking. The person victimizing a vulnerable adult may realize that they will never need to show up in your branch in person (and be caught on camera). Financial products such as ACH debits, remotely created checks, bill payer services, telephone banking, remote deposit, and online banking can offer an exploiter an anonymous means to withdraw funds from the account of a vulnerable or elder adult. The exploiter may also utilize your institution's electronic services to monitor account activity and target only those accounts that the victim rarely uses (e.g., special savings, Christmas club account, or a line of credit). For the victim, this activity may go unnoticed for weeks or months.

These electronic banking services may be exploited by either scam artists or exploiters with a personal relationship to the victim, e.g., family, friends, fiduciaries, etc. Anti-money laundering software may also pick up cases of financial exploitation.

TYPES OF FINANCIAL EXPLOITERS

PERSONAL RELATIONSHIP	SCAM ARTISTS
SUSPECT Is known to the customer. May be family member, friend, acquaintance, care takers, or fiduciary.	**SUSPECT** Is initially a stranger to the customer and employs person-to-person, mail fraud, telefraud or internet scams.
SUSPECT misuses a vulnerable adult's funds or property. **FINANCIAL EXPLOITATION**, which is sometimes combined with other forms of abuse or neglect, may include: Signing checks or documents without consent • Charging excessive fees for rent or caregiving services • Stealing money or property • Obtaining money or property by undue influence, misrepresentation, coercion, or fraud.	**SUSPECT** employs a person-to-person, mail fraud, telefraud or internet scam to obtain money. **COMMON SCAMS** are: ***The Bank Examiner*** Customer is enlisted by fake bank examiner to withdraw money as part of government investigation into teller fraud. • ***The Pigeon Drop*** The con (usually a woman) claims to be willing to split found money with customer if customer makes a "good faith" payment. • ***The Fake Accident Ploy*** The con gets the customer to withdraw money on the pretext that the customer's child or grandchild is hurt or in the hospital.

SYMPTOMS OF FINANCIAL EXPLOITATION:

SUSPICIOUS BEHAVIOR THAT MAY INDICATE FINANCIAL EXPLOITATION

A vulnerable or elder adult may be financially exploited if they are:

- Accompanied by:

- a stranger who encourages them to withdraw a large amount of cash,
- a family member or other person who seems to coerce them into making transactions, or
- a person who appears too interested in their financial status.

- Not allowed to speak for themselves or make decisions.

- Nervous or afraid of the person accompanying them or reluctant to discuss financial matters.

- Giving implausible explanations about what they are doing with their money.

- Concerned or confused about "missing funds" in their accounts.

- Unable to remember financial transactions or signing paperwork.

- So isolated or inaccessible that the financial institution cannot speak directly with them despite repeated attempts.

- Fearful that they will be evicted, or institutionalized, if money is not given to a caregiver.

- Neglected or receiving insufficient care given their needs or financial status.

- Isolated from other family members or support by a family member or acquaintance.

SYMPTOMS OF FINANCIAL EXPLOITATION:

POTENTIALLY SUSPICIOUS BANKING ACTIVITY

- **Unusual volume of banking activity:**
  - Frequent account changes from one branch or financial institution to another
  - Change withdrawal pattern (e.g. several in one day), or unusually large withdrawals
  - Large withdrawals or transfers from recently opened joint accounts

- **Banking activity inconsistent with customer's usual habits:**
  - Large withdrawals from previously inactive accounts or savings accounts
  - Frequent withdrawals made through ATMs, especially if customer is physically frail or has not used ATM previously
  - Uncharacteristic Non-Sufficient Fund activity or nonpayment for services, e.g. rent or utilities
  - Stable, single beneficiary trusts are revoked
  - Uncharacteristic attempts to wire large sums of money
  - Closing of CDs or accounts without regard to penalties
  - Distribution provisions are altered to require payments to third parties

- **Suspicious signatures on checks or other documents, like credit card applications:**
  - Customer's signature appears forged
  - Customer's signature appears correct, but amounts are written in a different handwriting
  - Use of different pens or inks may indicate that something is wrong

- **Sudden increases in incurred debt when customer appears unaware of transactions:**
  - Loans or second mortgages are obtained
  - Large credit card or reserve credit debts

- **A fiduciary or other person begins handling an elder customer's affairs and withdraws funds with no apparent benefit to the customer.**

- **Statements and cancelled checks are no longer sent to the customer's home (verify that this is the customer's wish).**

- **Implausible reasons for banking activity are given either by the customer or the person accompanying him or her.**

SYMPTOMS OF FINANCIAL EXPLOITATION:

POTENTIALLY SUSPICIOUS ELECTRONIC BANKING BEHAVIOR

- A change in the customer's normal banking behavior, especially if funds are being frequently withdrawn through electronic banking means.
- Longtime customer, who traditionally conducts their transactions in a branch, now has a sudden flurry of electronic debits.
- Numerous online banking withdrawals by official or cashier's check that are made payable to the same individual.
- Frequent presentment of Remotely Created Checks payable to the same individual.
- Utility payments made twice, but to different customer accounts. Your customer may have a pattern of making payments by check through the mail, but the account shows duplicate payments (e.g., two phone bill payments) by electronic means.
- Customer does not have an awareness of online banking, ACH debits, pay-by-phone services yet the account shows this activity.
- Customer is confused about an account change of address that was made by an online banking service.
- Frequent electronic transfers to a bank account held in the name of another individual.
- Electronic transactions are submitted from a different IP address than the one the customer normally uses.

SAMPLE FINANCIAL EXPLOITATION (FRAUD) ALERT FORM

FRAUD/FINANCIAL EXPLOITATION ALERT

Warning: Be Cautious About Cash or Check Withdrawals

In an effort to protect you from becoming a victim of fraud or exploitation, we ask you to read this form carefully. Feel free to ask our staff *any* questions you may have.

There are a number of methods commonly used to take people's money. In many cases those who want to take advantage of you appear to be friendly. If you are involved in a situation like any of the following, please let our staff know immediately. If necessary, we will assist you in getting help.

Have you been approached for money by someone who:

- **Claims to have found money and is now asking you to put up a "good faith" payment in order to split the cash?** This is a classic scam known as the "pigeon drop."
- **Claims to be involved with a law enforcement or regulatory agency and is asking you to help with a criminal investigation?** This ploy is known as the "bank examiner scam." Real investigators *never* ask people for money.
- **Claims to be a town inspector or other municipal official and insists that you owe cash for some service?** Never pay cash; always insist on a check. Confirm the identity of the individual by insisting on seeing identification. Call the agency he or she claims to represent.

Are you being pressured to give someone money?

Whether it is a stranger, friend or family member asking for money, it is improper, and possibly illegal, for him or her to pressure or threaten you: (a) for money or (b) to add his or her name to your account.

If a family member or someone you know is pressuring or threatening you for money, you may be a victim of financial exploitation. If you have any doubts about whether a transaction is "on the level," please talk to our staff about the matter.

Please Either Initial Option 1 or Check the Actions that Apply and Sign Option 2 Below:

Option 1. _____ I do not wish to process my requested financial transaction. I would like to speak confidentially to a manager about this matter.

Option 2. I have read and understand this statement. I still wish to process the financial transaction that involves: (Check all that apply)

_____ Lump sum withdrawal of $_____
_____ Transfer of assets
_____ Addition of name to account
_____ Other

Signature _____ **Name** _____

Address _____ **Telephone #** _____

Account Number _____ **Check Number** _____ **ID. #** _____

SECTION III

RESPONDING TO FINANCIAL EXPLOITATION

Tina was addicted to heroin and lived with her three children, boyfriend, and Mrs. D., her 94-year old great-grandmother. Mrs. D. was becoming very confused and had trouble remembering things. Tina began to help Mrs. D. with bill paying. Mrs. D.'s bank, in a small rural town, saw a sudden increase in checks written to Tina, some with signatures that tellers noticed did not look "right." Security contacted Adult Protective Services.

Bank statements and cancelled checks found in Mrs. D.'s home revealed that 300 checks in small amounts had been written. Seventy-five of the checks had been forged by Tina and four of her friends. All were arrested, but because Mrs. D. refused to testify against her great-granddaughter the case was not prosecuted.

Adult Protective Services helped Mrs. D. question Tina about the transactions and worked with the bank to set up a system where her accounts were protected from exploitation. The bank assists with monthly utility bill paying and has a flag on the account to check with Mrs. D. in suspicious circumstances. When Tina came to the bank recently to cash a check written to herself, the manager called Mrs. D. to see if the check was legitimate.

Tina still lives with her great-grandmother and helps with her care.

A. WHAT TO DO IF YOU SUSPECT FINANCIAL EXPLOITATION OF A CUSTOMER WHO IS IN YOUR INSTITUTION

Financial institution employees should report suspicions to security/management. They will assess the situation.

Employee awareness is the key to detecting financial exploitation. Like a person removing sunglasses in a dark room, when employees are alert to the symptoms of financial exploitation, they suddenly see cases that they would not have noticed before.

If confronted with a suspicious situation, the financial institution employee should perform the following action steps in a courteous manner.

REMEMBER: The longer you delay, the more likely the customer will recognize that something is wrong or the suspect will be frightened off.

1. LEARN THE REASON FOR LARGE TRANSACTIONS

This is especially important if the withdrawal is unusually large for the customer concerned. Ask the customer, *not* anyone with him or her, the reason for the withdrawal or change in activity. If the person with the customer does not let him or her speak, this is a red flag.

2. CHECK AUTHORIZATION TO ACT FOR CUSTOMER

If the person with the customer claims to be acting for them (or if they come in alone claiming to act for the customer), check all documentation. Exploiters often lie about their position or powers. The suspect may tell you that he or she is just helping out because the customer cannot visit the bank or credit union. Explain politely that you need verification of the customer's wishes. Some exploiters claim to be guardians or to possess a Power of Attorney. Always check documentation to be sure that the person claiming to be acting for the customer is authorized to do so. Signature cards *must always* be checked. If the signature or transaction appears suspicious, a telephone call can be made to the customer for verification.

3. PROVIDE A FRAUD/FINANCIAL EXPLOITATION ALERT FORM

Warn customers of the dangers of carrying cash. Ask them to read and sign a Fraud/Financial Exploitation Alert form. See page 17. Tell them this is a service your financial institution provides for customers' protection. Explain the form (you may want to read it aloud) and take time to answer questions.

4. GET PHOTOGRAPHIC EVIDENCE IF POSSIBLE

Photographic evidence of scams, which are carried out by strangers to the customer, is critical. A surveillance photograph may be the only way to identify the perpetrator.

Similarly, in family, acquaintance, or fiduciary exploitation, a surveillance photograph can effectively disprove a suspect's claim that he never went to the financial institution to cash the forged checks or to make withdrawals. Many experienced financial exploiters will attempt to avoid the surveillance cameras. Try to position the suspect so that the camera can get a clear image. Call the suspect over to you if necessary.

5. ASK THE CUSTOMER TO SPEAK WITH SECURITY/MANAGEMENT

If the customer, or anyone accompanying the customer, objects to your actions, politely repeat that the institution's policy is intended to protect customers. Ask the customer to speak with security/management, which can explain the reasons for your actions.

6. CONSULT WITH SECURITY/MANAGEMENT

Your financial institution will establish clear guidelines regarding the stage at which security/management *must* be notified about suspicious circumstances. However, you should feel free to consult security/management any time you feel uneasy. Your financial institution may also want you to fill in an "Incident/Suspected Abuse form," even if you were satisfied with the responses given by the customer.

7. NOTIFY SECURITY AT ONCE IF YOU FEEL THE CUSTOMER IS IN IMMEDIATE DANGER

Notify security ***immediately*** (before the customer leaves the building) if you feel there is a significant threat to his or her safety.

IMMEDIATE EMPLOYEE RESPONSE: ACTION STEPS

- Try to learn the reason for large transactions or withdrawals.
- Check authorization and documentation to act for customer.
- Provide Fraud/Financial Exploitation Alert form.
- Get photographic evidence (be able to describe suspect).
- Ask customer to speak with security/management.
- Consult with security/management at any time.
- Notify security AT ONCE if you believe the customer is in immediate danger.

REMEMBER:

- Time is the enemy of the financial exploiter.
- Justify your concern and emphasize the financial institution's commitment to protecting customers.
- Empathize with the customer and validate the customer's feelings.
- Ask clear, non-threatening, factual questions.
- Assure elderly or vulnerable customers that they are not alone (people are reluctant to reveal exploitation).
- Do not say that you are concerned simply because the customer is elderly.
- Do not let anyone else insist on speaking for an elderly or vulnerable customer. This is a "red flag" that something is wrong.

B. REPORTING SUSPECTED EXPLOITATION OF A CUSTOMER

Tellers or customer service representatives should report suspicions to security/management. Security/management will decide whether a report should be made to Adult Protective Services, the Long-Term Care Ombudsman, the police, and/or the State's Attorney. Security/management will also determine whether a Suspicious Activity Report should be made to FinCEN. While each financial institution will have its own policy and procedures, generally security/management will make the reports. The immunity statutes, however, protect any person who reports.

The system for reporting and investigating differs depending on whether the victim is an elder adult, a vulnerable adult, both, or neither. Generally, there will be a different reporting protocol for each of the four types of victims.

1. ELDER ADULTS

As of October 1, 2012, Maryland financial institutions are required to report suspected financial exploitation of elder adults, customers who are 65 or older and reside in Maryland. A reporter is provided immunity. Generally, a report must be made to the local Adult Protective Services (APS) office, law enforcement agency, and/or State's Attorney. As a practical matter, it will seldom make sense to report to the local State's Attorney, as they are not typically equipped to do investigations of this kind.

If a suspected elder financial exploitation matter appears to involve a crime in progress, e.g., repeated wire transfers for a probable swindle, the matter should be reported to the local law enforcement agency as soon as possible to thwart additional losses. If the situation does not appear to involve a clear crime in progress, security/management will decide whether to report to the local APS or law enforcement based upon a variety of factors, including whether the customer may be a vulnerable adult.

An elder-adult customer may or may not be a vulnerable adult. A vulnerable adult is someone who lacks the physical or mental capacity to provide for his or her daily needs. If the elder adult is clearly not a vulnerable adult, i.e., the elder has the mental and physical capacity to provide for his or her daily needs, a report of financial exploitation should be made to the local law enforcement agency because APS's ability to assist will be limited. (APS is authorized to investigate exploitation of vulnerable adults.) If the elder-adult customer is possibly a vulnerable adult and there is no clear crime in progress, then APS is probably the most appropriate agency to call. See Appendix A for local reporting procedures and APS numbers. APS will investigate a report and offer a range of services designed to stop any abuse. See Section IV below.

If a financial institution employee knows that the customer lives in a long-term care facility, e.g., a nursing home or assisted living facility, then the report must be made to the local Long-Term Care Ombudsman, law enforcement agency, and/or State's Attorney. (See Appendix B for local Ombudsmen Program numbers.)

When the suspected victim is an elder adult (or believed to be), a telephone report has to be made to one or more of the entities specified above within 24 hours after a financial institution employee knows or has reasonable cause to suspect that financial exploitation has occurred. A written report must follow within 3 business days.

2. VULNERABLE ADULTS LESS THAN 65

If a suspected victim of financial exploitation is possibly a vulnerable adult, but less than 65, reporting is encouraged, but not required. A report of suspected financial exploitation of a vulnerable adult under age 65 should be made to the local Adult Protective Services office. For vulnerable adults under age 65, immunity provisions protect only reports to Adult Protective Services. Whereas with elder adults, reports to the local Adult Protective Services, law enforcement, and State's Attorney are all protected by immunity provisions.

3. NEITHER VULNERABLE NOR ELDER ADULT

If the suspected victim is clearly not a vulnerable adult nor an elder adult, then the appropriate agency to contact may be the police or the Consumer Protection Division. However, contacts with the police or Consumer Protection should only be made in accordance with the financial institution's internal policies, which may require the customer's consent before contacting them. Of course, the liability protections in the vulnerable adult law and elder adult law are not applicable to situations that do not involve either an elder or vulnerable adult.

4. SUSPICIOUS ACTIVITY REPORT

There are separate standards for when to make a SAR report to FinCEN, regardless of whether the customer is an elder or vulnerable adult. If a SAR report is made, please make clear whether the suspected victim is an elder or vulnerable adult so FinCEN can gather statistics that are more helpful. Please see Appendix C for the FinCEN Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation.

5. PHYSICAL ABUSE OR NEGLECT

Financial exploitation is often found in combination with other forms of abuse. Physical abuse or neglect of a vulnerable adult should be reported to Adult Protective Services in accordance with your institution's policy. If your financial institution allows its employees to report suspected cases of physical abuse, neglect, or self-neglect, a report should not include any of the customer's financial information. Only report information contained in financial records when you believe financial exploitation has occurred.

6. FEDERAL LAWS

Under the Gramm-Leach-Bliley Act, Financial Institutions can disclose non-public personal information for the following reason:

(a) "to comply with federal, state or local laws, or rules and other applicable legal requirements" (15 U.S.C. § 6802(e)(8));

(b) "to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability" (15 U.S.C. § 6802(e)(3)(B));

(c) "to the extent specifically . . . required under other provision of law . . . for an investigation on a matter related to public safety" (15 U.S.C. § 6802(e)(5)).

In addition, the Right to Financial Privacy Act (RFPA) applies to the federal government and does not restrict the actions of state or local authorities in obtaining financial records. See 12 U.S.C. § 3401(3).

THREE STEP REPORTING PROTOCOL--VARIES BY VICTIM TYPE

VICTIM BELIEVED TO BE 65 OR OLDER AND RESIDE IN MARYLAND	**VICTIM POSSIBLY A VULNERABLE ADULT UNDER AGE 65**	**VICTIM CLEARLY NOT AN ELDER OR VULNERABLE ADULT**
Reporting Mandatory	Reporting Encouraged But Not Mandatory	Reporting Not Mandatory
1. Employee always makes oral report to security/management within 2 hours of employee's reasonable suspicion. Employee should not contact authorities unless authorized	1. Employee always makes oral report to security/management — no later than beginning of next business day. Employee should not contact APS unless authorized.	1. Employee makes oral report to security/management.
2. Security/management telephones in report within 24 hours of employee's reasonable suspicion to appropriate authorities: APS, Ombudsman, or police. Security/management: a. provides written report to authorities within three business days. The written report should include information listed in adjacent column, ------→ **and** b. submits SAR (see FinCEN Advisory 2011-A003).	2. Security/management makes oral report to APS as soon as practical. Security/management: a. provides written report to APS that includes: • Name, age (estimate), address, and telephone number of victim; • Name, relationship, and address of suspect (if known); • Description of suspicious circumstances; • Location of potential victim; **and** • Name and address of person responsible for the care of the victim (if known); **and** b. submits SAR (see FinCEN Advisory 2011-A003).	2. Security/management seeks customer consent to report to police. Security/management submits SAR, if appropriate. Contents of Any Report to Police: • Name, age (estimate), address, and telephone number of customer; • Full description of suspect; • Description of incident; • Location of incident (branch name and address); **and** • Description of suspect's car and license number (if known).
3. Written report filed by security/management for internal review and reference.	3. Written report filed by security/management for internal review and reference.	3. Written report filed by security/management for internal review and reference.

SECTION IV

FREQUENTLY ASKED QUESTIONS ABOUT ADULT PROTECTIVE SERVICES

Joe, in his seventies, contacted his local Adult Protective Services office to complain that his daughter was taking and cashing his Social Security check, and that his credit cards were at their limit. He requested that his credit union be contacted during the investigation. The same day the vice president of the credit union also made a report of suspected financial exploitation. Credit union employees had noticed that Joe's health seemed to be getting worse and that he often appeared worried and upset. They also realized there had been a dramatic increase in activity in the joint account Joe held with his daughter. The credit union had closed the account, which was seriously overdrawn, and had notified Joe by mail.

The Protective Services caseworker found that Joe had never seen this letter. His daughter was continuing to write checks on the account. Joe was also about to lose his home because his mortgage payments had not been made. Joe was denied access to his car, his mail was intercepted, and his daughter was threatening to take his medications away from him. He was being emotionally abused and financially exploited by his daughter and her boyfriend.

The vice president met with Joe and the APS caseworker. The credit union provided Joe with a printout of all activity in his account and the accompanying charges. The credit union agreed to waive the charges for bounced checks and helped Joe open a new account in his own name. Joe took out a restraining order against his daughter, accompanying the caseworker to court. The caseworker arranged to have emergency food delivered to his home until Joe was able to secure transportation to a local senior meal site. The APS caseworker also arranged for a volunteer Money Manager to help Joe with his finances.

A. What Is Adult Protective Services?

Maryland's Department of Human Resources administers and monitors a statewide system of 24 Adult Protective Services offices in each county and Baltimore City and the Abuse Referral Line (1-800-91-PREVENT) or 1-800-917-7383. The Adult Protective Services offices are part of each county's (and Baltimore City's) Department of Social Services. In Montgomery County, the local department is called the Department of Health and Human Services.

B. What Does APS Do?

1. Adult Protective Services seeks to: stabilize vulnerable adults in their own home, encourage self-sufficiency and safety, create the least disruption to lifestyle, and facilitate the least restrictive care alternatives. The primary focus is on alleviating or reducing a vulnerable adult's threatening situation by providing a variety of services and interventions.

The complexity and the differing needs of each situation require diverse interventions. For a very frail and dependent person, perhaps someone with severe Lou Gehrig's disease, who has been neglected by overburdened and/or stressed caregivers, appropriate interventions might include in-home aide services, respite care, individual or family counseling, or adult day care.

In contrast, for a healthier person, who has been financially exploited and physically abused by a grandson extorting money to support a drug habit, legal interventions, drug treatment program referrals for the grandson, or the provision of other housing options, may be more appropriate.

Adult Protective Services casework is provided without regard to income. Additional social services may also be provided at no charge to adults who are unable to pay. People who can afford additional services may be charged all or part of the cost, provided they are notified and consent to receiving services before they commence.

2. An APS Office must:

- Receive reports on a 24-hour basis.
- Investigate appropriate reports by contacting the victim in person.
- Assess the immediate needs of the victim within 24 hours of receiving an emergency report. An emergency means "a person is living in conditions which present a substantial risk of death or immediate and serious physical harm to himself or others."
- Report to the police and local State's Attorney incidents where a crime has possibly been committed.
- If abuse, neglect, self-neglect, or exploitation exists, develop a *Service Plan* that is appropriate to the functional capacity, situation and resources of the vulnerable adult.

3. Core professional services that can be provided are: intervention and counseling, coordination of services, advocacy, and court petitions. Other services that may be provided or arranged for either the victim, family caregiver, or the alleged exploiter include, but are not limited to:

- *Assistance with Finances:* bill paying assistance from trusted family members, friends, or volunteer Representative Payee programs and referral to a financial management agency for assistance in setting up trust funds;

- *Medical Services and Therapies:* in-home medical assessments or evaluations, hospitalization, and physical and speech therapy;

- *Home Health Services:* assistance with medications, home health aides, personal care nurse evaluations, and nursing and hospice services;

- *Mental Health Services:* emergency services, psychiatric services, competency evaluation, inpatient and outpatient counseling, substance abuse counseling, support groups, and crisis intervention;

- *In Home Services:* homemakers, chore services, and house maintenance;

- *Transportation:* ambulance, escort, and home care;

- *Education:* caretaking skills, job training, and employment assistance;

- *Nutrition Services:* emergency food, home delivered meals, and congregate meals;

- *Emergency , Home Energy, or Crisis Intervention Assistance:* fuel or financial assistance;

- *Socialization and Supervision:* social visits, companionship, and adult day care;

- *Institutional Placement:* long-term care and substance abuse detoxification;

- *Housing:* emergency shelters, relocation, assisted living, group home placement, and congregate housing;

- *Legal Services:* legal aid, restraining orders or injunctions against abusers, protective orders, and guardianship.

C. CAN A PERSON REFUSE HELP?

APS is sensitive to a person's right to live as he or she wants. A competent adult can refuse APS's assistance. APS cannot force a competent adult to accept its services. For example, a competent adult can refuse medical treatment and APS will not intervene to overturn that decision even if the vast majority of other people in similar circumstances would demand the medical treatment in question. However, if APS believes that an emergency situation exists, even with a competent adult, APS will contact the local police agency to have the individual transported to an appropriate health care facility.

D. WHAT MARYLAND LAWS REQUIRE REPORTING OF FINANCIAL EXPLOITATION TO ADULT PROTECTIVE SERVICES?

There are two separate Maryland statutes that require mandatory reporting of suspected financial exploitation:

1. FINANCIAL INSTITUTION EMPLOYEES

Starting October 1, 2012, Financial Institutions Article §1-306 requires financial institutions to report suspected financial exploitation of customers who are elder adults (defined as Marylanders who are 65 or older) to the local Adult Protective Services office, law enforcement, and/or State's Attorney, with one exception. If the elder adult resides in a long term care facility, e.g., a nursing home or assisted living facility, a report would be made to the local Long-Term Care Ombudsman instead of APS.

2. OTHER PROFESSIONALS

Family Law Article § 14-302 requires that certain professions (health practitioners, police officers, and human service workers) notify Adult Protective Services if they believe a vulnerable adult has been subjected to abuse, neglect, self-neglect, or exploitation.

"Abuse" means the sustaining of any physical injury by a vulnerable adult as a result of cruel or inhumane treatment or as a result of a malicious act by another person.

"Neglect" means the willful deprivation of a vulnerable adult of adequate food, clothing, essential medical treatment or habilitative therapy, shelter, or supervision.

"Self-neglect" means the inability of a vulnerable adult to provide or obtain services:

(i) that are necessary for the vulnerable adult's physical and mental health; and
(ii) the absence of which impairs or threatens the vulnerable adult's well-being.

"Exploitation" means any action which involves the misuse of a vulnerable adult's funds, property, or person.

E. DISCRETIONARY REPORTING OF FINANCIAL EXPLOITATION TO ADULT PROTECTIVE SERVICES

Before 2000, some financial institutions worried that contacting APS about customers who were financially exploited might result in the release of financial records and violate Maryland's Confidential Financial Records law. In 2000, the Maryland General Assembly passed a law clarifying that financial institutions and financial institution employees could report information to APS, including financial information, with complete immunity if they believed a vulnerable adult had been subjected to financial exploitation.

F. COMMUNICATION WITH APS

Adult Protective Services operates under statutes that require it to adhere to strict confidentiality standards. Your local APS will not be able to tell you what its investigation revealed. Sometimes financial institution employees are frustrated when, after a case has been referred to APS, they continue to see the victim influenced by the exploiter. They wonder whether the matter fell through the cracks somewhere along the line. This is unlikely, but if you encounter a situation like this report it to the appropriate person in security/management. They can call APS and ask if the case was accepted for investigation and to whom it was assigned. APS should be able to provide that information, which will confirm that the matter did not get overlooked.

SECTION V

FREQUENTLY ASKED QUESTIONS -- THE LONG-TERM CARE OMBUDSMAN PROGRAM

A. WHAT IS THE LONG TERM OMBUDSMAN PROGRAM?

The Ombudsman Program is authorized by the federal Older Americans Act as well as Maryland law. It covers facilities in all 23 counties and Baltimore City from the offices of the State's 19 area agencies on aging. See Appendix B for the local telephone numbers. Long-term care ombudsmen advocate for residents of nursing homes and assisted living facilities. While many residents receive good care in long-term care facilities, others are neglected, and other unfortunate incidents of psychological, physical, and other kinds of abuse, including financial abuse, do occur. Thus, trained staff and volunteer ombudsmen regularly visit long-term care facilities, monitor conditions and care, and provide a voice for those unable to speak for themselves. The Ombudsman Program helps residents of all ages maintain their legal rights, control over their own lives and personal dignity.

B. WHEN DOES FINANCIAL ABUSE HAVE TO BE REPORTED TO THE OMBUDSMAN?

Starting October 1, 2012, Financial Institutions Article §1-306 requires financial institutions to report suspected financial exploitation of customers who are elder adults (defined as Marylanders who are 65 or older) and who reside in a long term care facility, e.g., a nursing home or assisted living facility, to the local Long-Term Care Ombudsman, law enforcement, or State's Attorney. If the suspected exploiter works for the facility or a public agency, the entity to contact is the Ombudsman Program. See Appendix B for the correct telephone number. If the suspected exploiter does not work for the facility, a report should go to local APS, Law enforcement, or State's Attorney.

C. WHAT DO OMBUDSMEN DO?

The Ombudsman Program has many responsibilities that protect the rights and promote the well being of residents of long-term care facilities, including:

- Identifying, investigating, and resolving complaints related to any action, inaction, or decision of a provider of long-term care services, a public agency, or a health or

social service agency, that may adversely affect the health, safety, welfare, or rights of a resident;

- representing the interests of residents before governmental agencies and seeking administrative, legal, and other remedies to protect the health, safety, welfare, and rights of residents;

- providing information as appropriate to other agencies and the public regarding the problems and concerns of residents;

- informing residents, family members, and others acting on behalf of residents about how to access the assistance and services of the Program and the services and assistance of other providers or agencies, including legal services; and

- providing services to assist residents in protecting the health, safety, welfare, and rights of residents;

D. COMMUNICATION WITH OMBUDSMEN

The Ombudsman Program operates under statutes that require it to adhere to strict confidentiality standards. Your local ombudsmen will not be able to tell you what his or her investigation revealed. If your institution reports a case to the local ombudsman and you continue to see the victim influenced by the exploiter, let the appropriate security/management person know. They can call the ombudsman and ask if the complaint was accepted for investigation and to whom it was assigned. The local ombudsman should be able to provide that information, which will confirm that the matter did not get overlooked. Some cases may involve the Ombudsman referring the case to the regulatory agency, the Office of Health Care Quality, for further action.

SECTION VI

APPENDICES

APPENDIX A: **Local Adult Protective Services Reporting Procedures and Contacts For The Adult Protective Services Program**

APPENDIX B: **Local Long Term Care Ombudsman Telephone Numbers**

APPENDIX C: **FinCEN Advisory 2011-A003**

APPENDIX D: **Sample Elder Financial Abuse Reporting Form**

APPENDIX E: **Sample Cover Memo to Accompany Written Elder Financial Abuse Reports**

APPPENDIX A: LOCAL DEPARTMENT OF SOCIAL SERVICES REPORTING PROCEDURES AND CONTACTS FOR THE ADULT PROTECTIVE SERVICES PROGRAM

The following reporting procedures and contact information was provided by Maryland's Adult Protective Services Program and is current as of August 7, 2012. Please note, over time individual contacts and/or specific reporting procedures may change. As we become aware of changes, the following information sheet will be updated accordingly. A copy of this information (and any related updates) will be available on the web, including MBA's website (www.mdbankers.com) and the Maryland Department of Human Services, Adult Protective Services Program website (www.dhr.state.md.us/oas/aps).

The following information includes general call lines, as well as specific Adult Protective Services program contacts, after hour contacts, fax numbers and mailing addresses.

Call-in Reporting Procedures:

There are two primary ways in which a financial institution's security or authorized personnel can make a report of suspected financial abuse or exploitation through the Maryland Department of Human Resources' Adult Protective Services Program (APS):

(1) ***A report may be made to the Maryland Department of Human Resources by calling the General Information number (1-800-332-6347) or the Adult Abuse Referral Line (1-800-91PREVENT or 1-800-917-7383)***.

These numbers are staffed by a Customer Services state contractor on behalf of the department. When a financial institution's security or authorized personnel contacts this number, they will reach a voice active automated system. This voice active automated system will go as follows:

* Thank You for calling the Department of Human Resources
*To continue in English Press (1) or to continue in Spanish Press (2)
*For all other DHR departments please Press (4) and select from the available options
*Press (4) You have reached Customer Services, representatives are available Monday – Friday from 8:00 a.m. – 5:00 p.m.
*Press (3) to report Child Abuse or Adult Abuse & Neglect
*Press (2) for Adult Abuse & Neglect
*Caller will be transferred to a Customer Service Representative, who will ask the caller what type of report they are making, in what local department of social services did this action occur and transfer the caller directly to the specified local department offices' public telephone number. The caller will also be given the direct telephone number in case of disconnection.

Call-in Reporting Procedures (continued):

*Once the caller is transferred to the appropriate local department of social services office, caller will then be transferred to an appropriate Intake or Screening Unit Staff person who will take the report information and forward the report to the assigned Adult Services or Adult Protective Supervisor for review and assignment, if the report meets APS mandated investigation criteria to an Adult Protective case worker for investigation.

(2) ***A report may also be made by direct contacts to the local Adult Protective Services Program through the Local Department of Social Services (LDSS).***

Local Department of Social Services Offices and Adult Protective Service Program Contacts:

** Denotes After-hours coverage after normal business hours.*

ALLEGANY COUNTY DSS 1 Frederick Street Cumberland, Maryland 21502 Public: (301) 784-7000 Phone: (301) 784-7099 Fax: (301) 784-7266 After-hours: *911 Adult Services/APS Supervisor: Susan Bambacus, (301) 784-7050 ***NOTE*** The caller will receive a series of "phone tree" options and will need to select the option to report abuse, neglect or exploitation of a vulnerable adult. **After -Hours:** Reporters may call 911 to reach the county emergency dispatch. Dispatch will connect them to the ACDSS on-call worker. That worker will contact the reporter and collect the referral information. On-call workers are ACDSS employees.	***ANNE ARUNDEL COUNTY DSS*** 80 West Street Annapolis, Maryland 21401 Public: (410) 269-4500 APS Fax (410) 408-2041 After-hours: (410) 421-8400 Adult Services/APS Supervisor: Terry Mclean, (410) 897-3956 ***NOTE*** After-hours workers are DSS employees who are contacted by the answering service, who field calls at night and on weekends. A worker is supposed to call a reporter back within 30 minutes of being contacted by the answering service, to obtain their information.

BALTIMORE CITY DSS 300 Metro Plaza Adult Services Unit/APS Baltimore, Maryland 21215 Public: (443) 378-4600 Adult Services/APS: (410) 361-5000 After-hours: (410) 361-2235 APS Fax: (443) 423-6601 APS Program Manager: Tom Curtin, (443) 423-6612 Adult Services/APS Supervisor(s): Sharon Donnelly, (443) 423-6778 Ivey Scott, (443) 423-6645	***BALTIMORE COUNTY DSS*** 6401 York Road Drumcastle Government Center Baltimore, Maryland 21212 Public: (410) 853-3000 APS Intake: (410) 853-3000, Press Option #2 APS Fax: (410) 853-3599 After-hours Line: (410) 583-9398 Adult Services/APS Supervisors: LaWanda Salisbury, Intake Unit (410) 853-3541 Sharon Myers, Intake Unit (410) 853-3521 Blanche Coady, Information & Referral (410) 853-3551 ***NOTE*** The After-hours number goes directly to an answering service. The answering service will contact the social worker on coverage for APS when making a report.
CALVERT COUNTY DSS 200 Duke Street Prince Frederick, Maryland 20678 Public: 443-550-6900 Intake Line Monday – Friday , 8:00 a.m. to 5:00 p.m.: (443) 550-6969 After- hours evenings and weekends: 1-866-898-9848; (443) 550-6969 Fax: (410) 286-7429 Adult Services/APS Supervisor: Janis Pressley, (410) 550-6960 ***NOTE*** During the day (Monday through Friday), a caller should speak with an actual staff person, unless Intake staff person is already on a call. In that case, the phone system rolls-out the call, which will be answered by a back-up staff person (rotated among Adult Services and Child Welfare case workers/social workers (2-3 times per month on a 1/2-day basis). **After- hours:** A contractor takes calls and contacts the DSS Worker on call (rotated among the (1) Adult Services case worker and (4-5) Child Welfare case workers/social workers who have the experience and interest in working after-hours). They are supported by (2-3) DSS supervisors who rotate on a monthly basis.	***CAROLINE COUNTY DSS*** 207 South Third Street Denton, Maryland 21629 Public: (410) 819-4500 Adult Services/APS Fax: (410) 819-4505 After-hours: Sheriff's Dept. (410) 479-2515 Adult Services/APS Supervisor: Doreen Patrick, (410) 819-4480

CARROLL COUNTY DSS 1232 Tech Drive, Suite 1 Westminster, MD 21157 Public: (410) 386-3300 Adult Services/APS Fax: (410) 386-3429 After-hours: (410) 836-3434 Adult Services/APS Supervisor: Heather Robb, (410) 386-3384	***CECIL COUNTY DSS*** 170 East Main Street Elkton, MD 21921 Public: (410) 996-0100 Fax: (410) 996-0464 After-hours: (410) 996-5350 Adult Services/APS Supervisor: Trish Dana, (410) 996-0192
CHARLES COUNTY DSS 200 Kent Avenue La Plata, MD 20646 Public: (301) 392-6400 Fax: (301) 934-2662 APS After-hours Line: (301) 392-6724 Adult Services/APS Supervisor: Delia Meadows (301) 392-6733	***DORCHESTER COUNTY DSS*** 627 Race Street Cambridge, Maryland 21613 Public: (410) 901-4100 Fax: (410) 901-1060 After-hours: (410) 221-3246 Adult Services/APS Supervisor: Sue Todd (410) 901-4270
FREDERICK COUNTY DSS 100 East All Saints Street Frederick, Maryland 21701 Public: (301) 600-4541 APS Intake Line: (301) 600-2635 APS Fax: (301) 600-2639 After-hours: (301) 600-2464 Adult Services/APS Supervisor: Ray Brown (301) 600-4586 ***NOTE*** After-hours is handled by a Call Center through the main line (301) 600-2464. The Call Center takes down information and contacts the worker on call (handled by Child Protective Service workers). That worker in turn will contact the person who made the call and take the report. If the call is deemed an emergency then the worker contacts the APS supervisor for instruction. Otherwise, the information is taken and provided to APS the next business day.	***GARRETT COUNTY DSS*** 12578 Garrett Highway Oakland, Maryland 21550 Public: (301) 533-3000 Fax: (301) 334-5449 After-hours: (301) 533-3004 *911 Adult Services/APS Supervisor: Michael Dennis (301) 533-3060 ***NOTE*** Monday thru Friday, between 8:00 a.m. and 4:00 p.m. reports can be made by calling (301) 533-3004 (APS Hotline) or (301) 533-3040 (Services Unit). After 4:00 p.m. weekdays, on weekends, and on holidays callers will be directed to contact 911. 911 calls will be transferred to the Garrett County Sheriff's Department. Sheriff's Department will contact an after-hours, on-call worker. On-call workers are agency social workers who are trained to handle both APS and CPS situations.
HARFORD COUNTY DSS 2 South Bond Street, Suite 300 Bel Air, Maryland 21014 Public: 410-836-4717 Fax: (410) 836-4943 After-hours: (410) 838-6600 Adult Services/APS Supervisor: Christel Patton (410) 836-4739 ***NOTE*** The After-hours number is goes to the Harford County Police Department, then an After-hours CPS worker is contacted, then the APS After-hours worker is contacted.	***HOWARD COUNTY DSS*** 7121 Columbia Gateway Drive Columbia, Maryland 21046 Public: (410) 872-8700 APS Fax: (410) 872-2303 After-hours: (410) 313-2929 Adult Services/APS Supervisor: Beryl Gantt (410) 872-8807 ***NOTE*** The After-hours phone number is for the Howard County Police Department non-emergency reporting number.

KENT COUNTY DSS 350 High Street Chestertown, Maryland 21620 Public: (410) 810-7600 Fax: (410) 778-1497 After-hours: (410) 810-7600 *(410) 758-1101 Adult Services/APS Supervisor: Marti Lively (410) 810-7655 ***NOTE*** The After-hours phone number is for the Maryland State Police – Centreville Barrack.	***MONTGOMERY COUNTY DHHS*** Department of Health & Human Services 401 Hungerford Drive – 5th Floor Rockville, Maryland 20850 Public: (240) 777-4513 Fax: Adult Services/APS Intake (240) 777-1495 After-hours Intake: (240) 777-3000 Adult Services/APS Administrator: Mario Wawrzusin (240) 777-3144 ***NOTE*** After-hours: 5:00 p.m. - 8:30 a.m., Monday – Friday, Weekends and Holidays. APS referrals are handled by merit (APS screeners) staff Merit staff either at the Crisis Center w/Stand-By APS merit staff or contractors serving the same function. Weekend contractors also do CPS as well as APS.
PRINCE GEORGE'S COUNTY DSS 805 Brightseat Road Landover, Maryland 20785 Public: (301) 909-2000 APS Fax: (301) 909-2460 APS Intake: (301) 909-2228 After-hours: (301) 699-8605 Adult Services/APS Administrator: Glynda Walker (301) 909-2220	***QUEEN ANNE'S COUNTY DSS*** 125 Comet Drive Centreville, Maryland 21617 Public: (410) 758-8000 Fax: (410) 758-8110 After-hours: (410) 758-1101 Adult Services/APS Supervisor: Joyce Davis (410) 758-8038 ***NOTE*** If calls are made during business hours they will be directed to an Intake worker for Services as the staff rotate taking Intake calls.

ST MARY'S COUNTY DSS 23110 Leonard Hall Drive Leonardtown, Maryland 20650 Public: (240) 895-7000 Fax: (240) 895-7099 After-hours: (240) 895-7016 *(301) 475-8016 Adult Services/APS Administrator: Jeanne Schmitt (240) 895-7170 ***NOTE*** Our Protective Services business hours phone is answered by a person UNLESS both screeners are on the phone, in which case the caller gets an answering machine asking caller to leave a contact number so screeners can call them back. If person does not want to leave contact info, he/she is asked to call back. **After Hours**: Reporters are directed to call the county "Control Center", the emergency dispatch for all services -- law enforcement, fire, EMS, etc. The Control Center has a schedule of on-call DSS workers and supervisors and contacts the person on duty who returns call to the reporter and collects the detailed information. The on-call workers are contractual persons who do not work for this agency as regular employees. The supervision is rotated weekly by DSS supervisors.	***SOMERSET COUNTY DSS*** 30397 Mt. Vernon Road Princess Anne, Maryland 21853 Public: (410) 677-4200 Fax: (410) 677-4265 After-hours: *911 or (410) 651-0630 Adult Services/APS Supervisor: Jenny Roser (410) 677-4332 ***NOTE*** After-hours if calling in county is 911 and ask for the social worker on call. Out of county for After-hours would be (410) 651-0630 and ask for the social worker on-call.
TALBOT COUNTY DSS 301 Bay Street Easton, Maryland 21601 Public: (410) 770-4848 After-hours: *911 Fax: (410) 820-7067 or 7117 Adult Services/APS Supervisor: Debbe Fairbank (410) 770-5284 ***NOTE*** After-hours call 911 - the Maryland State Police - Easton Barrack, will contact the cell phone numbers and the name of the After- hours worker on duty.	***WASHINGTON COUNTY DSS*** 122 North Potomac Street Hagerstown, Maryland 21741 Public: (240) 420-2100 APS Intake (normal business hours): (240) 420-2155 APS After-hours: (240) 420-2222 APS Fax: (240) 420-2188 Adult Services/APS Supervisor: Nikki Snider 240-420-2160 ***NOTE*** After-hours Washington County DSS has a contract with CASA (a local agency that provides services related to domestic violence issues) to screen after-hours calls. If the CASA screener receives a call reporting abuse, neglect, or exploitation, the CASA screener calls the After-hours on-call DSS worker (either a CPS or APS worker depending on the schedule). The DSS on-call worker then follows-up with gathering more information if needed and determining the next steps to handle the report.

WICOMICO COUNTY DSS 201 Baptist Street Salisbury, Maryland 21802-2298 Public: (410) 713-3900 After-hours: (410) 713-3900 *(410) 548-4890 Fax: (410) 713-3675 Phone: (410) 713-3911 Adult Services/APS Supervisor: Pattie Jackson (410) 713-3911 ***NOTE*** The caller should dial (410) 713-3900 and then select option "5" to make an adult referral during normal business hours: Monday – Friday, 8:00 a.m. to 5:00 p.m. After normal business hours, Holidays & Weekends, the caller should call the Wicomico County Sheriff's Department, (410) 548-4890. The Sheriff's Department and our local department have an agreement to cover all After-hours CPS and APS referrals. We have CPS workers who work part-time and cover After-hour calls. The agency Services Supervisors rotates coverage for after hours supervision of the on-call staff.	***WORCESTER COUNTY DSS*** 299 Commerce Street Snow Hill, Maryland 21863 Public: (410) 677-6800 After-hours: (410) 632-1111 (Sheriff's office) Fax: (410) 677-6810 Adult Services/APS Supervisor: Becky Cornwell (410) 632-9915x173 ***NOTE*** The number for our MAP office where Adult Services is housed is (410) 632-9915. When a caller calls this number there will be a recording, Press 170 to be directed to Intake Unit.

APPPENDIX B: LOCAL LONG TERM CARE OMBUDSMAN TELEPHONE NUMBERS

ALLEGANY COUNTY
(301) 777-5970

ANNE ARUNDEL COUNTY
(410) 222-4464

BALTIMORE CITY
(410) 396-3144

BALTIMORE COUNTY
(410) 887-4200

CALVERT COUNTY
(410) 535-4606

CARROLL COUNTY
410-386-3800

CECIL COUNTY
(410) 996-8429

CHARLES COUNTY
301-934-0109

FREDERICK COUNTY
(301) 600-2877

GARRETT COUNTY
(301) 334-9431

HARFORD COUNTY
(410) 628-3025

HOWARD COUNTY
(410) 313-6423

LOWER SHORE (Dorchester, Somerset, Wicomico and Worcester)
(410) 742-0505

MONTGOMERY COUNTY
(240) 777-3369

PRINCE GEORGE'S COUNTY
(301) 265-8483

QUEEN ANNE'S COUNTY
(410) 758-0848

ST MARY'S COUNTY
(301) 475-4200

UPPER SHORE (Caroline, Kent, and Talbot)
(410) 778-6000

WASHINGTON COUNTY
(301) 790-0275

APPPENDIX C: FinCEN Advisory 2011-A003

DEPARTMENT OF THE TREASURY
FINANCIAL CRIMES ENFORCEMENT NETWORK

Advisory

FIN-2011-A003
Issued: February 22, 2011
Subject: Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation

---

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to assist the financial industry in reporting instances of financial exploitation of the elderly, a form of elder abuse.[1] Financial institutions can play a key role in addressing elder financial exploitation due to the nature of the client relationship. Often, financial institutions are quick to suspect elder financial exploitation based on bank personnel familiarity with their elderly customers. The valuable role financial institutions can play in alerting appropriate authorities to suspected elder financial exploitation has received increased attention at the state level; this focus is consistent with an upward trend at the federal level in Suspicious Activity Reports (SARs) describing instances of suspected elder financial exploitation.[2] Analysis of SARs reporting elder financial exploitation can provide critical information about specific frauds and potential trends, and can highlight abuses perpetrated against the elderly.

This advisory contains examples of "red flags" based on activity identified by various state and federal agencies and provides a common narrative term that will assist law enforcement in better identifying suspected cases of financial exploitation of the elderly reported in SARs.

Older Americans hold a high concentration of wealth as compared to the general population. In the instances where elderly individuals experience declining cognitive or physical abilities, they may find themselves more reliant on specific individuals for their physical well-being, financial management, and social interaction. While anyone can be a victim of a financial crime such as identity theft, embezzlement, and fraudulent schemes, certain elderly individuals may be particularly vulnerable.

Potential Indicators of Elder Financial Exploitation

The following red flags could indicate the existence of elder financial exploitation. This list of red flags identifies only *possible* signs of illicit activity. Financial institutions should evaluate indicators of potential financial exploitation in combination with other red flags and expected transaction activity being conducted by or on behalf of the elder. Additional investigation and analysis may be necessary to determine if the activity is suspicious.

Financial institutions may become aware of persons or entities perpetrating illicit activity against the elderly through monitoring transaction activity that is not consistent with expected behavior. In addition, financial institutions may become aware of such scams through their direct interactions with elderly customers who are being financially exploited. In many cases, branch personnel familiarity with specific victim customers may lead to identification of anomalous activity that could alert bank personnel to initiate a review of the customer activity.

- Erratic or unusual banking transactions, or changes in banking patterns:
    - Frequent large withdrawals, including daily maximum currency withdrawals from an ATM;
    - Sudden Non-Sufficient Fund activity;
    - Uncharacteristic nonpayment for services, which may indicate a loss of funds or access to funds;
    - Debit transactions that are inconsistent for the elder;
    - Uncharacteristic attempts to wire large sums of money;
    - Closing of CDs or accounts without regard to penalties.
- Interactions with customers or caregivers:
    - A caregiver or other individual shows excessive interest in the elder's finances or assets, does not allow the elder to speak for himself, or is reluctant to leave the elder's side during conversations;
    - The elder shows an unusual degree of fear or submissiveness toward a caregiver, or expresses a fear of eviction or nursing home placement if money is not given to a caretaker;
    - The financial institution is unable to speak directly with the elder, despite repeated attempts to contact him or her;
    - A new caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of the elder without proper documentation;
    - The customer moves away from existing relationships and toward new associations with other "friends" or strangers;
    - The elderly individual's financial management changes suddenly, such as through a change of power of attorney to a different family member or a new individual;
    - The elderly customer lacks knowledge about his or her financial status, or shows a sudden reluctance to discuss financial matters.

Suspicious Activity Reporting

SARs continue to be a valuable avenue for financial institutions to report elder financial exploitation. Consistent with the standard for reporting suspicious activity as provided for in 31 CFR Part 103 (future 31 CFR Chapter X), if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, the financial institution should then file a Suspicious Activity Report.[3]

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.

Elder abuse, including financial exploitation, is generally reported and investigated at the local level, with Adult Protective Services, District Attorney's offices, sheriff's offices, and police departments taking key roles. We emphasize that filers should continue to report all forms of elder abuse according to institutional policies and the requirements of state and local laws and regulations, where applicable. Financial institutions may wish to consider how their AML programs can complement their policies on reporting elder financial exploitation at the local and state level.

Financial institutions with questions or comments regarding this Advisory should contact FinCEN's Regulatory Helpline at 800-949-2732.

---

[1] Abuse and exploitation of the elderly is statutorily defined at the state level. The National Center on Elder Abuse offers the following definition of exploitation as a type of elder abuse: "the illegal taking, misuse, or concealment of funds, property, or assets of a vulnerable elder."
[2] Bank Secrecy Act data reflects increasing use of terms related to elder financial exploitation/abuse in SAR narratives.
[3] Financial institutions shall file with FinCEN to the extent and in the manner required a report of any suspicious transaction relevant to a possible violation of law or regulation. A financial institution may also file with FinCEN a Suspicious Activity Report with respect to any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by FinCEN regulations. *See, e.g.,* 31 CFR § 103.18(a) (future 31 CFR § 1020.320(a)).

APPENDIX D: SAMPLE ELDER FINANCIAL ABUSE REPORTING FORM

Note: If any item of information is unknown, enter "unknown."
Refer to page 3 for general reporting instructions.

Part I. Reporting Financial Institution Information

Employee Name (Last name first):
Title:
Telephone and E-mail:
Name of Financial Institution Employer:
Address of Financial Institution, City, State, Zip:
Address of Branch/Office location where observation occurred or knowledge/suspicion arose:

Part II. Suspected Victim Information

Name (Last name first):
Age (approximate if not known):
Date of Birth (if known):
Address (If Long-Term Care Facility, include name and notify ombudsman), City, State, Zip
Telephone:
Present Location (if different from above), City, State, Zip:
Telephone:
Name and address of person responsible for care of the victim (if known):

Part III. Suspected Perpetrator Information

Name (last name first):
Address:
Telephone:
Present Location (if different than above):
Relationship to suspected victim:
Description of suspected perpetrator:

Part IV. Incident Information (Observation, Obtaining Knowledge of Unusual Circumstances, Etc.)

Date/Time of Incident(s):
Address/location where incident(s) occurred:

Description of Incident (please include pertinent details such as): • The events/activities that lead to reasonable belief there may be financial abuse • Who, what, where, when, how • The suspected financial abuse

Part V. Information Regarding Telephone Report (Must be made within 24 Hours of Knowledge or Suspicion of Financial Abuse):

Name of Official Contacted:
Name of Agency:
Telephone Number Contacted:
Date and Time Telephone Report was Made:
Address, Fax, and/or e-mail of Agency:
Details included in Telephone Report (if they differ from incident information listed in Part IV):

Part VI. Written Report (Must be made within 3 Business Days of Knowledge or Suspicion of Financial Abuse):

Name of Official to whom written report was given:
Name of Agency:
Telephone Number
Address, Fax, and/or e-mail of Agency:
Date Written Report was Made (check which contact method applies and include related date): ☐ Mailed: ☐ Faxed: ☐ E-mailed:
Details included in Written Report (if they differ from incident information listed in Part IV):

Sample Elder Financial Abuse Reporting Form and related General Instructions were developed by the Maryland Bankers Association with input from the Maryland Department of Aging and Adult Protective Services Program

Maryland Report of Elder Financial Abuse
General Instructions

Purpose of Form: This form documents the information given by the reporting party on the known or suspected incident of financial abuse of an elder.

Maryland's Suspected Elder Abuse Reporting Requirements: Chapters 325/324 of the 2012 Laws of Maryland (codified primarily at Annotated Code of Maryland, Financial Institution, Section 1–305 and 1–306) amend Maryland's Confidential Financial Records Act to better protect "elder adults." The law requires banks and credit unions to report to specified agencies known or suspected "financial abuse" of elders. "Elders" are defined as Maryland residents who are at least 65 years of age. In general, "financial abuse" is taking property of an elder adult for a wrongful purpose or with intent to defraud. Specifically, the law defines "financial abuse" as to take, appropriate, obtain, or retain, or assist in taking, appropriating, obtaining, or retaining, real or personal property of an elder adult by any means, including undue influence, for a wrongful purpose or with intent to defraud the elder adult.

When Reporting is Required: Financial institutions must make an oral and written abuse report if an employee, while acting within the scope of employment, has (1) direct contact with an elder adult or reviews or approves an elder adult's financial documents, records, or transactions in connection with financial services provided to or for the elder adult; and (2) observes or obtains knowledge of unusual circumstances that lead the employee to know or have reasonable cause to suspect that the elder adult is the victim of financial abuse. An employee is anyone with a full or part-time job, who has contact with a customer or a customer's financial records. Examples include tellers, customer services representatives, managers, computer operators, etc. It does not include independent contractors.

Reporting Responsibilities: The appropriate staff person for the financial institution shall complete this form for each report of a known of suspected incident of elder financial abuse. ***Note:***

- **A telephone report must be made within 24 hours after a financial institution employee knows or has reasonable cause to suspect that financial abuse has occurred; and**

- **A written report must be made within three (3) business days after the financial institution employee knows or has reasonable cause to suspect financial abuse has occurred.**

- Telephone and written reports must be submitted ***to one*** of the responsible agencies identified below:

    - adult protective services program in a local department of social services agency,
    - the local law enforcement agency,
    - ***or*** a State's Attorney.

If the reporter knows that the elder adult resides in a long-term care facility located in the State, the abuse report must be submitted to:

- an ombudsman for the facility,
- the local law enforcement agency, ***or***
- a State's Attorney.

Liability Protection for Reporters: A financial institution and its employees are immune from civil and criminal liability that would otherwise result from an action or omission involved in making a report or disclosure, participating in an investigation resulting from a report, or declining to provide information on whether a report has been filed.

Failure to Report: A failure by a financial institution to file an abuse report concerning an elder adult is punishable by a civil penalty of up to $1,000 or, if the failure is willful, a civil penalty of up to $5,000. Any civil penalties may only be recovered in a civil action by the Attorney General against the financial institution and must be paid by the financial institution.

Disclosure of Report: A financial abuse report is confidential and disclosure of the information in a report is allowed only to the identified responsible agencies or as authorized by the elder adult. An unauthorized disclosure of information contained in an abuse report is a misdemeanor and punishable by a fine of up to $500.

Sample Elder Financial Abuse Reporting Form and related General Instructions were developed by the Maryland Bankers Association with input from the Maryland Department of Aging and Adult Protective Services Program

www.mdbankers.com • 186 Duke of Gloucester Street Annapolis, MD 21401 • 800.327.5977

EXHIBIT E: SAMPLE COVER MEMO TO ACCOMPANY WRITTEN ELDER FINANCIAL ABUSE REPORTS

To: _____

From: _____

Date: _____

RE: Written Report of Elder Financial Abuse Incident on _____[date]

An employee of [name of financial institution] observed or obtained knowledge of an actual or suspected case of financial elder abuse on the date shown above.

In accordance with Maryland Chapters 325/324, attached is a copy of [name of financial institution]'s written elder financial abuse incident report. This incident was reported by telephone as stated in the written report.

The relevant details of the elder financial abuse incident are included in the attached report. Please contact [name of appropriate staff person] at [phone / e-mail], if you have questions.

Thank you,

Name: _____
Title: _____
Financial Institution: _____
Telephone Number: _____
Fax Number: _____
E-mail: _____
Address: _____

Sample cover Memo to Accompany Written Elder Financial Abuse Reports was developed by the Maryland Bankers Association