Financial Exploitation Investigative Guide for Law Enforcement

The Financial Exploitation (FE) Investigative Guide was developed to aid law enforcement and others investigating allegations of elder financial abuse. It is intended that the users of this investigative guide will avail themselves of only those sections of the guide that relate to their specific allegation.

Each investigation is unique, and no guide can predict all the steps that a particular investigation may need. Some suggested steps may not relate to your investigation while other steps pertinent to your investigation may need to be added.

Bank Information

- Obtain information from the financial institution. The suggested wording and the documents to request are discussed in ***Requests to Financial Institutions***.
- When the financial documents are received, review the information for completeness and confirm that all requested information was received.
- Review the information to determine if anyone has been added to the accounts as either an owner or a signatory, and if the address has changed. All yes answers should be discussed with the victim to determine the reason(s) for the changes and additions.
- If you wish to perform a high-level review of the account to see if there are patterns that might indicate financial exploitation, use the test that best suits the level of account activity and the statement format. Please note that the *Monthly Bank Statement Analysis* is better suited for some banks than others. It depends on the bank statement format.
    - For savings, investment, or other accounts with little overall activity, schedule out the period ending date and account balance at that time. To see the overall shape of the data, create a line graph of the information. (Instructions to quickly create a line graph, ***see*** (reference to data visualization material.)
    - For checking and other accounts with a lot of activity, schedule the activity in the ***Monthly Statement Analysis*** spreadsheet. This spreadsheet can show trends in changes of banking, and dollar amounts in deposits and withdrawals by type.
    - If the statements are not suited for the Monthly Statement Analysis, schedule out the deposits and withdrawals for each period, and create a clustered column chart or two column charts (one each for deposits and withdrawals). (Instructions to quickly create a line graph, ***see*** (reference to data visualization material.)
- If the entire statements will be analyzed, it is recommended that the statements be converted into an Excel or other software spreadsheet. The ***Detailed Review Worksheet*** can be used as a template. One worksheet per account. Once all the data is entered into the *Detailed Review Worksheet*, it is recommend saving a copy of the file as a master file, not to be touched unless needed.

- Review deposits in the *Detailed Review Worksheet* for:
    - Missing or diverted revenue
    - Proceeds of disposed assets
    - Deposits from unknown sources
    - Deposits made by the alleged perpetrator

- Review the deposit material for the source of the deposits and to determine if there were any split deposits. Split deposits are indicated by the phrase "cash out". For all split deposits, determine who received the cash and why.
- Review the withdrawals in the *Detailed Review Worksheet* for:
    - Questionable payee and amounts. This includes:
        - Identify checks made payable to cash.
        - Payee that doesn't make sense for the older adult.
        - Payee whose services are unfamiliar.
        - Payments to vendors that bill monthly but are paid more frequently than that.
        - Payments to "boyfriend, girlfriend, new acquaintance" or power of attorney.
        - Payments to the same vendor but with different account references.
        - Credit cards or utility bills that are paid infrequently.
        - Significant increase in monthly expenses paid.
        - Payments to caregiver or family members above agreed upon amount or frequency.
        - Items or services that weren't previously purchased.
    - Expenses that do not agree with the victim's description of their expenses, credit card usage, etc.
    - Large dollar value or recurring payment amounts. Is the payee appropriate? For recurring payments, the payee may be a deceptive business.
    - New payment types that may indicate that someone new is handling the finances or is using a debit card/ bank information without permission. Note that many people adopted mobile and online banking when the paramedic began in 2020.
- Review any out-of-sync check numbers. These are check numbers that are outliers to the other check numbers paid during the month. The easiest way to perform this test is to look at the bank statements. Each month there is a list of the check numbers that were processed. Out-of-sync checks could indicate that someone stole those checks from the victim's checkbook or check stock, someone obtained new checks for the account using a different set of check numbers, or that the victim misplaced their checkbook and used a check from their check stock.
- For Transfers out of the account:
    - Determine who owns the account that received the funds. List this account in the "offset" column.
    - If the money is transferred into a *known* account held be the victim, the transfer can be removed from the list of questionable expenditures because the money still is an asset to the victim.
    - If the money is transferred into an *unknown* account held by the victim, keep on the transfers on the list and send a request to the financial institution for the new account. Once it can be confirmed that the victim is the actual owner of the account, which received the funds, these

transfers can be removed from the list of questionable expenditures. Review the new account statements for questionable / suspect transactions.

- Obtain the vendor's records of the transactions if necessary to determine how the funds were applied or what was purchased.
- Review list of questionable and suspect expenditures with the victim. If the victim cannot provide an explanation, ask who made the purchase / who had the opportunity to make the purchase. Be aware of characteristics of scams (discussed below) when reviewing expenditures with the victim.
- For the purposes of presenting the information to the District Attorney's Office, it may be useful to group transactions by commonality (ATM withdrawals, cash payments to the perpetrator, etc.) or by the crimes codes section which may apply.

Credit Cards

For each credit card:

- Obtain credit card statements. (***See***: Request to credit card companies)
- Review statements for propriety and schedule out questionable expenditures. (***See*** Credit Card Spreadsheet). Red flags related to credit card purchases listed below. (***See*** Red Flags of FE)
  - Cash advances or check withdrawals with no prior history of such use.
  - Large credit card transactions and/or unusual increase in credit card debt.
  - Abrupt increase in credit card activity.
  - Expenses that are unusual for the victim.
  - Purchases made from vendors that are unusual for the victim.
  - Items or services being purchased that weren't typically purchased in the past by the victim.
  - Purchases in locations that are unusual for the victim.
- Determine from the victim who has / had control of the credit cards during the time period under review.

Credit Reports

Everyone can obtain a free credit report from each of the three credit reporting agencies once during a 12-month period. All three of reports can be ordered at once or spaced out over the course of the year. It is recommended that the free reports be staggered over the year.

There's only one official source, authorized by federal law and sponsored by the three major bureaus: AnnualCreditReport.com. This website does not ask for payment, although you may see ads for paid credit monitoring services. **If you're being asked to pay to see your reports, you may have accidentally gone to an imposter website.**

The credit reports can be requested online, over the phone, or by mail. The first two methods require the requestor to answer security questions based upon the individual's credit report. If requesting by mail, it is recommended to use certified mail or a tracking number when mailing in a request. Either service can be used to confirm that receipt of your request by the credit reporting bureau. Specific contact details for each method are found at annualcreditreport.com/gettingReports.action

Identity Theft[1]

During the investigation, be alert for indicators of identity theft. Section 4120 of the Pennsylvania Crimes Code defines identity theft as, "A person commits the offense of identity theft of another person if he possesses or uses, through any means, identifying information of another person without the consent of that other person to further any unlawful purpose.

The Crimes Code contains the following definitions:

"Identifying information." Any document, photographic, pictorial or computer image of another person, or any fact used to establish identity, including, but not limited to, a name, birth date, Social Security number, driver's license number, nondriver governmental identification number, telephone number, checking account number, savings account number, student identification number, employee or payroll number or electronic signature.

"**Document**." Any writing, including, but not limited to, birth certificate, Social Security card, driver's license, nondriver government-issued identification card, baptismal certificate, access device card, employee identification card, school identification card or other identifying information recorded by any other method, including, but not limited to, information stored on any computer, computer disc, computer printout, computer system, or part thereof, or by any other mechanical or electronic means.

Perpetrator's Financial Records

When reviewing the perpetrator's financial records, the items to review include, but are not limited to, the following:

- Deposits that match withdrawals or checks written from the victim's account.
- Lack of withdrawal activity that one would expect from an adult (no rent or mortgage payments, no ATM withdrawals, no payments for typical bills). These expenses could be being paid from the victim's accounts.
- Conversely, habitual spending beyond the suspect's discernible income. How is this being financed?

[1] The information in this section is current as of March 31, 2020.

Power of Attorney Documents

With a power of attorney (POA) document, one person, known as the principal, authorizes another person, the agent, to act on the principals behalf. The permitted duties the agent can undertake are outlined in the document and in the Pennsylvania Power of Attorney Act (20 Pa. C.S. § 5601 et seq.)

In regards to the Agent's duties, § 5601.3 of the PA Power of Attorney Act states includes the following general rule:

> Notwithstanding any provision in the power of attorney, an agent that has accepted appointment shall:
>
> (1) Act in accordance with the principal's reasonable expectations to the extent actually known by the agent and, otherwise, in the principal's best interest.
> (2) Act in good faith.
> (3) Act only within the scope of authority granted in the power of attorney.

Do not take anyone's word that they are the power of attorney agent. Obtain the document.

The PA Power of Attorney Act requires the POA document to contain certain items to be a valid document.

- Does the document contain the required Acknowledgement/Warning Notice signed by the victim? This is in all capitals and is the first page of the document.
- Does the document contain the required Acknowledgement signed by the agent?
- For POA documents signed after January 1, 2015, was the document witnessed by two people, neither of whom is the agent?
- For POA documents signed after January 1, 2015, was the document notarized?
  Note: POA's executed before January 1, 2015, are still valid without being notarized or witnessed and containing the old acknowledgement forms.

Other items to consider when reviewing a POA document.

- Does the document appear to be signed by the victim based on comparison to other signature samples?
- Did the victim have capacity on the date the document was signed?

When reviewing the principal/ Victim's financial records:

- Does the agent appear to be acting in the best interest of the victim?
- If the agent is writing checks to him/herself or other individuals – does the document allow for gifting?
  - Limited Gifting – limited to the federal gift tax exemption amount (see IRS guideline) and only to certain family members

- Unlimited Gifting – the document must specify guidance on how the unlimited gifting is to be carried out.

- Are there any evidence of financial exploitation? ***Red Flags of Financial Exploitation*** contains a section relating to fiduciaries.

Real Property

For each property:

- Find who currently owns the property through the tax assessment office or the Recorder of Deeds office in the county where the property is located (public information).
- If no longer owned by victim or if with a new joint owner(s), obtain copy of deed (public information).
  - Does the victim's signature appear to be forged?
  - Did the power of attorney (POA) agent sign for the victim?
  - If the property was refinanced when the new joint owners were added to the deed, are those new owners listed as co-borrowers on the mortgage?
  - Confirm sale with the victim.
- Review sales price for reasonableness. (Comparable prices can be found on Real estate websites such as Zillow.com.)
- Verify sale proceeds were deposited into victim's account or used for the victim's benefit.
- It may be necessary to obtain the settlement sheet to see how the sale proceeds were distributed e.g., mortgage holder, seller, back taxes. Settlement sheets can be obtained from the victim, their real estate agent who handled the sale or the title company. The title company may be listed on the deed filed with the Recorder of Deeds.
- If the home is still owned by victim, are there any liens or mortgages on the property? Obtain copy.
  - Does the victim's signature appear to be forged?
  - Did the POA sign for the victim?
  - Were the proceeds deposited into the victim's account?
  - Confirm liens / mortgages with the victim.
- For suspicious real estate transactions:
  - What was the relationship between the victim and the buyer?
  - Was the victim mentally capable of understanding the transaction?
  - Did the buyer promise anything to the victim in exchange for the sale?
  - Obtain all paperwork documenting the transaction.
- If the victim owns a rental property, are the rental payments being deposited into the victim's account?

Occasionally financial exploitation can result in the victim losing their real property and /or being evicted. Listed below are some situations that can result in loss of property / eviction. If the victim needs assistance, and is 60 or older, please contact your local Area Agency on Aging.

- There are unpaid taxes.
- The property is listed in a sheriff's or other government property sale announcement.
- The victim sold or gave their home to someone with the understanding that the victim could stay there, and there is not a written tenancy agreement documenting this agreement.

Scams

The variety of scams committed against victims of any age is endless. When talking to a victim or reviewing their financial records, please be aware for characteristics of common scams such as:

- Threatening to take action against the victim, e.g. legal action/ arrest / credit report if they don't send money.
- Requiring the victim to pay money in order to receive a prize or lottery winning.
- Offering deals too good to be true, "high-profit, low risk."
- Pressuring the victim into making a quick decision to invest / purchase something.
- Telling the victim to keep the deal or conversation quiet and not tell anyone.
- Requiring the victim to send money by wire transfer / money order / gift cards.
- Failing to perform work paid by the victim.
- Doing subpar work that has already been paid for by the victim.

IMPORTANT: If someone reports that money was just mailed as part of a scam, obtain as much information as possible regarding the date, the address of the receiver, the address of the person mailing the item, a description of the item, and tracking or other identifying number. Immediately contact the delivery company. For items mailed through the United States Post Office, contact the local postal inspectors. There is a brief opportunity to intercept the package / envelope.