

Vulnerable Adult Protection

Best Practices

The information presented in this document is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this document.

Financial exploitation of vulnerable adults is one of the fastest-growing forms of fraud affecting credit union members today. Older adults and individuals with physical, cognitive, or developmental disabilities are increasingly targeted by scammers, caregivers, family members, and other bad actors seeking to gain access to their finances.

Because credit unions maintain trusted relationships with their members and are often the first to observe unusual account activity, they play a critical role in identifying potential exploitation and intervening when appropriate. By implementing consistent policies, educating employees, recognizing warning signs, and responding promptly to suspicious transactions, credit unions can help safeguard their members' financial well-being while balancing member autonomy, privacy, and regulatory responsibilities. This document outlines best practices to assist credit unions in detecting, preventing, and responding to suspected financial exploitation of vulnerable adults.

Table of Contents

1. Subject Matter Terms
 - Vulnerable Adult
 - Financial Exploitation
 - Elder Financial Abuse
 - Undue Influence
 - Caregiver Abuse
 - Power of Attorney
 - Conservator/Guardian
 - Trusted Contact Person
2. Legal and Regulatory Considerations
 - Federal Laws and Guidance
 - State Adult Protective Services Requirements
 - Privacy Considerations
 - Member Confidentiality
 - Documentation Standards
 - Record Retention
3. Governance and Risk Management
 - Board Oversight
 - Management Responsibilities
 - Written Policies
 - Risk Assessment
 - Internal Controls
4. Employee Training

- Annual Training Requirements
- Recognizing Behavioral Red Flags
- Transaction Red Flags
- Escalation Procedures
- Documentation Expectations

5. Recognizing Red Flags

- Member Behaviors
- Transaction Patterns
- Caregiver or Third-Party Behaviors
- Account Activity Indicators
- Digital Banking Warning Signs

6. Member Interaction Best Practices

- Speaking with the Member
- Asking Open-Ended Questions
- Private Conversations
- Assessing Capacity Without Diagnosing
- Respecting Member Independence

7. High-Risk Transactions

- Large Cash Withdrawals
- Wire Transfers
- Cashier's Checks
- Gift Card Purchases
- Cryptocurrency Transactions
- New Joint Owners
- Changes to Beneficiaries

- Adding Authorized Signers
- Opening New Accounts
- Safe Deposit Box Access

8. Responding to Suspected Exploitation

- Immediate Actions
- Supervisory Notification
- Fraud Department Review
- Documentation Requirements
- Temporary Holds (where permitted)
- When to Refuse or Delay a Transaction
- Member Follow-Up

9. Reporting Procedures

- Adult Protective Services
- Local Law Enforcement
- State Reporting Requirements
- Federal Reporting (when applicable)
- Suspicious Activity Reports (for applicable institutions)
- Internal Reporting Process

10. Working with Third Parties

- Powers of Attorney
- Guardians and Conservators
- Trustees
- Trusted Contacts
- Family Members
- Caregivers

11. Fraud Prevention Strategies

- Member Education
- Scam Awareness Campaigns
- Account Monitoring
- Transaction Alerts
- Dual Approval Processes
- Trusted Contact Programs

12. Documentation Standards

- Objective Note Taking
- Required Information
- Supporting Documentation
- Maintaining Confidentiality

13. Quality Assurance and Program Review

- Internal Audits
- Incident Reviews
- Trend Analysis
- Policy Updates
- Continuous Improvement

14. Job Aids

- Vulnerable Adult Red Flag Checklist
- Employee Response Flowchart
- Transaction Decision Tree
- Sample Documentation Form
- Sample Escalation Form
- Member Conversation Guide

- Trusted Contact Authorization Form
- Frequently Asked Questions
- Resource Directory
- Training Checklist

Subject Matter Terms

Vulnerable Adult

A vulnerable adult is an individual who, because of age, physical disability, cognitive impairment, developmental disability, mental illness, or other condition, may be unable to fully protect their own interests or manage their financial affairs and may be at increased risk of abuse, neglect, or financial exploitation. The legal definition may vary by state.

Financial Exploitation

Financial exploitation is the illegal or improper use of a person's money, assets, property, or financial resources for another person's benefit through deception, coercion, undue influence, intimidation, or abuse of trust.

Elder Financial Abuse

Elder financial abuse is a form of financial exploitation involving an older adult, typically age 60 or older (or as defined by state law). It includes theft, fraud, scams, forgery, misuse of authority, or the unauthorized or improper use of an older adult's financial resources.

Undue Influence

Undue influence occurs when an individual uses excessive pressure, manipulation, coercion, intimidation, or a position of trust to improperly influence another person's financial decisions, causing them to act contrary to their own best interests.

Caregiver Abuse

Caregiver abuse occurs when a person responsible for providing care or assistance to a vulnerable adult misuse their position to financially exploit, neglect, emotional abuse, physically abuse, or otherwise harm the individual.

Power of Attorney (POA)

A Power of Attorney is a legal document that authorizes one person (the agent or attorney-in-fact) to act on behalf of another person (the principal) in financial, legal, or other specified matters. The scope of authority depends on the terms of the document and applicable state law. A POA does not eliminate the principal's ownership or rights over their accounts.

Conservator/Guardian

A conservator or guardian is an individual or organization appointed by a court to manage the personal, financial, or legal affairs of a person who has been determined to be unable to do so independently. The authority granted is defined by the court order and applicable state law.

Trusted Contact Person

A trusted contact person is an individual designated by a member whom the credit union may contact if there are concerns about the member's well-being, suspected financial exploitation, diminished capacity, or difficulty reaching the member. A trusted contact does not have authority to conduct transactions or access account information unless separately authorized by the member.

Adult Protective Services (APS)

Adult Protective Services is a state or local government agency responsible for investigating reports of abuse, neglect, self-neglect, and financial exploitation involving vulnerable adults, and for coordinating protective services when appropriate. While this is the title of agencies currently in place in some states, they name may be different by state or locality.

Financial Capacity

Financial capacity refers to an individual's ability to understand financial information, make informed financial decisions, appreciate the consequences of those decisions, and manage their financial affairs. Credit union employees should not attempt to determine legal capacity but should recognize signs that may warrant additional review or escalation.

Scam

A scam is a deceptive scheme designed to trick an individual into voluntarily sending money, sharing sensitive information, or granting access to financial accounts under false pretenses. Common scams include romance scams, impersonation scams, lottery scams, investment fraud, tech support scams, and cryptocurrency schemes.

Exploiter

An exploiter is any individual or organization that improperly obtains or attempts to obtain a vulnerable adult's money, assets, or financial resources through fraud, deception, coercion, manipulation, abuse of trust, or other unlawful means. Exploiters may include strangers, family members, caregivers, acquaintances, or trusted professionals.

Red Flag

A red flag is any behavior, circumstance, transaction, or pattern of activity that may indicate a vulnerable adult is being financially exploited or is at increased risk of exploitation. While a single red flag may not confirm abuse, multiple indicators should prompt further review and appropriate escalation.

Legal and Regulatory Considerations

Federal Laws and Guidance

While there is no single federal law governing vulnerable adult financial protection, several federal laws, regulations, and interagency guidance establish expectations for financial institutions to detect, prevent, and report suspected financial exploitation. Credit unions should be familiar with applicable requirements issued by the National Credit Union Administration (NCUA), Financial Crimes Enforcement Network (FinCEN), Consumer Financial Protection Bureau (CFPB), and other regulatory agencies, as well as applicable provisions of the Bank Secrecy Act (BSA), anti-money laundering (AML) regulations, and state laws.

State APS Requirements

Each state has laws governing the reporting and investigation of suspected abuse, neglect, and financial exploitation of vulnerable adults. APS agencies are responsible for receiving and investigating reports and coordinating protective services. Credit unions should understand their state's reporting requirements, including whether financial institutions or employees are mandatory reporters, what information may be disclosed, and when reports should be made.

Privacy Considerations

Credit unions must balance the protection of vulnerable members with their obligation to safeguard member information. Applicable privacy laws generally permit the sharing of information with law enforcement, APS, or other authorized entities when allowed or required by law. Employees should disclose only the information necessary to fulfill legal or regulatory obligations and should follow established internal procedures before releasing member information.

Member Confidentiality

Members have the right to expect that their personal and financial information will be handled confidentially. Employees should avoid discussing suspected exploitation with unauthorized individuals, including family members who do not have legal authority over the account. Information regarding investigations or concerns should be shared only with individuals who have a legitimate business need or legal authority to receive it.

Documentation Standards

Accurate, objective, and timely documentation is essential whenever financial exploitation is suspected. Employees should record factual observations, member statements, transaction details, actions taken, and the reasons for any decisions made. Documentation should avoid personal opinions, assumptions, or medical conclusions and should clearly support the credit union's actions if reviewed by management, regulators, law enforcement, or the courts.

Record Retention

Records related to suspected financial exploitation should be retained in accordance with the credit union's record retention policy and all applicable federal and state legal and regulatory requirements. Documentation may include account records, transaction histories, copies of relevant documents, surveillance images, employee notes, internal reports, and communications related to the investigation. Maintaining complete and organized records supports regulatory compliance, law enforcement investigations, litigation, and future account reviews.

Governance and Risk Management

Effective governance and risk management provide the foundation for a credit union's vulnerable adult protection program. The board of directors and management are responsible for establishing a culture that prioritizes the detection and prevention of financial exploitation while ensuring compliance with applicable laws and regulations. A comprehensive program should include clearly defined responsibilities, written policies, employee training, risk assessments, and internal controls designed to identify, mitigate, and respond to potential financial exploitation.

Board Oversight

The board of directors is responsible for providing strategic oversight of the credit union's vulnerable adult protection program. This includes approving applicable policies, ensuring adequate resources are available, understanding the risks of financial exploitation, and receiving periodic reports regarding significant incidents, emerging fraud trends, training initiatives, and the effectiveness of the program. The board should promote a culture that emphasizes member protection, ethical conduct, and regulatory compliance.

Management Responsibilities

Executive management is responsible for implementing the board's direction by developing procedures, assigning responsibilities, providing employee training, and ensuring appropriate controls are in place to identify and respond to suspected financial exploitation. Management should establish clear escalation procedures, monitor compliance with policies, coordinate investigations, and periodically evaluate the effectiveness of the program through reporting, quality assurance, and ongoing risk assessments.

Written Policies

Credit unions should maintain written policies and procedures that establish consistent expectations for identifying, documenting, escalating, investigating, and reporting suspected financial exploitation. Policies should clearly define employee responsibilities, approval authorities, documentation requirements, reporting obligations, member communication protocols, and record retention practices. Policies should be reviewed and updated at least annually to reflect changes in laws, regulations, fraud trends, and operational practices.

Risk Assessment

Credit unions should periodically assess their exposure to vulnerable adult financial exploitation risks. The assessment should consider factors such as the member demographics, products and services offered, transaction channels, fraud trends, staffing, technology, and existing controls. The results should be used to identify areas of elevated risk, prioritize mitigation efforts, strengthen internal controls, and allocate resources appropriately.

Internal Controls

Internal controls are the policies, procedures, systems, and monitoring activities designed to prevent, detect, and respond to suspected financial exploitation. Examples include transaction monitoring, dual approval requirements for high-risk transactions, escalation protocols, supervisory review, employee training, exception reporting, documentation standards, account alerts, and periodic audits. Effective internal controls reduce risk, promote consistency, and help ensure that suspicious activity is identified and addressed in a timely manner.

Employee Training

Employees are the credit union's first line of defense against the financial exploitation of vulnerable adults. Effective training equips staff to recognize warning signs, respond appropriately, document concerns objectively, and escalate situations in accordance with established procedures. Training should be ongoing, role-based, and reinforced through regular communication and real-world examples.

Annual Training Requirements

All employees who interact with members or process financial transactions should receive initial and annual training on recognizing and responding to suspected financial exploitation of vulnerable adults. Training should be tailored to employee responsibilities, with enhanced instruction provided to frontline staff, call center personnel, lending staff, fraud investigators, branch management, and compliance personnel.

Training should cover applicable laws, credit union policies, common fraud schemes, red flags, documentation requirements, reporting obligations, and member communication techniques.

Best Practices

- Provide mandatory training for all employees upon hire and annually thereafter.
- Deliver role-specific training based on employee responsibilities.
- Incorporate current fraud trends and real case studies.
- Conduct periodic refresher training throughout the year.
- Test employee understanding through quizzes or scenario-based exercises.
- Maintain documentation of all completed training.
- Review training content annually and update it as fraud trends evolve.

Recognizing Behavioral Red Flags

Behavioral red flags are changes in a member's appearance, demeanor, decision-making, or interactions that may indicate financial exploitation, coercion, or diminished financial capacity. While no single behavior confirms exploitation, multiple indicators should prompt additional questions and supervisory review.

Best Practices

Employees should remain alert for situations such as:

- A member appears fearful, anxious, intimidated, or unusually nervous.
- A third-party refuses to allow the member to speak independently.
- The member appears confused about the purpose of a transaction.

- The member suddenly becomes accompanied by a new caregiver or acquaintance who directs financial decisions.
- The member expresses urgency based on threats, fear, or promises of financial gain.
- The member mentions online relationships, romance partners, government officials, celebrities, or investment opportunities requesting money.
- The member cannot clearly explain the purpose or recipient of a transaction.
- The member states they have been instructed not to tell anyone about the transaction.
- The member's financial habits change significantly without a reasonable explanation.

Employees should respectfully engage the member in conversation and, whenever possible, speak with the member privately before proceeding with high-risk transactions.

Transaction Red Flags

Certain transaction patterns are commonly associated with financial exploitation. Employees should evaluate unusual activity within the context of the member's normal account behavior and consider whether additional review is warranted.

Best Practices

Examples of transaction red flags include:

- Large or unusual cash withdrawals.
- Frequent cashier's checks or money orders.
- Wire transfers to unfamiliar individuals or overseas recipients.
- Multiple gift card purchases.
- Cryptocurrency-related transactions that are inconsistent with the member's history.
- Sudden liquidation of savings, certificates, or investment accounts.
- Adding joint owners or authorized signers without a clear explanation.
- Significant changes to beneficiary designations.
- Unusual ATM withdrawals or debit card usage.
- New online banking enrollment followed by high-dollar transfers.
- Multiple failed authentication attempts before successful account access.
- Transfers to recently opened accounts.

- Repeated transactions just below internal review thresholds.
- Transactions inconsistent with the member's historical activity.

Employees should not assume these transactions are fraudulent but should determine whether additional review or discussion is appropriate.

Escalation Procedures

Employees should never feel solely responsible for determining whether financial exploitation has occurred. Instead, they should promptly escalate concerns through established internal procedures so that trained personnel can evaluate the situation and determine appropriate next steps.

Best Practices

Credit unions should establish clear escalation procedures that include:

- Immediate notification of a supervisor when concerns arise.
- Prompt referral to the fraud, compliance, or risk management department.
- Clearly defined decision-making authority for delaying or declining transactions when permitted by law.
- Procedures for consulting legal counsel when appropriate.
- Guidance for reporting suspected exploitation to APS, law enforcement, or other agencies as required.
- Procedures for documenting all actions taken.
- Escalation contact information readily available to all employees.
- After-hours procedures for urgent situations.
- Periodic testing of escalation procedures to ensure employees understand their responsibilities.

Employees should never accuse a member or third party of fraud or exploitation and should avoid actions that could unnecessarily escalate the situation.

Documentation Expectations

Accurate documentation is essential for protecting members, supporting investigations, demonstrating regulatory compliance, and providing evidence if legal action becomes necessary. Documentation should be objective, factual, and completed as soon as practical after the interaction.

Best Practices

Employees should document:

- The date, time, and location of the interaction.

- Individuals present during the transaction.
- The member's statements using direct quotes whenever practical.
- Objective observations of behavior or circumstances.
- Details of the requested transaction.
- Questions asked and the member's responses.
- Actions taken by the employee.
- Supervisory notifications and recommendations.
- Any reports made to internal departments or external agencies.
- The final disposition of the transaction, if known.
-

Documentation should never include speculation, assumptions, personal opinions, or medical diagnoses. Employees should describe observable facts rather than attempting to determine whether a member lacks capacity or is being exploited.

Recognizing Red Flags

Early recognition of red flags is critical to preventing financial exploitation. Employees are often in the best position to identify unusual behaviors or transaction activity that may indicate a vulnerable adult is being manipulated, coerced, or victimized. While no single indicator confirms exploitation, multiple red flags occurring together should prompt additional review and appropriate escalation. Employees should evaluate each situation based on the member's normal behavior and transaction history and document objective observations.

Member Behaviors

Changes in a member's behavior, appearance, or ability to make financial decisions may indicate that they are being financially exploited or are experiencing diminished financial capacity. Employees should remain attentive to behaviors that are inconsistent with the member's normal interactions or suggest that another individual is exerting undue influence.

Best Practices

Employees should be alert for members who:

- Appear confused, disoriented, fearful, or unusually anxious.
- Seem intimidated or reluctant to speak openly.
- Frequently look to another individual before answering questions.
- Are unable to explain the purpose of a transaction.
- Express urgency due to threats, fear, or pressure.
- State they have been instructed to keep the transaction secret.
- Mention online relationships, romance partners, government officials, or investment opportunities requesting money.
- Demonstrate sudden changes in spending habits or financial decision-making.
- Appear withdrawn or reluctant to question unusual requests.
- Exhibit signs of neglect, poor hygiene, or physical distress that are inconsistent with previous visits.

Employees should respectfully engage the member in conversation and, when appropriate, request to speak with the member privately.

Transaction Patterns

Unusual or inconsistent transaction activity is often one of the earliest indicators of financial exploitation. Employees should consider whether the transaction aligns with the member's established financial habits and whether it appears reasonable based on information provided by the member.

Best Practices

Review transactions for patterns such as:

- Large cash withdrawals that are inconsistent with the member's history.
- Frequent cashier's checks or money orders.
- Multiple wire transfers to unfamiliar recipients.
- Purchases of large amounts of gift cards.
- Cryptocurrency transactions initiated by members with little or no prior experience.
- Sudden liquidation of savings, certificates, or investment accounts.
- Multiple transfers to newly established accounts.
- Repeated withdrawals shortly after deposits.
- Significant transactions benefiting a new acquaintance or caregiver.
- Transactions that appear structured to avoid internal review thresholds.
- Unusual activity immediately following the addition of a joint owner or authorized signer.

Employees should ask open-ended questions to better understand the purpose of unusual transactions before processing them.

Caregiver or Third-Party Behaviors

Individuals who accompany vulnerable adults may be legitimate caregivers, family members, or trusted advisors. However, financial exploitation frequently involves someone known to the member. Employees should remain alert for behaviors suggesting a third party is improperly influencing or controlling the member's financial decisions.

Best Practices

Be alert when a third party:

- Speaks for the member or refuses to allow the member to answer questions.
- Insists on remaining present during all conversations.
- Appears overly interested in the member's finances or account balances.
- Attempts to rush or pressure employees to complete transactions.
- Becomes angry or defensive when routine questions are asked.
- Requests access to accounts without appropriate legal authority.
- Encourages the member to make transactions inconsistent with their financial history.

- Frequently accompanies the member during significant financial transactions despite no prior involvement.
- Attempts to isolate the member from credit union staff or family members.
- Presents legal documents that appear altered, incomplete, or questionable.

Employees should verify all legal authorities, such as powers of attorney or guardianship orders, before granting account access or acting on instructions from third parties.

Account Activity Indicators

Account activity often provides objective evidence that a member may be experiencing financial exploitation. Monitoring for unusual changes in account usage can help identify suspicious activity before significant financial losses occur.

Best Practices

Watch for:

- Sudden increases in account activity.
- Large or frequent ATM withdrawals.
- Numerous overdrafts or insufficient funds.
- Unusual debit card spending patterns.
- New recurring electronic payments.
- Multiple transfers between accounts without a clear purpose.
- Addition or removal of account owners or beneficiaries.
- Changes to mailing addresses, email addresses, or telephone numbers shortly before significant transactions.
- Closure of long-standing accounts without an apparent reason.
- Checks written out of sequence or with significantly different handwriting.
- Increased requests for account statements or transaction histories by third parties.

Transaction monitoring systems should be configured, where feasible, to identify unusual account behavior and generate alerts for further review.

Digital Banking Warning Signs

As financial exploitation increasingly occurs through digital channels, employees should recognize warning signs associated with online banking, mobile banking, and electronic payment services. Account takeover schemes, impersonation scams, and remote access fraud frequently target vulnerable adults.

Best Practices

Monitor for indicators such as:

- Enrollment in online or mobile banking by a member who has never previously used digital services.
- Password resets or changes to security credentials followed by large transfers.
- Changes to multifactor authentication methods, email addresses, or telephone numbers.
- New external transfer accounts being added.
- Large electronic transfers shortly after new payees are established.
- Login attempts from unfamiliar devices or geographic locations.
- Multiple failed login attempts followed by successful account access.
- Significant increases in peer-to-peer payment activity.
- Requests to increase transaction limits without a reasonable explanation.
- Members reporting that someone instructed them to install remote access software or share one-time passcodes.
- Members stating they are receiving instructions from someone over the phone or online while completing transactions.

Credit unions should implement layered fraud detection tools, multifactor authentication, transaction monitoring, device recognition, and behavioral analytics to help identify potentially fraudulent digital banking activity.

Member Interaction Best Practices

Credit union employees play a critical role in protecting vulnerable adults while preserving the dignity, rights, and independence of every member. Conversations regarding unusual or potentially suspicious transactions should be conducted professionally, respectfully, and without assumptions. Employees should focus on understanding the purpose of the transaction, identifying potential signs of financial exploitation, and providing members with an opportunity to make informed financial decisions. The goal is not to interrogate the member, but to ensure they are acting voluntarily and understand the nature and consequences of the transaction.

Speaking with the Member

When concerns arise regarding a transaction, employees should engage the member in a calm, respectful, and non-confrontational conversation. The discussion should focus on understanding the member's intentions and identifying any indications of coercion, fraud, or undue influence. Employees should avoid accusatory language and should never suggest that the member is incapable of managing their finances.

Best Practices

Employees should:

- Speak calmly, respectfully, and without judgment.
- Address the member directly, even when another individual is present.
- Use language the member can easily understand.
- Explain that questions are being asked to help protect all members from fraud and scams.
- Allow the member sufficient time to respond without interruption.
- Observe both verbal and non-verbal cues.
- Remain patient and avoid creating a sense of urgency.
- Reassure the member that the credit union's priority is their financial well-being.
- Avoid confronting or accusing accompanying individuals of wrongdoing.

Asking Open-Ended Questions

Open-ended questions encourage members to explain transactions in their own words and often provide valuable information that may not be revealed through simple "yes" or "no" questions. These conversations can help employees identify potential scams, undue influence, or confusion while allowing members to maintain control of the discussion.

Best Practices

Employees should ask questions such as:

- "Can you tell me about this transaction?"

- "What do you plan to use these funds for?"
- "How did you become acquainted with the recipient?"
- "How long have you known this individual or organization?"
- "Has anyone asked you to keep this transaction confidential?"
- "Did someone instruct you to come to the credit union today?"
- "Has anyone pressured you to complete this transaction quickly?"
- "What would happen if you decided not to send the money today?"
- "Have you discussed this transaction with someone you trust?"

Employees should avoid leading questions or suggesting answers and should carefully listen for inconsistencies or indications of coercion.

Private Conversations

When a third party accompanies a member, it may be appropriate to speak with the member privately to determine whether they are acting voluntarily. A private conversation often allows members to express concerns they may be reluctant to discuss in the presence of another individual.

Best Practices

Whenever appropriate, employees should:

- Politely request an opportunity to speak with the member alone.
- Explain that private conversations are a standard procedure for certain transactions.
- Ensure the discussion occurs in a comfortable and confidential setting.
- Continue treating accompanying individuals professionally and respectfully.
- Observe whether the member's responses change when the third party is absent.
- Immediately escalate concerns if the accompanying individual refuses to allow a private conversation or becomes hostile.

Employees should never place themselves or the member in an unsafe situation.

Assessing Capacity Without Diagnosing

Credit union employees are not medical professionals and should never attempt to determine whether a member has diminished capacity or diagnose a medical condition. Their responsibility is limited to observing behaviors that may affect the member's ability to understand or authorize a transaction and documenting objective facts. If concerns arise, employees should follow established escalation procedures for further review.

Best Practices

Employees should:

- Focus on observable behaviors rather than medical conclusions.
- Determine whether the member appears to understand the nature and purpose of the transaction.
- Ask the member to explain the transaction in their own words.
- Note any confusion, inconsistency, or inability to describe the transaction.
- Document factual observations rather than opinions.
- Escalate concerns to management or the fraud department when appropriate.
- Follow established policies before delaying or declining a transaction.

Employees should never state or imply that a member is incompetent, mentally impaired, or incapable of making financial decisions.

Respecting Member Independence

Adults have the right to make their own financial decisions, including decisions that others may consider unwise, provided they are acting voluntarily and understand the consequences of their actions. Credit unions should balance fraud prevention with respect for member autonomy, privacy, and legal rights.

Best Practices

Credit unions should:

- Treat every member with dignity, courtesy, and respect.
- Presume members are capable of making their own financial decisions unless legal documentation indicates otherwise.
- Avoid stereotypes based on age, disability, or appearance.
- Provide information and education rather than directing a member's decision.
- Encourage members to consult trusted family members, legal advisors, or financial professionals when appropriate.
- Verify legal authority before discussing account information with family members or caregivers.
- Apply vulnerable adult protection procedures consistently to all members.
- Document concerns objectively while respecting member privacy.

The credit union's role is to educate, identify potential risks, and respond appropriately to suspected financial exploitation—not to make financial decisions on behalf of competent members.

High-Risk Transactions

Certain financial transactions present an increased risk for vulnerable adults because they may involve large transfers of funds, changes to account ownership, access by third parties, or payment methods commonly used in scams and financial exploitation schemes. While these transactions are not inherently suspicious, employees should consider the member's normal account activity, stated purpose of the transaction, relationship with involved parties, and any accompanying red flags. Credit unions should establish consistent procedures for reviewing high-risk transactions while respecting members' rights to make their own financial decisions. The goal is not to prevent legitimate transactions, but to identify situations where additional questions, education, documentation, or escalation may be appropriate.

Large Cash Withdrawals

Large cash withdrawals may be associated with legitimate member needs; however, cash is a common method used by scammers and exploiters because it is difficult to recover once provided to another person. Vulnerable adults may be pressured into withdrawing cash for romance scams, government impersonation scams, investment scams, or requests from caregivers or acquaintances.

Best Practices

Employees should:

- Understand the member's stated purpose for the withdrawal.
- Compare the transaction to the member's historical account activity.
- Ask open-ended questions about how the funds will be used.
- Watch for signs that another person is directing or pressuring the member.
- Educate members about common scams when appropriate.
- Consider additional review when:
 - The withdrawal is unusually large.
 - The member appears nervous or confused.
 - A new acquaintance or third party is involved.
 - The member states they were instructed to withdraw cash.

Credit unions should consider transaction monitoring alerts for unusual cash activity involving vulnerable adult accounts.

Wire Transfers

Wire transfers are a frequent method used in financial exploitation because funds are typically transferred quickly and may be difficult to recover. Scammers often use urgency, threats, romance, investment opportunities, or impersonation tactics to convince members to send wires.

Best Practices

Employees should:

- Confirm the member understands who will receive the funds and why.
- Ask how the member knows the recipient.
- Verify whether the member initiated the transaction independently.
- Watch for:
 - New wire recipients.
 - International wires inconsistent with account history.
 - Instructions from someone directing the member remotely.
 - Transfers related to investments, emergencies, or secrecy.
- Provide scam warnings when appropriate.
- Follow wire authorization and verification procedures.

Additional review should be considered when the member appears hesitant, confused, or unable to explain the purpose of the wire.

Cashier's Checks

Cashier's checks are often perceived as secure and are commonly requested in scams because they provide a trusted form of payment. Vulnerable adults may be persuaded to purchase checks for fake investments, fraudulent purchases, romance relationships, or impersonation schemes.

Best Practices

Employees should:

- Ask the purpose of the cashier's check.
- Confirm the recipient's relationship to the member.
- Be alert when checks are payable to unfamiliar individuals or businesses.
- Watch for requests involving:
 - Online relationships.
 - Prize or lottery winnings.

- "Overpayment" refund schemes.
- Investment opportunities.
- Requests to send funds to another person for safekeeping.
- Encourage members to verify the legitimacy of requests before sending funds.

Gift Card Purchases

Gift cards are frequently used in scams because they can be purchased quickly, transferred electronically, and are difficult to recover. Government impersonation, technology support scams, and romance scams often involve requests for gift cards.

Best Practices

Employees should ask questions when members purchase unusual amounts or quantities of gift cards, including:

- "Can you tell me what the gift cards are for?"
- "Did anyone instruct you to purchase these?"
- "Are you being asked to provide the gift card numbers or PINs?"
- "Has anyone told you to keep this transaction secret?"

Employees should be alert for:

- Multiple gift card purchases.
- Large-dollar purchases.
- Members who appear anxious or rushed.
- Instructions received by phone, email, or text.

Consider posting scam warnings near gift card purchase locations.

Cryptocurrency Transactions

Cryptocurrency-related fraud has increased significantly and often targets individuals unfamiliar with digital assets. Scammers may convince members to transfer funds to cryptocurrency platforms, ATMs, or wallets as part of fake investments, romance scams, or impersonation schemes.

Best Practices

Employees should:

- Ask whether the member understands cryptocurrency and the purpose of the transaction.
- Determine whether someone instructed the member to purchase cryptocurrency.
- Watch for:

- First-time cryptocurrency purchases.
- Large cryptocurrency ATM transactions.
- Transfers to unknown wallets.
- Members being coached while completing transactions.
- Promises of guaranteed returns.
- Educate members that legitimate government agencies and reputable businesses do not demand cryptocurrency payments.

New Joint Owners

Adding a joint owner gives another individual significant access and control over an account. While adding a joint owner is often appropriate for convenience or caregiving purposes, it can also create opportunities for financial exploitation.

Best Practices

Employees should:

- Confirm the member understands the rights being granted.
- Explain that joint owners may have access to funds and account information.
- Ask the member about the purpose of adding the individual.
- Verify that the request is voluntary.
- Be alert when:
 - A new acquaintance is being added.
 - The member appears pressured.
 - The individual requesting access answers questions for the member.
- Ensure required documentation is completed.

Employees should never assume a family relationship automatically means the arrangement is appropriate.

Changes to Beneficiaries

Changes to beneficiaries can significantly affect the distribution of a member's assets. Sudden or unusual beneficiary changes may be a warning sign of undue influence, especially when made in favor of new acquaintances or individuals with limited prior involvement.

Best Practices

Employees should:

- Confirm the member understands the change being requested.
- Ensure the member is acting voluntarily.
- Ask whether the member has discussed the change with trusted advisors or family members, if appropriate.
- Be alert for:
 - Frequent beneficiary changes.
 - Last-minute changes during illness or vulnerability.
 - Changes benefiting caregivers or new acquaintances.
 - Third parties directing the request.

Employees should follow the account agreement requirements and avoid providing legal advice.

Adding Authorized Signers

Adding an authorized signer provides another person with the ability to conduct certain transactions on an account. Improper access can expose vulnerable adults to unauthorized withdrawals or misuse of funds.

Best Practices

Employees should:

- Explain the authority being granted.
- Confirm the member understands the access provided.
- Verify identity and authorization requirements.
- Ask whether the member initiated the request.
- Watch for:
 - Third parties controlling the conversation.
 - Pressure to add access quickly.
 - Individuals seeking access without a clear need.

Opening New Accounts

New accounts can be used by exploiters to gain access to a vulnerable adult's funds or establish channels for fraudulent activity. Changes in account relationships or unusual account openings may warrant additional attention.

Best Practices

Employees should:

- Verify identity and account ownership.
- Understand the purpose of the new account.
- Confirm who will have access.
- Watch for:
 - Accounts opened immediately after a scam event.
 - Third parties directing account setup.
 - Unusual requests for account access.
 - Rapid movement of funds after opening.

Follow standard account opening procedures and apply enhanced review when red flags exist.

Safe Deposit Box Access

Safe deposit boxes may contain valuable assets, documents, or personal property. Changes in access rights or unusual activity may create opportunities for exploitation.

Best Practices

Employees should:

- Verify authorized access before granting entry.
- Maintain accurate access records.
- Monitor unusual changes in authorized users.
- Be alert when:
 - A new individual is added shortly before a member's decline in health.
 - A third party seeks access without proper authority.
 - There are disputes among family members or potential heirs.
- Follow established procedures for guardians, powers of attorney, and estate representatives.

Responding to Suspected Exploitation

When a credit union identifies potential financial exploitation of a vulnerable adult, a timely, consistent, and well-documented response is essential. Employees should focus on protecting the member while respecting the member's rights, maintaining confidentiality, and following applicable laws and internal procedures. The purpose of the response process is not to determine guilt or make assumptions, but to gather information, assess risk, and take appropriate action to prevent or minimize financial harm.

Immediate Actions

The first response to suspected exploitation can significantly impact the member's financial safety. Employees should take immediate steps to gather information, ensure the member is safe, and prevent further unauthorized or suspicious activity when appropriate and permitted.

Best Practices

Employees should:

- Remain calm, professional, and supportive when interacting with the member.
- Avoid confronting or accusing the suspected exploiter.
- Ask questions to better understand the circumstances surrounding the transaction.
- Determine whether the transaction is pending, completed, or can still be stopped.
- Identify whether additional suspicious activity may be occurring on the account.
- Protect sensitive member information from unauthorized individuals.
- Follow established escalation procedures without unnecessary delay.
- Prioritize employee and member safety if the situation becomes confrontational.

Credit unions should provide employees with clear procedures for handling urgent situations, including after-hours escalation contacts.

Supervisory Notification

Frontline employees should not be expected to independently determine whether exploitation has occurred. Prompt notification of a supervisor ensures that concerns are reviewed consistently and that appropriate resources are involved.

Best Practices

Credit unions should establish procedures requiring employees to notify appropriate personnel when concerns arise, including:

- Branch management or supervisors.
- Fraud, risk management, compliance, or security departments.

- Designated vulnerable adult protection contacts.
- Senior management when significant financial loss or reputational risk exists.

Supervisors should:

- Review the facts objectively.
- Ensure documentation is completed.
- Determine whether additional review is necessary.
- Confirm that appropriate escalation steps are followed.
- Avoid dismissing concerns without adequate review.

Fraud Department Review

A fraud or risk department review provides a structured evaluation of the circumstances surrounding suspected exploitation. Trained personnel can analyze account activity, transaction history, member information, and available evidence to determine appropriate next steps.

Best Practices

Fraud personnel should:

- Review recent account activity and transaction history.
- Identify patterns consistent with scams, coercion, or unauthorized activity.
- Review related accounts or connected relationships, when appropriate.
- Evaluate whether account takeover, identity theft, or other fraud schemes may be involved.
- Review supporting documentation and employee observations.
- Determine whether additional monitoring or controls are appropriate.
- Coordinate with compliance, legal counsel, law enforcement, or APS when necessary.

Reviews should be documented with sufficient detail to demonstrate the basis for decisions made.

Documentation Requirements

Complete and objective documentation is critical when responding to suspected exploitation. Documentation supports internal decision-making, regulatory review, law enforcement inquiries, and future account monitoring.

Best Practices

Documentation should include:

- Date, time, and location of the interaction.
- Names and roles of individuals involved.

- Description of the transaction or activity.
- Specific behaviors or statements observed.
- Member responses to questions asked.
- Names of employees involved in the review.
- Actions taken and decisions made.
- Notifications provided internally or externally.
- Supporting documentation, when applicable.

Employees should document facts, not conclusions. For example, document that a member stated, “My grandson told me I must send this money today,” rather than documenting that the member was “being scammed” unless confirmed through the investigation.

Temporary Holds (Where Permitted)

In certain circumstances and where authorized by law, credit unions may be permitted to delay or place temporary holds on transactions when there is a reasonable belief that financial exploitation may be occurring. These actions must be carefully managed to balance member protection with the member’s right to access their funds.

Best Practices

Credit unions should:

- Understand applicable federal and state laws regarding transaction delays or holds.
- Establish written procedures outlining when holds may be considered.
- Define approval authority for delaying transactions.
- Document the reason for any delay or hold.
- Provide required notices to the member when applicable.
- Monitor the situation and complete reviews promptly.
- Avoid unnecessary delays that could negatively impact members.

Employees should never place holds outside established authority or procedures.

When to Refuse or Delay a Transaction

A credit union should generally avoid refusing transactions solely because they appear unusual or because employees believe a member is making a poor financial decision. However, transactions may warrant delay or refusal when permitted by law, when required by account agreements, or when there is sufficient concern regarding fraud, legal authority, or account restrictions.

Best Practices

A transaction may warrant additional review when:

- The member appears to lack understanding of the transaction.
- The transaction appears to be the result of coercion or undue influence.
- The person requesting the transaction lacks proper authority.
- The transaction involves suspected fraud or unauthorized activity.
- The member indicates they are being threatened, pressured, or instructed by another person.
- Required documentation or legal authority is missing or questionable.
- The transaction violates applicable laws, regulations, or credit union policies.

Before delaying or refusing a transaction, employees should:

- Consult established procedures.
- Escalate to appropriate personnel.
- Document the facts supporting the decision.
- Apply procedures consistently.

Member Follow-Up

Follow-up after a suspected exploitation event helps protect the member from continued harm and reinforces the credit union's commitment to member well-being. Follow-up should be conducted carefully to avoid creating additional risk or compromising an investigation.

Best Practices

Credit unions should consider:

- Contacting the member to confirm their safety and understanding of the situation.
- Reviewing account security settings and available fraud prevention tools.
- Educating the member about common scams and warning signs.
- Offering resources such as trusted contacts, fraud alerts, or account monitoring tools.
- Confirming that suspicious activity has stopped.
- Monitoring the account for continued unusual activity.
- Documenting follow-up efforts and outcomes.

Follow-up communications should be handled discreetly and should avoid revealing confidential information to unauthorized individuals.

Reporting Procedures

A consistent reporting process ensures that suspected financial exploitation is identified, reviewed, documented, and escalated appropriately. Reporting procedures should provide employees with clear direction on when concerns should be reported, who is responsible for review, and what information should be included. The goal of reporting is to protect members, support investigations, comply with applicable laws, and ensure appropriate action is taken.

APS

APS agencies investigate allegations of abuse, neglect, exploitation, or self-neglect involving vulnerable adults. APS involvement may be appropriate when a credit union suspects that a member is being financially exploited or is unable to protect their own interests.

Best Practices

Credit unions should:

- Understand applicable state APS reporting requirements.
- Maintain current APS contact information.
- Establish procedures for determining when a report should be made.
- Document the facts supporting the report.
- Provide requested information when legally permitted.
- Coordinate with compliance or legal counsel when appropriate.
- Avoid notifying suspected exploiters that a report has been made when doing so could increase risk to the member.

Local Law Enforcement

Law enforcement involvement may be appropriate when exploitation involves suspected theft, fraud, identity theft, threats, coercion, forgery, or other criminal activity. Law enforcement can assist with investigations, recovery efforts, and protection of the member.

Best Practices

Credit unions should:

- Contact law enforcement when criminal activity is suspected or required by policy or law.
- Provide relevant documentation and account records when authorized.
- Preserve evidence such as transaction records, surveillance, communications, and supporting documents.
- Maintain records of law enforcement contacts and responses.
- Coordinate communications through designated personnel.

State Reporting Requirements

State laws vary regarding reporting obligations, permissible disclosures, immunity protections, and procedures for financial institutions reporting suspected exploitation. Credit unions should understand requirements applicable in each state where they operate.

Best Practices

Credit unions should:

- Maintain a current state reporting matrix.
- Identify whether employees or the institution have mandatory reporting obligations.
- Define required timelines and procedures.
- Train employees on applicable requirements.
- Consult legal counsel when requirements are unclear.
- Periodically review state law changes.

Federal Reporting (When Applicable)

Federal regulations and guidance provide expectations for financial institutions regarding detection and reporting of suspicious activity and financial exploitation. Certain situations may require reporting to federal agencies or compliance with federal requirements.

Best Practices

Credit unions should:

- Understand applicable federal guidance.
- Coordinate vulnerable adult exploitation reviews with BSA/AML processes when appropriate.
- Ensure reporting decisions are made by qualified personnel.
- Maintain confidentiality regarding regulatory filings.
- Avoid unnecessary disclosure of internal investigations.

Suspicious Activity Reports (SARs) (For Applicable Institutions)

SARs may be required when transactions involve known or suspected violations of law, including fraud, theft, money laundering, or other suspicious activity. Financial exploitation may be a factor considered during SAR review.

Best Practices

Credit unions should:

- Follow established BSA/AML procedures.
- Evaluate whether suspected exploitation meets SAR filing criteria.

- Document the basis for SAR decisions.
- Coordinate between fraud, BSA, and compliance departments.
- Maintain SAR confidentiality.
- Avoid disclosing SAR filings to members or unauthorized individuals.

Internal Reporting Process

An internal reporting process ensures concerns are reviewed consistently and routed to individuals with appropriate expertise and authority.

Best Practices

Credit unions should establish:

- A designated reporting channel.
- Clear escalation responsibilities.
- Defined investigation ownership.
- Required documentation standards.
- Response timelines.
- Management reporting expectations.
- Tracking and trending of reported concerns.

Employees should feel empowered to report concerns without fear of criticism or retaliation.

Working With Third Parties

Third parties may play an important role in assisting vulnerable adults with financial matters. However, individuals with legitimate access can also present risk if authority is misused. Credit unions should verify authority, understand account relationships, and remain alert for potential exploitation.

Powers of Attorney (POA)

A Power of Attorney allows an individual (agent) to act on behalf of another person (principal) regarding financial or legal matters. The authority granted depends on the document and applicable law.

Best Practices

Credit unions should:

- Verify the validity and authority granted by the POA.
- Review documentation according to established procedures.
- Understand whether authority is immediate, limited, or durable.
- Monitor unusual activity conducted by agents.
- Confirm transactions are consistent with the member's interests.
- Document concerns regarding potential misuse.

Guardians and Conservators

Guardians and conservators are court-appointed individuals authorized to manage personal or financial affairs for someone determined to require assistance.

Best Practices

Credit unions should:

- Obtain and verify court documentation.
- Understand the scope of authority granted.
- Maintain current records.
- Monitor transactions for unusual activity.
- Follow court orders and applicable laws.
- Escalate concerns regarding misuse of authority.

Trustees

A trustee manages assets held in a trust according to the terms of the trust agreement and applicable law.

Best Practices

Credit unions should:

- Verify trustee authority.

- Review trust documents as required.
- Confirm transactions align with trust purposes.
- Maintain appropriate documentation.
- Escalate concerns regarding misuse of trust assets.

Trusted Contacts

A trusted contact is an individual authorized by the member to be contacted if concerns arise regarding suspected exploitation, unusual activity, or difficulty reaching the member. A trusted contact does not have account access unless separately authorized.

Best Practices

Credit unions should:

- Offer trusted contact programs to members.
- Clearly explain the purpose and limitations.
- Obtain proper authorization.
- Document contact information.
- Use trusted contacts appropriately.

Family Members

Family members may provide valuable support; however, family relationships alone do not grant authority to access accounts or receive confidential information.

Best Practices

Credit unions should:

- Verify legal authority before sharing information.
- Avoid assuming family members have the member's best interests.
- Maintain confidentiality.
- Treat concerns objectively regardless of relationship.

Caregivers

Caregivers often assist vulnerable adults with daily needs but may also create opportunities for financial exploitation.

Best Practices

Employees should:

- Verify caregiver authority.

- Watch for controlling or coercive behavior.
- Ensure the member's wishes are independently understood.
- Escalate concerns regarding unusual financial activity.

Fraud Prevention Strategies

A proactive fraud prevention program helps credit unions identify risks before financial harm occurs. Prevention strategies should combine employee awareness, member education, technology solutions, transaction monitoring, and strong internal controls. The goal is to reduce opportunities for exploitation while maintaining member trust and respecting member independence.

Member Education

Educating members is one of the most effective ways to prevent financial exploitation. Members who understand common scams, warning signs, and available protection tools are better equipped to recognize and avoid fraudulent activity.

Best Practices

Credit unions should:

- Provide ongoing fraud prevention education.
- Share information through statements, newsletters, websites, social media, and branch materials.
- Focus education on common scams affecting vulnerable adults.
- Encourage members to contact the credit union before sending large or unusual payments.
- Explain available security features and account protections.
- Provide resources in formats accessible to all members.

Scam Awareness Campaigns

Scam awareness campaigns help members recognize emerging fraud trends and understand how scammers manipulate victims. Frequent communication reinforces awareness and demonstrates the credit union's commitment to member protection.

Best Practices

Credit unions should:

- Regularly communicate current scam trends.
- Highlight common schemes, including:
 - Romance scams
 - Government impersonation scams
 - Technology support scams
 - Investment scams
 - Family emergency scams

- Cryptocurrency scams
- Provide examples of scam tactics and warning signs.
- Display fraud warnings near high-risk transaction areas.
- Update messaging as new fraud trends emerge.

Account Monitoring

Account monitoring helps identify unusual activity that may indicate financial exploitation, account takeover, or fraud. Monitoring should consider the member's normal behavior and transaction history.

Best Practices

Credit unions should consider monitoring for:

- Unusual changes in transaction patterns.
- Large withdrawals that are inconsistent with history.
- Frequent transfers to new recipients.
- Changes in account ownership or access.
- Increased electronic payments.
- Activity following changes to contact information.
- Transactions involving known scam indicators.

Monitoring tools should support employee review rather than replace human judgment.

Transaction Alerts

Transaction alerts provide an additional layer of protection by notifying members or employees when certain account activity occurs. Alerts can help identify unauthorized activity quickly and encourage members to report concerns.

Best Practices

Credit unions should offer or consider:

- Debit card transaction alerts.
- Large withdrawal alerts.
- Wire transfer notifications.
- Online banking security alerts.
- Changes to account access information.
- New payee or external transfer alerts.

Alerts should be easy for members to understand and available through preferred communication channels.

Dual Approval Processes

Dual approval controls require review or authorization by more than one employee before completing certain high-risk transactions or account changes. These controls reduce errors, misconduct, and opportunities for exploitation.

Best Practices

Credit unions should consider dual approval for:

- Large cash withdrawals.
- Significant account changes.
- Removal or addition of account owners.
- High-risk wire transactions.
- Exceptions to established procedures.

Approval requirements should be clearly documented and consistently applied.

Trusted Contact Programs

Trusted contact programs provide credit unions with an additional resource when concerns arise regarding a member's well-being, suspected exploitation, or difficulty contacting the member. A trusted contact does not have authority over the member's account unless separately authorized.

Documentation Standards

Accurate documentation supports member protection, regulatory compliance, investigations, and future account reviews. Documentation should be completed promptly and contain objective facts.

Objective Note Taking

Objective documentation records what occurred without assumptions, opinions, or conclusions. Clear documentation allows another reviewer to understand the circumstances and decisions made.

Best Practices

Employees should:

- Record facts, not opinions.
- Use direct quotes when possible.
- Describe observable behaviors.
- Include dates, times, and individuals involved.
- Avoid medical conclusions or statements about capacity.
- Avoid labeling individuals as scammers or exploiters unless confirmed.

Required Information

Consistent documentation ensures that important details are captured during reviews.

Best Practices

Documentation should include:

- Member name and account information.
- Date and time of concern.
- Transaction details.
- Individuals involved.
- Member statements.
- Employee observations.
- Questions asked and responses received.
- Actions taken.
- Internal notifications.
- Final disposition.

Supporting Documentation

Supporting documentation strengthens investigations and provides evidence of actions taken.

Best Practices

Maintain, when applicable:

- Transaction records.
- Account history.
- Copies of documents provided.
- Surveillance footage.
- Call recordings.
- Emails or communications.
- Investigation notes.
- Reports made to outside agencies.

Records should be maintained according to applicable retention requirements.

Maintaining Confidentiality

Information related to suspected exploitation must be handled carefully to protect member privacy and comply with applicable laws.

Best Practices

Employees should:

- Share information only with individuals who have a legitimate business need.
- Avoid discussing investigations with unauthorized individuals.
- Protect member information during internal and external communications.
- Follow privacy and confidentiality policies.
- Maintain confidentiality regarding regulatory filings.

Quality Assurance and Program Review

A strong vulnerable adult protection program requires ongoing evaluation to ensure policies, procedures, training, and controls remain effective.

Internal Audits

Internal audits provide independent evaluation of whether the credit union's program is operating effectively and consistently.

Best Practices

Audits should review:

- Policy compliance.
- Employee training completion.
- Documentation quality.
- Reporting procedures.
- Escalation practices.
- Case management processes.
- Control effectiveness.

Incident Reviews

Reviewing suspected exploitation incidents helps identify lessons learned and opportunities for improvement.

Best Practices

Credit unions should:

- Conduct post-incident reviews.
- Identify root causes.
- Evaluate response effectiveness.
- Determine whether controls operated as intended.
- Update procedures when needed.
- Share lessons learned through training.

Trend Analysis

Trend analysis identifies patterns and emerging risks by reviewing reported cases, losses, transaction activity, and member concerns.

Best Practices

Credit unions should monitor:

- Types of exploitation attempts.
- Transaction methods used.
- Common scam themes.
- Employee escalation patterns.
- Member demographics affected.
- Control weaknesses.

Policy Updates

Policies should evolve as fraud trends, regulations, technology, and member needs change.

Best Practices

Credit unions should:

- Review policies periodically.
- Update procedures based on lessons learned.
- Incorporate regulatory changes.
- Obtain appropriate approval.
- Communicate updates to employees.

Continuous Improvement

A mature vulnerable adult protection program continually evaluates effectiveness and identifies opportunities to strengthen member protection.

Best Practices

Credit unions should:

- Encourage employee feedback.
- Evaluate training effectiveness.
- Review fraud trends.
- Enhance technology controls.
- Benchmark against industry practices.
- Maintain a culture of prevention and awareness.

Job Aids

Job Aids provide practical tools employees can use when identifying, documenting, and responding to suspected exploitation.

Vulnerable Adult Red Flag Checklist

A checklist of behavioral, transaction, and account activity indicators employees can reference during member interactions.

Best Practices:

- Keep easily accessible.
- Update periodically.
- Use as a guide, not a replacement for judgment.

Employee Response Flowchart

A visual guide that outlines steps employees should take when concerns arise.

Best Practices:

- Include escalation contacts.
- Clearly identify decision points.
- Provide branch and after-hours procedures.

Transaction Decision Tree

A step-by-step guide to help employees determine when additional questions, escalation, or review may be appropriate.

Best Practices:

- Include high-risk transaction examples.
- Align with policies and legal requirements.

Sample Documentation Form

A standardized form to capture concerns consistently.

Best Practices:

Include:

- Member information.
- Transaction details.
- Observations.
- Actions taken.

- Escalation details.

Sample Escalation Form

A tool for employees to report concerns to management or fraud personnel.

Best Practices:

- Provide clear instructions.
- Require factual information.
- Maintain confidentiality.

Member Conversation Guide

A resource to help employees conduct respectful conversations.

Best Practices:

Include:

- Suggested questions.
- Communication tips.
- Scam education talking points.

Trusted Contact Authorization Form

A form allowing members to designate individuals the credit union may contact under specific circumstances.

Best Practices:

- Clearly explain limitations.
- Obtain member authorization.
- Maintain records securely.

Frequently Asked Questions

A resource addressing common employee and member questions.

Resource Directory

A centralized list of helpful resources.

May include:

- APS contacts.
- Law enforcement contacts.
- Fraud prevention resources.

- Regulatory guidance.
- Community assistance organizations.

Training Checklist

A tool to confirm employees have completed required training.

May include:

- Employee name.
- Training date.
- Topics completed.
- Assessment results.
- Trainer or system verification.