

SAFTA

SENIOR ABUSE FINANCIAL TRACKING AND ACCOUNTING

GUIDE



SAFTA was produced by the International Association of Chiefs of Police (IACP), with assistance from Webber CPA, PLLC and the National White Collar Crime Center (NW3C), and supported by the Elder Justice Initiative, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in SAFTA are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The objective of the Senior Abuse Financial Tracking and Accounting (SAFTA) Tool is to provide law enforcement with a simplified method for investigating suspicious financial patterns and prosecuting cases of suspected financial exploitation of older adults. This SAFTA Guide provides strategies for navigating the following phases of a financial exploitation investigation with easy-to-use templates and helpful tips.

PHASE	TEMPLATE	PAGE NO.
Identifying Financial Exploitation	• Questionnaire	2
Gathering Financial Records	• Standard Request Form	3
Analyzing Bank Statements	• SAFTA Tool	4

This Guide and related resources are available online at <https://www.theiacp.org/elder-abuse>.

For questions, comments, and training on the SAFTA Tool, please contact Jim Foley, Vice President, Training and Curriculum Development, National White Collar Crime Center: jfoley@nw3c.org.

NOTE REGARDING SECURITY: The SAFTA Tool is a downloadable file that resides on your (the user's) device or network. Any data entered is stored on your device or network, and not by International Association of Chiefs of Police (IACP) or the National White Collar Crime Center (NW3C). Password features within the file offer additional security as explained on page 5 of this Guide.

Identifying Financial Exploitation

Over 35 states have a [criminal financial exploitation statute](#), although there is tremendous variability in the statutory language. Each state's statute and possible charges can be found in the Elder Abuse Guide for Law Enforcement ([EAGLE](#)) available at eagle.trea.usc.edu/.

Financial exploitation often co-occurs with other forms of abuse such as physical, sexual, emotional, or neglect, and only comes to light after an investigation begins. Rarely do people report to police that they have been a victim of financial exploitation. Screening for possible financial exploitation should be standard procedure for investigating allegations of abuse of any kind against older adults. While a "yes" to any of the questions below could simply indicate that an older adult is no longer able to manage daily activities independently, it might also signal wrongdoing and abuse.

Questions for the alleged victim:

- Do you have any concerns/worries about your care or finances?
- Do you lack (need) food or any necessities?
- Are you missing any medication?
- Are you missing any valuable or sentimental property?
- Have you recently sold any property?
- Has anyone asked you to sign any legal paperwork recently?
- Are any of your (rent, mortgage, utility) bills late or in arrears?
- Does anyone prevent (keep) you from accessing your bank account, credit card, check book, or monthly statements?
- Do you notice any unauthorized (or strange) transactions in your statements?
- Do you have any new loans, credit card(s), or debt?
- Have you been the victim of a scam?
- Has anyone asked you to co-sign or help them with a loan such as a car loan or mortgage?

Questions for involved parties (directly or indirectly):

- Have the older adult's living arrangements changed?
- Have you noticed any new relatives or companions?
- Has the older adult expressed any concerns about care or finances?
- Have you witnessed any strange activity at the older adult's residence?
- Have you noticed a change in the older adult's appearance or demeanor (behavior)?

Observations in the home:

- Isolation from family, friends, or other resources
- Lack of food, poor hygiene or inappropriate clothing
- Multiple phone calls from unknown persons
- Unopened mail, unpaid bills, eviction or foreclosure notices
- Hoarding
- Disparity in living situation between the older adult and others in the home (safety, comfort, health)
- Reliance on or deference to others for answers to questions, care, or financial decisions

KEEP IN MIND

To counteract ageism, consider using the term "older adult" instead of "elder" when communicating with a potential victim of financial exploitation. Older adults may have cognitive impairments that affect their ability to answer certain questions accurately, if at all.

However, a dementia diagnosis doesn't mean you can't trust anything the older adult says. It's important to understand that there is considerable variability in the symptoms associated with dementia and consideration must be given to their responses.

For more information on dementia and Alzheimer's please visit the [Alzheimer's Association](#) and read about tips on [communicating with someone who has dementia](#).

Gathering Financial Records

Financial records are the most important piece of any financial exploitation investigation. Legal process (subpoena or search warrant) can be used to obtain account information from the bank(s) or credit union(s) where the victim and the suspect maintain checking and/or savings accounts. Developed for adult protective services (APS), you may also access [National Guidelines for Financial Institutions: Working Together to Protect Older Persons from Financial Abuse](#), which contains sample record request forms.

However, investigators should first try to obtain these records with the account holder's consent. For best results, consider requesting:

- Monthly statements for *any and all* accounts held individually and jointly by the alleged victim*
- Copies of supporting records for each account, including:
 - Signature cards and account opening/change records
 - Deposit items
 - Canceled checks (front and back)
 - Withdrawal slips
 - Wire transfer details
 - Teller notes
 - Power of Attorney
- Loans, line of credit, and/or credit card statements and documents

Additional records helpful to an investigation of financial exploitation include:

- Investment/retirement account statements and records
- Tax returns
- Credit report(s)
- Social Security statement
- Public record search results
- Hospital/facility records
- Power of Attorney documents
- Health Care Proxy forms
- Last Will and Testament
- Trust documents
- Life insurance policies
- Vehicle titles
- Property appraisals and titles
- Adult Protective Services case files
- Suspicious Activity Reports (SARs)

Pro Tip:

Obtaining a credit report or tax return is a good source for finding additional accounts the alleged victim might have.

*If you know when the suspected perpetrator became involved with the victim's finances, consider requesting six months prior to that time to gain an understanding of the victim's usual financial activities prior to the alleged exploitation. This will be important when demonstrating changes in financial behavior after the suspect became involved; aberrant patterns after this date may be more easily attributed to the suspect. One of the features of the SAFTA Tool allows you to include this date on your charts and graphs as a visual aid. See page 16 for instructions on how to do this.

FAST TRACK

Two editable subpoena templates that contain this information are available for download on the SAFTA site. [Click](#), or copy and paste the following link in your internet browser:
<https://www.theiacp.org/elder-abuse>

Financial institutions differ in how they process a subpoena. Therefore, it is important to confirm the appropriate address and point of contact person with the financial institution before sending the subpoena to avoid unnecessary delays.

A Note About SARs:

SARs are available to law enforcement personnel via each state's FinCEN coordinator and are subject to strict confidentiality rules. Discuss your case with a prosecutor before using a SAR.

Follow the Money: Analyzing Bank Statements

Once you have received the statements and supporting records from the financial institution, the real investigation begins, and you're ready to enter data! Analyzing financial institution records is the most important piece of a financial exploitation case puzzle.

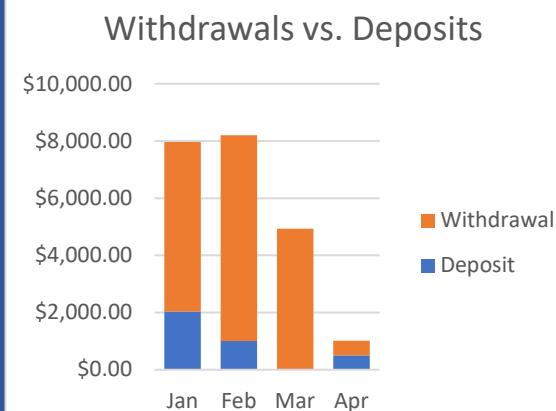
The SAFTA Tool is available for download on the [IACP's Elder Abuse webpage \(https://www.theiacp.org/elder-abuse\)](https://www.theiacp.org/elder-abuse), and this section of the Guide will walk you through the data entry and analysis process.

Step 1: Laying the Foundation

Excel Basics

Microsoft Excel is a powerful tool for analyzing financial data. The SAFTA Tool is a Microsoft Excel macro-enabled workbook that allows users to sort, filter, and summarize transactions from a victim's or suspect's bank statements by date, category, or other important characteristic, so that patterns are more easily observable.

Excel workbooks are composed of multiple worksheets, which are accessible using the tabs across the bottom of the workbook. Each worksheet is composed of individual cells (or blocks) which are organized by columns, labeled alphabetically across the top of the worksheet, and rows, labeled numerically down the left side of the worksheet. For purposes of this tool, users are restricted from entering data directly in cells to protect the code written into the tool. This special code creates the customized dialog boxes, prompts, and formulas (called "macros") that guide users through the tool. Data is entered into the workbook via dialog boxes and prompts so that users who are not familiar with Excel can navigate the tool successfully.



Recognizing patterns and demonstrating changes in those patterns are the most crucial pieces of evidence in a financial exploitation case. In this scenario, the alleged victim saw a sudden drop in both income (i.e. deposits) and spending (withdrawals) which is a suspicious change in behavior.

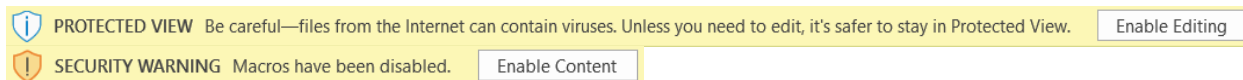
This chart is just one of the chart options available as part of the SAFTA Tool. Learn more about how to create charts and graphs on page 15.

! Reminder!

SAVE YOUR EXCEL FILE REGULARLY TO AVOID DATA LOSS. CONSIDER ENABLING AUTO-SAVE IN YOUR SETTING PREFERENCES. FOR INSTRUCTIONS, WATCH [HTTPS://YOUTU.BE/TGJLHXBLF1A](https://youtu.be/TGJLHXBLF1A).

Getting Started

To get started, open the SAFTA Tool workbook. Depending on your computer settings, you may have to click “Enable Editing” and/or “Enable Content” in the top ribbon before you begin.



When setting up a new workbook, it will request that you “Add New User.” You, the user, will create a user name and password the first time you open SAFTA. The **user name** must contain at least six characters. The **password** must contain:

- one upper case letter
- one lower case letter
- one number or special character
- at least eight total characters

Create a new user name and password and choose the type of user: “Admin” or “Normal”. Admin access allows users to set control and customization features for the SAFTA Tool, while Normal access allows users only the data entry and analysis features of the SAFTA Tool. The first user that you add to the workbook should be an Admin. Passwords cannot be recovered, so maintain each in a secure location.

A screenshot of the "Add New User" dialog box. The title bar says "Add New User" with a close button. The main heading is "Add New User". Below it, instructions state: "Username must be at least 6 characters" and "Password must have a lowercase and uppercase letter and a non alpha-numeric character". There are two input fields: "New User Name:" and "Password:". Below these is a "User Type" section with two radio buttons: "Admin" and "Normal User". At the bottom is an "Add New User" button.

Once the appropriate credentials are entered, click the “Add New User” button and the workbook will display the “Introductory Menu” on the Welcome Tab.

The Welcome Tab is an introductory menu showing nine buttons that will help you navigate the SAFTA Tool. The first six of these buttons, “**Enter Case Details**” through “**Dashboard**,” are the key functions of the SAFTA Tool and require data entry from the financial records collected by the investigators. The following pages are a step by step guide to using the key functions of the SAFTA Tool.




The Enter Case details button calls up a dialog box where you can enter basic information about your case, such as:

- Case Number (Maximum of 11 characters)
- Victim’s Name
- Lead Investigator
- Notes
- Investigation Start
- End Date of Investigation
- Number of Suspects

To navigate to the next field of each dialog box throughout the SAFTA Tool, use the “Tab” key on your keyboard. Click the button at the bottom of each dialog box to save the information you entered and close the dialog box.

You can review the Case Details entered at any time by selecting the Case Details Tab at the bottom of the workbook. You can edit or update the case details at any time by choosing “Enter Case Details” from the Welcome Tab.




Suspect and Victim Data
Entry

The Suspect and Victim Data Entry Tab calls up a dialog box where you can enter demographic information about the Victim and Suspect(s) in your case, such as:

- Name
- Address
- Telephone
- Gender
- Date of Birth

Additional fields exist to enter victim information such as Power of Attorney or representative payee detail, referral source, and summary of abuse; and suspect information such as relationship to the victim and duration of the relationship.

After clicking “Input Data,” an additional dialog box will appear asking “Would you like to input another Suspect or Victim?” Select “Yes” to input another victim or suspect, or select “No” to close the dialog box and proceed with entering bank account information.



Enter Bank Account
Information

The Enter Bank Account Information Button calls up a dialog box where you can enter specific account details such as:

- Account Number (maximum 13 characters)
- Financial Institution
- Account Type
- Account Owners
- Owner Type
 - Victim
 - Suspect
 - Both
 - Unknown
 - Other

Once you click the “Input Account Summary” button at the bottom of the dialog box, two tabs will be created to host the data for that account, and another dialog box will appear asking you whether you want to add another account. You can add as many accounts as you need. It is recommended that one SAFTA Tool is used for the victim’s accounts, and a separate SAFTA Tool for the suspect’s accounts. Additionally, to keep the tab titles short, it is recommended that you use the last four numbers of an account and an abbreviation of the banking institution (ex. If the account number is 0123456789 from Bank XYZ, you might use 6789 or XYZ6789). Abbreviating is especially helpful if you are adding multiple accounts.

**Enter Monthly Bank
Statement Summary Data**

The first page of a bank statement usually contains summary information such as the total deposits, withdrawals, checks, fees, or other types of transactions that took place in the account during the calendar period covered by the statement, such as a month, quarter, or year. The “Enter Monthly Bank Statement Summary Data” button on the Welcome Tab calls up a dialog box that prompts the user to enter that summary information from each statement. First, select an account that you added in the previous step related to the information you want to enter.

For each statement you review, enter the following summary data elements (if given on the face of the statement) using the dialog box:

-
- Statement Date
- Beginning Balance
- Deposits
- Transfers In
- ATM Withdrawals
- Checks
- Debit Card Purchases
- Transfers Out
- Other Withdrawals
- Ending Balance

Remember:
To navigate to the next field of each dialog box throughout the SAFTA Tool, use the “Tab” key on your keyboard .

Each entry automatically populates a row on a newly created “Statement Summary” tab for the account being examined. When finished, your Statement Summary tab will show all the summary information entered for that account.

Viewing the summarized information chronologically reveals patterns that may not have been so easily visible otherwise. For example, a user might interpret from the populated Statement Summary tab below that:

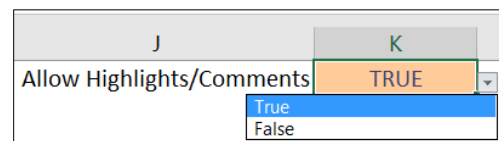
- The victim maintains an \$11,000 account balance, on average, from month to month
- He withdraws \$600-800 per month cash at the ATM, with some exceptions, but this seems to jump to over \$1,000 consistently by December 2011 when the suspect moved in
- Check spending varies, so we'll probably want to take a closer look at where these funds are being spent

Statement Date	Beginning Balance	Deposits	Transfers In	ATM Withdrawals	Checks	Debit Card Purchases	Transfers Out	Other Withdrawals	Ending Balance	
01/13/2011	11657.94	3730.00		800.00	3017.44				11570.50	Remove Line?
02/13/2011	11570.50	3730.00		800.00	2922.92				11577.58	Remove Line?
03/13/2011	11577.58	3730.00		600.00	2270.40			194.19	12242.99	Remove Line?
04/13/2011	12242.99	3730.00		1200.00	2654.50			186.41	11932.08	Remove Line?
05/15/2011	11932.08	3730.00		800.00	2774.07				12088.01	Remove Line?
06/13/2011	12088.01	3730.00		1000.00	2415.35			132.52	12270.14	Remove Line?
07/13/2011	12270.14	3730.00		1020.00	3322.49				11657.65	Remove Line?
08/14/2011	11657.65	3730.00		820.00	6841.20			69.79	7656.66	Remove Line?
09/13/2011	7656.66	3730.00		220.00	2152.71			34.48	8979.47	Remove Line?
10/13/2011	8979.47	3730.00		1020.00	2800.80				8888.67	Remove Line?
11/13/2011	8888.67	3730.00		600.00	1472.71			80.65	10465.31	Remove Line?
12/13/2011	10465.31	3730.00		1400.00	2472.81			173.09	10149.41	Remove Line?
01/13/2012	10149.41	3878.00		1400.00	1108.05			140.68	11378.68	Remove Line?
02/13/2012	11378.68	3878.00		1400.00	3315.80			51.56	10489.32	Remove Line?
03/13/2012	10489.32	3878.00		1000.00	3495.94			189.80	9741.58	Remove Line?
04/13/2012	9741.58	3878.00		1200.00	2403.51				10016.07	Remove Line?
05/11/2012	10016.07	3878.00		1000.00	1611.23			99.92	11182.92	Remove Line?
06/13/2012	11182.92	5663.00		1600.00	3959.75			51.34	11234.83	Remove Line?
07/15/2012	11234.83	3663.00		1000.00	2452.95				11444.88	Remove Line?
08/13/2012	11444.88	3663.00		1200.00	2044.59				11863.29	Remove Line?
09/13/2012	11863.29	3663.00		1000.00	2436.56			37.33	12052.40	Remove Line?
10/12/2012	12052.40	3663.00		1000.00	3131.60			25.68	11558.12	Remove Line?
11/13/2012	11558.12	3663.00		1000.00	3672.48			38.28	10510.36	Remove Line?
12/13/2012	10510.36	3663.00		800.00	2255.54			53.57	11064.25	Remove Line?

The Statement Summary Tab also allows users to:

- **Amend data:** Click on the cell you want to edit, enter the new data in the “Cell Value” field and click Amend Value.
- **Delete rows:** Click “Delete Row” to remove the entire row from your data set. This could be used if duplicate data was entered by mistake.
- **Highlight areas of concern:** Click on the cell want to call attention to and select the “Highlight Cell” checkbox. Then click Amend Value.
- **Make notes on important facts:** Click on the cell you want to comment on, then enter text in the “Cell Comment” field. Then click Amend Value. The cell comments box can be dragged to a location that will not block data.

To navigate the Statement Summary Tab without the “Add A Comment To Cell” dialog box appearing each time you click on a cell, click on cell K1 and change the “Allow Highlights/Comments” option to “False.” The highlights will still appear on the sheet, but the comments will only appear if you click on the cell.



You may notice significant changes in activity after or around the time of the suspect’s involvement. The SAFTA tool also enables a deeper dive into transaction-level data to investigate these changes. To do this, navigate back to the Welcome Tab and select the “Enter Transaction Data” button.



The “Enter Transaction Data” button on the Welcome Tab calls up a dialog box that prompts the user to enter individual transactions from each statement, versus only the summary data as entered before. First, select the account that you added in the previous step related to the information you want to enter.

At minimum, you should be able to enter the core elements of each transaction. While the transaction information given on bank statements may differ among financial institutions, the core elements appear on most bank statements. These are:

✓ **Statement Date**

The “statement date” is the last day of the time period presented on the bank statements and is usually shown on the first page. Bank statements are usually issued monthly, but some banks may issue them quarterly. Monthly statements normally correspond to calendar months, such as March 1 through March 31, in which case, the statement date would be the last date of the month: March 31, 20XX. However, a statement period may begin and end on dates that fall in the middle of the month, such as October 9 through November 8. In that case, the statement date would be November 8, 20XX. Each transaction from a single statement will have the same statement date.

Why it matters:
Recording statement dates during Data Entry will help you analyze transaction patterns from month to month when you build your Pivot Table.

✓ **Transaction Date**

The “Transaction Date” is the date on which a specific financial transaction occurred. Enter the transaction date as follows: MM/DD/YYYY.

- **Why it matters:** *Recording transaction dates during data entry will help you search for transaction activity on a certain date or within a date range and may allow you to connect dots between the suspect and victim activities.*

✓ **Deposit or Withdrawal**

A transaction can only be one of two things: a deposit, meaning money was added to the account, or a withdrawal, meaning money was taken out of the account. Select from the drop-down menu “Deposit” or “Withdrawal.”

- **Why it matters:** *Recording whether a transaction is a deposit or a withdrawal helps summarize the movement of money into and out of the account.*

✓ **Transaction Type**

Deposits and withdrawals take many forms. Select the transaction type from the dropdown menu. Typical deposit types may include:

- Social Security or pension income
- Veteran benefits
- Interest
- Deposits made at the bank (checks or cash)
- Transfers from other accounts

- Other

Typical withdrawal types may include:

- ATM withdrawals
- Checks
- Debit card/point of sale “POS” purchases
- Automatic (ACH or EFT) payments
- Transfers to other accounts
- Fees
- Other

This list isn’t all-inclusive, but it provides some examples of what “Types” you may want to include in your data.

- ***Why it matters: Recording types of deposits and withdrawals will help you further sort and analyze the movement of money into or out of an account to identify patterns of income or unusual spending.***

✓ **Check No.**

Check numbers are shown on the bank statements when applicable. Every withdrawal type labeled “Check” in your data should have a corresponding check number listed.

- ***Why it matters: Recording check numbers is important for identifying gaps or aberrant patterns in check sequences. Recording check numbers will also help you match copies of canceled checks to the corresponding transaction in your dataset.***

✓ **Payor/Payee**

A “Payor” is an individual or organization that makes a payment, while a “Payee” is the recipient of that payment. If the victim deposited a \$1,200 tax refund, the payor would be the United States Treasury. If the victim wrote a check for an electric bill, the payee would be “ABC Utility Company” as shown on the check copy received or on the statement itself.

- ***Why it matters: Recording payor and payee data is very important because this information will help you determine where funds came from, and ultimately where they went. This level of detail will help you determine which income and expense items might be expected versus which might be unusual for the victim.***

✓ **Amount**

Last, but certainly not least, “Amount” is the dollar amount of a specific transaction. If the statements show a number as negative, such as for a withdrawal or debit, just enter the number as a positive figure. The SAFTA Tool will identify it as a withdrawal based on your selection from the “Deposit or Withdrawal” dropdown menu.

- ***Why it matters: If you can’t demonstrate approximately how much money is missing, you don’t have a case. Accuracy is key.***

Attention to Detail

Requesting copies of deposit items, withdrawal slips, and canceled checks (front and back) in addition to bank statements is necessary for obtaining complete payor/payee data. Without this information, you will not be able to paint a complete picture of your victim's financial situation. If you did not receive these items from the financial institution with the first subpoena, make a second request using one of the editable subpoena templates available for download on IACP's Elder Abuse webpage:

<https://www.theiacp.org/elder-abuse>

Additional elements are pieces of information other than the core elements described above that you may wish to include in your data set for further analysis, such as:

✓ **Location**

Sometimes statements indicate where a transaction took place; for example, the address of a specific ATM, or the city in which a debit card was used to purchase gasoline. Summarizing location information may help identify transactions that your victim did or did not authorize.

✓ **Memo**

Most standard checks have a memo line, which may or may not be used. Information written on the memo line may be helpful to your case by indicating the reason a payment was made to an individual or organization. For example, checks written to the alleged perpetrator may contain memo details such as "for care", "gift", or "birthday", which you may want to inquire about.

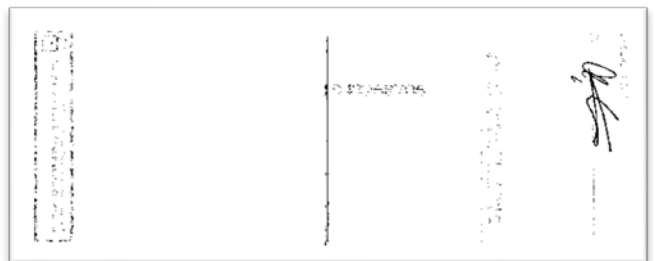
✓ **Signature**

The front of every check contains a signature line and must be signed for a financial institution to honor it. Signatures are especially important in cases where a power of attorney or a joint account holder had access to a victim's funds. Including the name of the individual signing the check in your data may help you determine which transactions were conducted by the victim and which were conducted by another party. When forgery is suspected, close examination of signatures may also help you determine which instruments may have been forged.

✓ **Endorsement**

Endorsements are the signatures or other information written or stamped on the back of checks when they are deposited or cashed. Endorsements are particularly important for obtaining samples of an alleged perpetrator's signature, and for determining who was the last holder of any checks written to "Cash." While you do not have to record the endorsements for every check written, you may want to consider recording

the endorsements on checks written to individuals such as the victim and the alleged perpetrator, and checks written to "Cash." Examples of endorsements on checks include stamps from payee



organizations, signatures of individuals who deposited or cashed the check, or a notation such as "For Deposit Only."

✓ **Bank Stamp**

For checks payable to the victim, the alleged perpetrator, or to "Cash," you may also want to make note of any bank stamps on the backs of checks. Bank stamps, if present, indicate the bank at which the check was honored, which may help you identify other financial institutions to send subpoenas to. Requesting documents from these banks may reveal additional accounts for either the victim or the suspect, and financial activity you were otherwise unaware of.

Users can assign transactions to the victim or the suspect based on either the facts of the case or some reasonable assumption.

- For those transactions you can easily assign to the victim as normal, reasonable, or authorized, select “Victim” from the drop-down menu.
- For those transactions you can easily assign to the suspect, potentially based on the type, location, or time frame in which the transaction occurred, select “Suspect” from the drop-down menu.
- There will be some (or many) transactions for which sufficient evidence does not exist to assign the transactions to either the victim or suspect. For these transactions select “Unknown” from the drop-down menu. Further investigation may be required to account for these transactions.

Each transaction entry automatically populates a row on a newly created “Transaction Data” tab for the account being examined, which in turn, populates the “Pivot Table” tab as explained in the next section.

Step 2: Building Your Case

Pivot Table Tab

When you’ve completed your data entry, the “Pivot Table” tab will summarize your transaction data by various characteristics like dates, payees, or amounts, to reveal sums, patterns, and anomalies that are key to your investigation. **Note: Transaction-level data is required to populate the pivot table. Account summary-level data will not populate the table.**

The SAFTA Tool pivot table is arranged by deposit/withdrawal, transaction type, and payee, in chronological order according to statement date, as shown. Use the plus (+) or minus (-) signs next to each field to expand or collapse the information in each field. Expanding the rows at the left will show you the individual transactions for each type.

Sum of Amount	Column Labels <input type="button" value="v"/>			
Row Labels <input type="button" value="v"/>	<input type="button" value="+"/> Jan	<input type="button" value="+"/> Feb	<input type="button" value="+"/> Mar	<input type="button" value="+"/> Apr
<input type="button" value="+"/> Deposit	2037.36	1004		500
<input type="button" value="-"/> Withdrawal				
<input type="button" value="+"/> ATM	1180	2451.24	1912	
<input type="button" value="+"/> Check	4079.74	4202.51	2775.54	321.54

To review your case, fully expand your pivot table. A fully expanded pivot table will show you patterns in both deposits and withdrawals from period to period. After you orient yourself to the categories, types, and payees contained in your pivot table, consider the following:

General

- Are there any “unknown” or “blank” categories that appear on the pivot table? If so, are additional documents or evidence required?
- If transfers to other accounts appear in either category (deposits or withdrawals), who owns those other accounts, and did you request records for these?
- Did the address listed on the statements change at any point during the period of your review?

Deposits

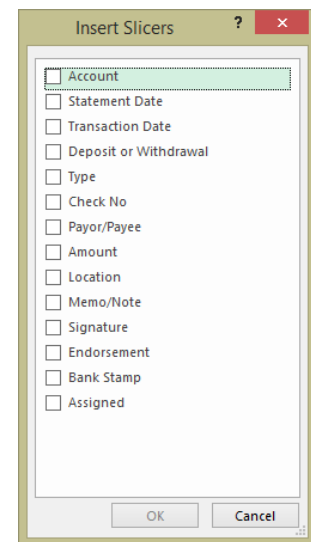
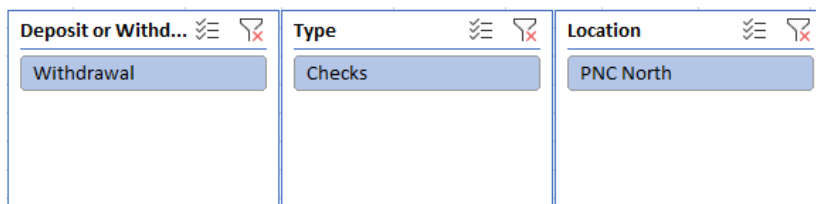
- What is the victim’s regular income, and is it deposited regularly?
- Is there a change in deposit patterns when the suspect became involved?
- Do deposits other than income appear in the statements? Where are these from: other accounts, assets, or individuals?
- If the account is a joint account or names a power of attorney, do any deposits belong to an individual other than the victim, indicating that funds are being comingled?

Withdrawals

- Is there a change in spending patterns when the suspect became involved?
- If you observe ATM transactions or debit card purchases, who had possession of the card?
- If withdrawals were made at the bank, who signed the slips?
- If there are checks, who signed them?
- Are check numbers used out of sequence?
- If checks were payable to cash, who endorsed them?
- If checks were payable to the suspect, where were they deposited?
- If there are payments to credit cards or loans, have you requested a credit report to determine any outstanding debt?
- Are there regular payments for expenses like utilities, insurance premiums, or housing? If any payments are missing or skipped in a certain month, is the victim in danger of shutoff, dropped coverage, or eviction? Are any payments made more than once in a given month?

Slicers in the Pivot Table tab allow you to change how much data you are viewing. Use of slicers is key for isolating activity occurring before the suspect’s involvement with the victim versus during or after. To use the slicers, click on the “Analyze” tab in Excel and then “Insert Slicer.”

All of the transaction-level details are presented as options for selection. Click the types of data that you would like to compare. After you click “OK,” the data will be presented as separate boxes, by selecting one or multiple options within each box, transactions meeting those characteristics will be presented.



There are many more questions to consider as you review your data, and more analysis can be done using worksheet and pivot table features like sorting and filtering by date, text, and other characteristics. For other tips on using pivot tables, check out the following links:

- <https://youtu.be/9NUjHBNWe9M>
- <https://youtu.be/dis9tg6xwmw>
- <https://youtu.be/-8nd5hrndje>

Step 3: Graph Dashboard – Creating a Visual

Pictures are worth a thousand words: The SAFTA Tool contains four graph templates that help present your data visually located on the Dashboard Tab. These graphs can show whether a victim’s account balance decreased after the suspect became involved, whether spending increased during that period, or exceeded income, what the most common form of withdrawal was, and how much spending may have been for the victim versus the suspect.

1. Account Balance Line Graph

The Account Balance line graph takes balance information from your data entry tab, and graphs it so you can see when and whether the account increased or decreased in value during the period of your review.

2. Income and Spending Comparison Bar Graph

The Income and Spending Comparison bar graph sums deposits and withdrawals and presents them by color so you can see whether income exceeded spending in a given period, or whether spending exceeded income. *Note: This chart will only appear if Transaction level data is entered.*

3. Spending Activity Line Graph

The Spending Activity line graph takes withdrawal information from the data entry tab, and graphs it so you can see whether and when spending patterns changed. You can also add a line to indicate the date at which the suspect became involved. Instructions for this feature are on the following page.

4. Withdrawals by Type Pie Chart

The Withdrawals by Type pie chart sums all spending by check, ATM, debit card, etc. based on the statement data entered on the data entry tab. *Note: This chart will only appear if Transaction level data is entered.*

Additional charts can be created on the Dashboard. You can select from Summary or Transaction data, one or multiple accounts, the type of chart you’d like to create (line, bar, or pie), and the variables available for the type of chart you selected.

To add a key date to your line graph, select the “Add a Timeline” button at the top of your Dashboard. Enter your key date – such as the date the suspect became POA, or the date that the victim received a dementia diagnosis – in the MM/DD/YYYY format. Once entered, a vertical line indicating this date will be added to “Balance of Accounts” graph and the “Income vs. Spending” graph. To remove timeline(s) from your graphs, select the “Delete Timelines” button at the top of your dashboard.

Presenting Financial Evidence

Consider using a PowerPoint slideshow to help organize your facts and findings for prosecution. Copy and paste the PivotTable and any graphs you create into the template to tell the story of how the financial exploitation happened.

Use of Experts

Don't forget your local Adult Protective Services office. They may have additional resources or be able to support your investigation with deeper analysis. APS might also be able to help prevent further exploitation. Financial management or other services may be arranged through the local Office for the Aging, or other community resources. To find local elder justice resources in your state, click the U.S. Department of Justice's Elder Justice Initiative [Neighborhood Map](#) or visit <https://www.justice.gov/elderjustice/support/resources-neighborhood>.

While the SAFTA Tool is useful for analyzing checking and savings accounts, many financial exploitation cases involve other assets or transactions. For more complex cases, consider the use of financial experts such as accountants, forensic accountants, and financial advisors or investment brokers.

- ✓ **Traditional accountants** typically prepare financial statements and tax returns for individuals and entities and may also perform financial statement audits. When considering the use of an accountant as an expert in your case, look for an accountant who is a Certified Public Accountant, commonly known as a "CPA". CPAs must pass a rigorous exam to become licensed and comply with ongoing education requirements to maintain their licensure.
- ✓ **Forensic accountants** typically perform nontraditional accounting and auditing services such as fraud investigations, compliance audits, asset valuations, and other consulting services. Forensic accountants usually possess a CPA license as well as other exam-based certifications such as Certified Fraud Examiner (CFE), Certified Internal Auditor (CIA), Certified in Financial Forensics (CFF), and others.
- ✓ **Financial advisors or investment brokers** perform investment advisory services and must also pass various exams in order to trade securities like stocks, bonds, and mutual funds. Financial advisors may also be licensed to sell insurance products. When questions arise on investment accounts, insurance policies, and annuity contracts, consider asking a local financial advisor or investment broker to provide insight or guidance.

If you plan to provide the expert with any documents obtained via subpoena, you may need a sharing order. Contact your local district attorney's office before you share any evidence with a third party.

LOCATING A FORENSIC ACCOUNTANT

Each state has a [Board of Accountancy](#) that maintains a database of verified CPAs within that state.

If you are aware of an accountant practicing in your area and want to determine whether they hold an active CPA license, the National Association of State Boards of Accountancy (NASBA) maintains a database of CPAs called CPA Verify at <https://cpaverify.org/>. Note, however, that all states do not submit data to CPA Verify.

The Association of Certified Fraud Examiners (ACFE) also maintains a database of CFEs via their "Find a CFE" page at www.acfe.com/findacfe.aspx.

If your jurisdiction has an active elder abuse multi-disciplinary team or Financial Abuse Specialty Team, reach out to the coordinating agency and ask whether they are aware of a forensic accountant with elder abuse experience.