TENNESSEE LEAGUE

The Voice for Tennessee Credit Unions

Elder Financial Exploitation

White Paper

2022

Table of Contents

Introduction

The American public is aging, and as more and more of the population ages, a more significant segment becomes vulnerable to exploitation. Between 2012 and 2050, the United States will experience considerable growth in its older population. In 2050, the population aged 65 and older will be 83.7 million, almost double its estimated population of 43.1 million in 2012. These men and women are increasingly subject to elder financial abuse. While credit unions do a fine job identifying people they feel are being taken advantage of, there are many questions and concerns regarding the reporting process.

According to the National Center on Elder Abuse (NCEA), the definition of elder financial abuse is defined as "illegal taking, misuse, or concealment of funds, property or assets of a vulnerable elder at risk for harm by another due to changes in physical functioning, mental functioning, or both."

The US Census shows that adults aged 65 or higher are the fastest-growing demographic group, and abuses against them continue to rise steadily. A 2011 MetLife report estimated that financial losses by seniors were $2.9 billion in 2010. Among the many forms of elder abuse, financial exploitation is increasingly common.

Overview of the Issues

There are many types of elder financial abuse, with new schemes and scams being concocted frequently to trick elders and vulnerable adults for personal gain. While not comprehensive, the following is a list of the typical types of elder abuse observed, in many cases perpetrated by a family member or caregiver:

- Theft of property
- Misuse of income or assets
- Forged checks
- Fraudulent use of the power of attorney
- Lotteries and phony contests
- Phony solicitation from charities
- Investment Frauds
- Medical Scams
- Contractor Scams
- Grandparent/Grandchild Imposter Emergency Scam
- Sweetheart/Romance Scams

The credit unions of Tennessee, with a long history of helping members avoid financial pitfalls, are committed to protecting members' assets and providing timely reports to authorities when signs of abuse are evident. Credit union tellers and member services staff, who interact with members daily, are in a unique position to detect and take appropriate action when financial abuse of elderly or vulnerable persons is suspected.

In 2017 the Tennessee General Assembly passed legislation to give credit unions and other financial institutions more tools to assist them if they feel someone is being taken advantage of. Senate Bill 1267, the "Elderly and Vulnerable Adult Financial Exploitation Prevention Act," became Public Chapter on May 11, 2017.

As part of this legislation, the Tennessee Department of Financial Institutions was tasked with working with the associations for credit unions and banks and other state agencies to develop a more robust solution to elder abuse. The Tennessee Credit Union League has worked with the Tennessee Department of Financial Institutions, the Consumer Financial Protection Bureau (CFPB), the Tennessee Commission on Aging & Disability, and other state agencies on this issue. We have compiled information and resources to assist Tennessee credit unions in identifying, reporting, and deterring financial exploitation.

Understanding Tennessee's New Law regarding Financial Exploitation

On July 7, 2017, a new law took effect in Tennessee that gives financial institutions tools and greater flexibility to help protect their customers who are elderly or vulnerable where the institutions suspect elder abuse or financial exploitation. The new law, which is currently scheduled to sunset on June 30, 2022, is called the "Elderly and Vulnerable Adult Financial Exploitation Prevention Act,"

The Act affords credit unions a process and the authority to take specific actions when there is "reasonable cause" to suspect financial exploitation of an elderly adult (defined as being a person age 65 or older) or of a vulnerable adult (defined as a person age 18 or older who, because of intellectual disability or physical dysfunction, is unable to manage their resources fully, to carry out all or a portion of the activities of daily living, or to protect fully against neglect, exploitation, or hazardous or abusive situations without assistance from others).

Steps a credit union may take when financial exploitation is suspected

- As a preliminary precaution, establishing a list of persons the member would like to have contacted if the credit union suspects the member is a victim of financial exploitation or financial theft;
- Refuse to accept an authorized power of attorney (POA) or durable power of attorney (DPOA) if it is suspected that the agent or attorney-in-fact (AIF) is conducting financial exploitation or financial theft against the member; and
- Authority to delay or refuse a transaction from the account of an elderly member or vulnerable adult.

If you have reasonable cause to suspect that financial exploitation may have occurred, may have been attempted, or is being attempted, you may, but are not required to, refuse a transaction or delay a transaction on account of:

The elderly or vulnerable adult

On the account that the elderly or vulnerable adult is a beneficiary, including a trust, guardianship, or conservatorship account

Or on the account of a person suspected of perpetrating financial exploitation.

You May

- Refuse or delay a transaction if the department of human services or a law enforcement agency provides information to you demonstrating that it is reasonable to believe that financial exploitation may have occurred, may have been attempted, or is being attempted.

- Except as ordered by a court, you are not required to refuse or delay a transaction when provided with information by the department of human services or a law enforcement agency alleging that financial exploitation may have occurred, may have been attempted, or is being attempted, but may use your discretion to determine whether to refuse the transaction or hold the transaction based on the information available to you.

If you refuse or hold a transaction based on reasonable cause to suspect that financial exploitation may have occurred, may have been attempted, or is being attempted, you are required to:

- Except with regard to an account administered by a bank or trust company in a fiduciary capacity, make a reasonable effort to notify one or more parties authorized to transact business on the account orally or in writing.

- No notice is required to be provided to any party authorized on the account if the party is the suspected perpetrator of financial exploitation.

- If it involves financial exploitation, report the incident to the department of human services adult protection services.

Any refusal to conduct a financial transaction or hold a transaction based on your reasonable cause to suspect that financial exploitation may have occurred may have been attempted, or is being attempted expires upon the earlier of:

- Ten business days after the date on which you first refused or held the financial transaction (unless earlier terminated by order of a court of competent jurisdiction), if the transaction involved the sale of a security or offer to sell a security and the person selling or offering to sell is not required to register under title 48, chapter 1, part 1;

- Five business days after the date on which you first refused or held the financial transaction, if the transaction did not involve the sale of security unless terminated earlier by order of a court of competent jurisdiction;

- The time when you reasonably believe that the financial transaction will not result in financial exploitation; or

- When the member requesting the transaction has been advised of potential risk in the transaction, the member has asked for the transaction to continue as long as the member is not the suspected perpetrator of financial exploitation.

The credit union may extend the time permitted in this section to refuse or hold a transaction based on a reasonable belief that additional time is needed to investigate the transaction or prevent financial exploitation.

A court of competent jurisdiction may enter an order extending the time that you must refuse a transaction or hold based on reasonable cause to suspect that financial exploitation may have occurred, may have been attempted, or is being attempted.

The credit union, or an employee of the credit union, is immune from all criminal, civil, and administrative liability:

- For refusing or not refusing a financial transaction, or holding or not holding a financial transaction

- For actions taken to further the determination, the decision was based upon a reasonable belief.

The credit union is authorized to offer to an elderly or vulnerable adult the opportunity to submit and periodically update a list of persons that the elderly or vulnerable adult allows the credit union to contact when the credit union has reasonable cause to suspect that the adult is a victim or a target of financial exploitation.

The credit union, or an officer or employee of the credit union, that has reasonable cause to suspect that an elderly or vulnerable adult is the victim or target of financial exploitation may convey the suspicion to one or more of the following, providing that the person is not the suspected perpetrator:

- Persons on the list, if a list has been provided by the elderly or vulnerable adult;

- A co-owner, additional authorized signatory, or beneficiary on the elderly or vulnerable adult's account; or

- The credit union knows a person to be a family member, including parent, adult child, or sibling.

When providing information under this section, the credit union may limit the information and disclose only that the credit union has reasonable cause to suspect that the elderly or vulnerable adult may be a victim or target of financial exploitation without revealing any other details or confidential personal information regarding the financial affairs of the elderly or vulnerable adult.

The credit union may choose not to contact one or more persons on the list if the credit union suspects that the person or persons are engaged in financial exploitation.

The credit union, or an employee of the credit union, will be immune from all criminal, civil, and administrative liability for contacting a person or electing not to contact a person under this section and for actions taken in furtherance of that determination if the determination was made based on reasonable belief.

Contact with any person and any information provided under the above provisions will be exempt from the present law's customer consent and customer notice provisions.

Power of Attorney

A credit union is authorized to refuse to accept an acknowledged power of attorney if the credit union has reasonable cause to suspect that the principal may be the victim or target of financial exploitation by the agent or persons acting for or with the agent.

A credit union, or an employee of the credit union, will be immune from all criminal, civil, and administrative liability for refusing to accept a power of attorney or for getting a power of attorney and for actions taken in furtherance of that determination if the determination was based upon reasonable belief.

Tennessee is a Mandatory Reporting State

- **Abuse of the elderly and vulnerable adults is against the law, and Tennessee is a *mandatory reporting* state.**
- **If you see abuse, or even only suspect that an adult is being abused, neglected, or exploited, you must report it**
- **Call the Tennessee Department of Human Services Adult Protective Services unit at 1-888-APS-TENN (1-800-277-8366)**
- **Or contact your local law enforcement agency.**

Financial Institutions often cite concerns about the possibility of being charged with a violation of the federal statutes that govern the disclosure of private financial records as a barrier to participation in reporting programs. However, the law most frequently cited in this regard, the Financial Services Modernization Act of 1999, better known as the Gramm-Leach-Bliley Act, **does not prohibit reporting to Adult Protective Services (APS) or law enforcement.** While the Act does contain extensive privacy provisions, several exceptions permit the disclosure of "nonpublic personal information." And essential for reporting on Elder Financial Abuse, these exemptions apply to mandatory reporting, voluntary reporting, or both.

Expressly, Subsection (e)(3)(B) permits disclosure "to protect against or to prevent actual or potential fraud, unauthorized transactions, claims, or other liability." Subsection (e)(5) permits disclosure "to the extent specifically permitted or required under other provisions of law… to law enforcement agencies… or for an investigation on a matter related to public safety. In addition, Subsection (e)(8), which permits disclosure "to comply with Federal, State, or local laws, rules, and other applicable legal requirements," would allow disclosures in connection with an APS investigation. **In plain language: reporting suspected financial abuse falls within the exceptions to the Act.**

- To further clarify this point, on September 24, 2013, the NCUA and seven other regulatory agencies issued guidance explaining that reporting suspected financial abuse of older adults to appropriate local, state, or federal agencies does not, in general, violate the privacy provisions of the GLBA or its implementing regulations. Specific privacy provisions of the GLBA and its implementing regulations permit the sharing of this type of information under appropriate circumstances without complying with notice and opt-out requirements.
- In addition, there are essential protections from civil liability from the Safe Harbor for Regulated Financial institutions From Civil Liability for Suspicious Activity Reporting. Federal law (31 USC 5318(g)(3)) provides protection from civil liability for all reports of suspicious transactions made to

appropriate authorities, including supporting documentation, regardless of whether such notifications are filed under the SAR instructions.

- Specifically, the law provides that a bank or credit union and its directors, officers, employees, and agents that disclose to the appropriate authorities of any possible violation of law or regulation, including disclosure in connection with the preparation of SARs, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including an arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." The safe harbor applies to SARs filed within the required reporting thresholds and to SARs filed voluntarily on any activity below the threshold.

Further Clarification on Reporting

In February 2011, FinCEN issued an advisory to financial institutions on filing suspicious activity reports regarding elder financial exploitation. FinCEN noted that SARs are 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… [now codified at 31 CFR § 1020.320], 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. 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.

Red Flags of Financial Exploitation

Tellers and Member Services personnel can be the first line of defense when looking for signs that indicate elder or vulnerable adult financial abuse may be occurring. While one or two of these 'red flags' may not necessarily mean elder abuse, the more red flags you detect, the more likely it is that you see a pattern of financial abuse.

- **Uncharacteristic banking activity:** there may be unusual shifts in the senior member's banking activity compared to the past. These types of shifts may include frequently changing transactions from one branch to another, changes in and frequencies of withdrawals, large withdrawals or transfers from recently opened joint accounts or previously inactive accounts, and frequent ATM withdrawals, especially if the member is isolated or has not accessed an ATM recently.
- **Suspicious signatures:** there may be signs that the signature was forged, withdrawal slips, or applications made out in another person's handwriting.
- **A sudden increase in debt:** if a senior or vulnerable adult member has a large loan, takes out a second mortgage if they take out a loan on top of an existing mortgage, or if there are a large amount of credit card transactions, there may be signs of elder financial abuse taking place.
- **Additional red flags:** a power of attorney is executed by a senior member or vulnerable adult who appears to be confused; there are changes to the member's property titles, will, or other documents relating to their finances; there is somebody else handling the member's financial affairs with no apparent benefit to the member; bank statements and checks are no longer being sent to the member's residence; implausible reasons for banking activity stated by the member or accompanying person.

Suspicious Behavior

In addition to the "red flags" mentioned above, there may be noticeable differences in the member's behavior that signal a possibility of elder financial abuse. Be on the lookout for these signals and contact your supervisor immediately if any of these behaviors are observed:

- Accompanied by a stranger
- Withdrawals of large amounts of cash
- Coerced into making transactions
- Not allowed to speak for themselves or make decisions
- The accompanying acquaintance appears far too interested in the member's finances
- Seems nervous or afraid of the person with them
- Concerned or confused about "missing funds" in their accounts
- Unable to answer questions, confused about financial transactions, or signing paperwork
- Fearful that they will be evicted and institutionalized
- Appears neglected or receiving insufficient care given their economic status
- Bruising or broken bones (other signs of physical abuse)

Training

BankSafe empowers frontline employees to identify red flags for financial exploitation and develop skills to ensure older Americans are not defrauded out of their hard-earned money.

AARP has partnered with a digital learning and instructional design leader and collaborated with more than 200 bank and credit union experts to develop BankSafe.

This first-of-its-kind course is free, interactive, and self-paced. Designed with the frontline-user in mind, the BankSafe training:

- Includes interactive modules, real-life scenarios, and fun games to test skills.
- Provides short, bite-size education and training activities; and
- Allows users to train and monitor their progress at their own pace.

Model Policy 2245: Protecting the Elderly and Vulnerable from Frau

Model Policy Revised Date: 6/26/2019

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 outcome.

8. **IMMUNITY FROM CIVIL AND ADMINISTRATIVE LIABILITY.** In order for the Credit Union and reporting employee(s) to be immune from administrative and civil proceeding, under Federal law, for disclosing suspected exploitation of a senior citizen (defined as 65 years or older), the Credit Union has procedures that include the following:

   A. At the time of disclosure, the reporting employee is a supervisor or in a compliance/legal function.
   B. The disclosure was made in good faith and with reasonable care; and
   C. The employee received training conducted by the Credit Union that meets the requirements outlined below:

      i. Content of the training is retained and made available to a covered agency with examination authority.
      ii. Training provides instruction on how to identify and report the suspected exploitation of a senior citizen internally and, as appropriate to law enforcement (or government officials), including common signs that indicate financial exploitation and that discusses the need to protect the privacy, respect the integrity of each member and is appropriate to the employee and their job responsibilities;
      iii. Training is provided as soon as reasonably practicable and no later than one year after start of employment; and
      iv. Records of training are maintained for all individuals, even if the training was conducted before the individual was employed with the Credit Union