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

---

[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.

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.

---

[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)).

Pennsylvania House Aging and Older Adult Services Committee

House Bill 2549

Credit Union Efforts to Combat Elder Financial Abuse

September 5, 2018

4309 North Front Street, Harrisburg, Pennsylvania 17110-1618 | 717.234.3156 | PCUA.org | iBelong.org

On behalf of the Pennsylvania Credit Union Association (PCUA), we write in support of House Bill 2549, legislation that would modernize the Older Adult Services Protection Act. PCUA is a state-wide advocacy organization that represents a majority of the nearly 400 credit unions located in the Commonwealth of Pennsylvania. Credit unions are not-for-profit, mutually owned financial cooperatives that do not issue capital stock. Profits made by credit unions are returned to members in the form of higher dividends on savings, lower interest rates, and expansion of services. A core mission of credit unions is to promote thrift and teach the wise use of credit. Because credit unions are not-for-profit and have low overhead costs, they are usually able to offer lower interest rates on loans and higher dividends on members' shares (savings).

As member-owned financial cooperatives, credit unions exist only to serve their members. In promoting thrift among their members, credit unions regularly provide financial education to their members in various forms. They often provide scholarships for higher education; open branches in schools; teach financial literacy in schools and to adults; and, most importantly, work closely with their members so that their members can achieve their financial goals. Part of credit unions financial education efforts include providing elderly members tools and resources to better protect themselves from financial exploitation and wrong-doing. Credit union staff involved in those efforts are trained and knowledgeable in handling a number of complex situations including how to recognize the financial exploitation of elderly credit union members.

One area of particular interest that PCUA supports in House Bill 2549 are the training and reporting requirements to prevent elder financial exploitation. Elder financial exploitation includes the illegal or improper use of an older adult's funds, property, or assets. Recent studies suggest that financial exploitation is the most common form of elder abuse and that only a small fraction of incidents are reported. Older adults are often targets of financial exploitation by family members, caregivers, scam artists, financial advisers, home repair contractors, agents with power of attorney, and others.

According to research from insurance provider MetLife, financial abuse by itself costs older Americans over $2.6 billion dollars annually[1]. Credit unions are taking several steps to curb this escalating problem, including staff training to identify and report abuse, instituting new computer programs that can recognize irregular activity, and community outreach to help educate vulnerable members about avoiding theft and fraud. The Commonwealth should be proud to know that Pennsylvania credit unions have led the charge against the financial exploitation of our elderly population.

It is current practice for credit unions to report questionable transactions through suspicious activity reports (SARs) as required by the Financial Crimes and Enforcement Network (FinCEN), a

[1] MetLife Mature Market Institute, The National Committee for the Prevention of Elder Abuse, The Center for Gerontology at Virginia Polytechnic Institute and State University. *Broken Trust: Elders, Family & Finances* (PDF).

bureau of the U.S. Department of Treasury. A specific category for financial elder abuse is included on the SARs form if the credit union suspects this type of activity.

The basic concept underlying FinCEN's core activities is "follow the money." FinCEN partners with law enforcement at all levels of government and supports the nation's foreign policy and national security objectives. Law enforcement agencies successfully use similar techniques, including searching information collected by FinCEN from credit unions, to investigate and hold accountable a broad range of criminals, including perpetrators of financial elder abuse.

Due to FinCEN requirements, Pennsylvania credit unions have policies and procedures in place to curb fraudulent financial activity against its elderly members to protect them from any catastrophic loss. To illustrate, attached is a Generalized Policy Statement offered by PCUA for credit unions to adopt if internal guidelines are needed. Credit unions also adopt internal policies to identify financial exploitation and how to report to local authorities when it is suspected.

To complement the internal policies of a credit union, the National Credit Union Administration (NCUA), the Bureau of Consumer Financial Protection (BCFP), and the Pennsylvania Department of Banking and Securities (PA DOBS) provide education resources for credit union staff, and no-cost financial literacy products for members to build savings and achieve their financial objectives. These supplemental tools enable credit union staff to facilitate outreach to the members and communities they serve. One resource that many credit unions offer to its elderly members is the *Money Smart for Older Adults* (*Money Smart*) program. *Money Smart* is an instructor-led training developed in part by the Bureau of Consumer Financial Protection (BCFP). The module assists credit unions to create awareness among older adults and their caregivers on how to prevent elder financial exploitation and to encourage advance planning and informed financial decision-making.

In addition, earlier this summer PA DOBS announced that it is offering its Senior$afe Program to financial institutions, including credit unions. This free training "helps financial professionals identify the several "red flags" of suspicious behavior of their clients and/or those close to their clients, as well as types of financial account activity that could indicate fraud, exploitation, or abuse. Additionally, Senior$afe helps financial professionals understand how Adult Protective Services works to protect senior citizens and how they themselves can report suspicious behavior or account activity to help protect their clients. PCUA has partnered with the PA DOBS to provide this form of training to Pennsylvania credit unions.

The recent passage of S. 2155, the Economic Growth, Regulatory Relief, and Consumer Protection Act, provides financial institutions a safe harbor to report elder financial abuse, so long as credit union staff are trained in identifying and properly reporting suspected financial exploitation of their elder members. The combination of credit unions' internal policies, best practices, federal requirements and proactive measures found in House Bill 2459 will provide older adults thorough protection to limit their chances of being taken advantage of financially.

In closing, credit unions serve and intervene on behalf of their older credit union members when financial exploitation is suspected. Credit unions take pride in their "people helping people" philosophy which is demonstrated daily in the close relationships they have with their members and protecting them from unforeseeable financial harm. Thank you for allowing PCUA the opportunity to share how credit unions are proactively combatting financial exploitation of Pennsylvania's elderly.

Model Policy 2245: Protecting the Elderly and Vulnerable from Fraud

Model Policy Revised Date: 06/27/2015

General Policy Statement:

Credit Unions are in a unique position to detect and prevent financial exploitation and fraud. The primary roles of [[CUname]] (Credit Union) is the protection of its members' assets and the prevention of financial losses. The Credit Union will take steps to protect elderly (over 62 years of age) and vulnerable (generally described as individuals over the age of 18 who lack the physical and mental capability to care for themselves) members from financial exploitation and fraud by training staff to recognize the types of financial scams, the red flags of potential abuse and what to do when fraud is suspected. The Credit Union may disclose nonpublic personal information to comply with federal, state, or local laws, rules and other applicable legal requirements, such as state laws that require reporting by financial institutions of suspected abuse.

Guidelines:

1. **ROLE OF BOARD OF DIRECTORS**. The Board of Directors will (1) approve the credit union's written Elderly and Vulnerable Protection policy and program; and (2) oversee the development, implementation, and maintenance of the Credit Union's program, including assigning specific responsibility for its implementation, and reviewing reports from management.

2. **ROLE OF MANAGEMENT TEAM.** The management team will (1) oversee the development and implementation of the Elderly and Vulnerable Protection program; (2) draft procedures to ensure compliance with the program; (3) monitor, evaluate and suggest adjustments to the program; (4) ensure that staff are trained on these issues at least annually; and (5) brief the Board of Directors of the Credit Union at least annually on the status of the program. In addition to the annual report, the Board of Directors may allow the management team the option to provide [[2245-1]] reports.

3. **TYPES OF FINANCIAL EXPLOITATION.** Credit Union staff should be aware of the following types of financial exploitation:

    A. **Theft of Income.** The most common form of financial fraud and exploitation, typically involving less than $1,000 per transaction.

    B. **Theft of Assets.** This is often more expensive and typically involves abuse associated with Powers of Attorney, real estate transactions, identity theft or

tax manipulation.

4. **TYPES OF FINANCIAL SCAMS.** Although this is not an exhaustive list, Credit Union staff will be trained to be aware of the following types of financial scams:

   A. **Power of Attorney Fraud.** The perpetrator obtains a Limited or Special Power of Attorney, which specifies that legal rights are given to manage the funds in the account. Once the rights are given, the perpetrator uses the funds for personal gain.

   B. **Advance Fee Fraud or "419" Fraud.** Named after the relevant section of the Nigerian Criminal Code, this fraud involves a multitude of schemes and scams – mail, e-mail, fax and telephone promises that the victims will receive a percentage for their assistance in the scheme proposed in the correspondence.

   C. **Pigeon Drop.** The victim puts up "good faith" money in the false hope of sharing the proceeds of an apparently large sum of cash or item(s) of worth which are "found" in the presence of the victim.

   D. **Financial Institution Examiner Fraud.** The victim believes that he or she is assisting authorities to gain evidence leading to the apprehension of a financial institution employee or examiner that is committing a crime. The victim is asked to provide cash to bait the crooked employee. The cash is then seized as evidence by the "authorities" to be returned to the victim after the case.

   E. **Inheritance Scams.** Victims receive mail from an "estate locator" or "research specialist" purporting an unclaimed inheritance, refund or escheatment. The victim is lured into sending a fee to receive information about how to obtain the purported asset.

   F. **Financial Institution Employee Fraud.** The perpetrator calls the victim pretending to be a security officer from the victim's financial institution. The perpetrator advises the victim that there is a system problem or internal investigation being conducted. The victim is asked to provide his or her Social Security number for "verification purposes" before the conversation continues. The number is then used for identity theft or other illegal activity.

   G. **International Lottery Fraud.** Scam operators, often based in Canada, use telephone and direct mail to notify victims that they have won a lottery. To show good faith, the perpetrator may send the victims a check. The victim is

then instructed to deposit the check and immediately send (via wire) the money back to the lottery committee. The perpetrator will create a "sense of urgency," compelling the victim to send the money before the check, which is counterfeit, is returned. The victim is typically instructed to pay taxes, attorney's fees, and exchange rate differences in order to receive the rest of the prize. These lottery solicitations violate U.S. law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail.

H. **Fake Prizes.** A perpetrator claims the victim has won a nonexistent prize and either asks the person to send a check to pay the taxes or obtains the credit card or checking account number to pay for shipping and handling charges.

I. **Internet Sales or Online Auction Fraud.** The perpetrator agrees to buy an item for sale over the Internet or in an online auction. The seller is told that he or she will be sent an official check (e.g., cashier's check) via overnight mail. When the check arrives, it is several hundred or thousand dollars more than the agreed-upon selling price. The seller is instructed to deposit the check and refund the overpayment. The official check is later returned as a counterfeit but the refund has already been sent. The seller is left with a loss, potentially of both the merchandise and the refund.

J. **Government Grant Scams.** Victims are called with the claim that the government has chosen their family to receive a grant. In order to receive the money, victims must provide their checking account number and/or other personal information. The perpetrator may electronically debit the victim's account for a processing fee, but the grant money is never received.

K. **Spoofing.** An unauthorized website mimics a legitimate website for the purpose of deceiving consumers. Consumers are lured to the site and asked to log in, thereby providing the perpetrator with authentication information that the perpetrator can use at the victim's legitimate financial institution's website to perform unauthorized transactions.

L. **Phishing/Vishing/Smishing.** Technology or social engineering is used to entice victims to supply personal information (i.e., account numbers, login IDs, passwords, and other verifiable information) that can then be exploited for fraudulent purposes, including identity theft. These scams are most often perpetrated through mass e-mails, spoofed websites, phone calls or text messages.

M. **Stop Foreclosure Scam.** The perpetrator claims to be able to instantly stop foreclosure proceedings on the victim's real property. The scam often involves the victim deeding the property to the perpetrator who says that the victim will be allowed to rent the property until some predetermined future date when the victim's credit will have been repaired, and the property will be deeded back to the victim without cost. Alternatively, the perpetrator may offer the victim a loan to bridge his or her delinquent payments, perhaps even with cash back. Once the paperwork is reviewed, the victim finds that his or her property was deeded to the perpetrator. A new loan may have been taken out with an inflated property value with cash back to the perpetrator, who now owns the property. The property very quickly falls back into foreclosure and the victim/tenant is evicted.

5. **ROLE OF CREDIT UNION STAFF.** Although this is not an exhaustive list, Credit Union staff will be trained to spot the following red flags that are often associated with financial scams:

A. Signatures seem forged or unusual.

B. Check numbers are out-of-sync.

C. A vulnerable adult informs staff that funds are "missing" from his or her account.

D. Abrupt changes in a will or other financial documents.

E. It is requested that account or credit card statements are to be sent to an address other than the vulnerable adult's home.

F. Unusual cash withdrawals from a checking account within a short period of time.

G. Abrupt increase in credit card activity.

H. A sudden flurry of bounced checks.

I. An account shows ATM activity when it is known that the vulnerable adult is physically unable to leave his or her home.

J. The vulnerable adult is accompanied by a third party who encourages the withdrawal of a large sum of cash, and may not allow the vulnerable adult to

speak.

K. Abrupt and unexplained change in a financial Power of Attorney; new names added to signature cards; new joint account created.

L. Discovery of incapacitated vulnerable adult's signature for financial transactions or for title of real or personal property.

M. Sudden appearance of previously uninvolved relatives claiming rights to the adult's affairs and possessions.

N. Adult has no knowledge of newly-issued ATM, debit or credit card.

O. Adult is confused about account balance or transaction on his or her account.

P. A caregiver appears to be getting paid too much or too often.

Q. Significant increases in monthly expenses being paid from the account.

R. Adult reports concern over having given out personal information to a solicitor over the phone.

S. Unexplained sudden transfer of assets, particularly real property.

T. Expressed excitement about winning a sweepstakes, lottery or inheritance.

U. Refinance of the adult's property, with significant cash out, or with the addition of new owners on the deed, but not on the loan.

6. **WHAT TO DO IF FRAUD IS SUSPECTED.** Management will develop procedures, and Credit Union staff will be trained to take the following actions when fraud is suspected:

A. Carefully verify anyone's authority who is acting on the member's behalf.

B. Use probing questions to determine the member's intent regarding a transaction.

C. Create an "Awareness Document" and for large cash withdrawals that appear out of the ordinary, have the member read and sign it prior to the receipt of

funds. This form could include the following:

i. Brief overviews of common fraud schemes.

ii. Warnings that perpetrators of such schemes could present themselves as an FBI agent, financial institution examiner or official, police officer, or detective.

iii. Warnings that members should use caution if they are asked for information about their account, or asked to withdraw money to help "catch someone," or provide money to show "good faith."

iv. Notice that the Credit Union does not conduct investigations or verification of accounts by telephone, nor will local, state or federal law enforcement authorities, financial institution regulatory authorities or officials conduct investigations by asking individuals to withdraw cash from their account for any reason.

v. Phone numbers for the appropriate agencies, if any of the circumstances listed about are in evidence, with instructions to members that they should contact their branch, local police department, Adult Protective Services or the Federal Trade Commission to investigate before they withdraw money.

vi. Reminders that swindlers are almost always friendly and have "honest" faces and that they particularly tend to take advantage of older individuals.

vii. The amount the member has requested, with a request to read and sign the document.

D. Delay the suspicious transaction, if possible, by advising the member that additional verification of the transaction is required.

E. Contact management for assistance and guidance. Management may be required to contact the Credit Union's legal counsel for such assistance.

F. File a Suspicious Activity Report (SAR), using the term "Elder Financial Exploitation" in the narrative.

G. Report the incident to law enforcement following the Credit Union's normal protocol.

7. **LOSS PREVENTION AND SECURITY.** Management will develop procedures, and Credit Union staff will be trained to take the following loss prevention and security steps when financial fraud occurs or is suspected:

   A. Document the situation.

   B. File a SAR, using the term "Elder Financial Exploitation" in the narrative

   C. Take immediate protective action on accounts by placing holds or restraints and follow normal prevention and recovery steps to follow the money as needed.

   D. Make a verbal report to the local Adult Protective Services and provide investigative research and services as needed.

   E. Continue to monitor the account during legal proceedings, of necessary.

   F. Document files of final outcome.

Note: This policy has not been updated since the passage of S. 2155.