

Carefull

# Stop Elder Fraud

## A Checklist for Credit Unions

Now more than ever, credit unions should be taking a comprehensive approach to combat the growing threat of elder financial exploitation.

Losses to elder fraud are estimated to be as high as $61.5 billion annually when accounting for underreporting of incidents, according to the Federal Trade Commission. In fact, the scope of the problem is so great that federal and state financial regulatory agencies recently issued a directive urging financial institutions to adopt a range of strategies to prevent financial exploitation of older adults.

**The following checklist can help:**

- ◯ Train staff to detect and report elder exploitation
- ◯ Adopt comprehensive financial monitoring
- ◯ Know the warning signs of exploitation
- ◯ Educate members on fraud avoidance
- ◯ Leverage trusted contacts
- ◯ Monitor for changes in cognitive or behavioral patterns
- ◯ Offer member-side scam tools

## Train staff to detect and report elder exploitation

Frontline employees are often the first line of defense in identifying exploitation. Comprehensive training ensures they are equipped to recognize, respond, and report red flags before irreversible harm is caused. The Senior Safe Act shields financial institutions and certain employees from lawsuits if they report suspected fraud to law enforcement, as long as they have completed proper training.



**Foundational awareness of elder exploitation**

- Define elder financial exploitation and differentiate it from other types of fraud.
- Discuss vulnerabilities that put older adults at risk, such as isolation, cognitive decline, and reliance on others for caregiving support.

**Approaches to prevent exploitation**

- Train staff to build relationships, especially with older or isolated account holders.
- Reinforce the importance of creating a safe environment where older members feel comfortable asking questions and raising concerns.

**Strategies to detect transactional and behavioral red flags of exploitation. Procedures to intervene and report suspected cases**

- In states with "hold" laws, provide guidelines for delaying transactions when financial exploitation is suspected.
- Outline steps for reporting suspected exploitation to appropriate federal, state, and local authorities and filing Suspected Activity Reports with FinCEN.Outline.
- Ensure staff understand protections under the Senior Safe Act and applicable state laws.

## Adopt comprehensive financial monitoring

Because fraudsters are increasingly bypassing traditional defenses by manipulating consumers directly, credit unions must go beyond traditional approaches and invest in technologies built to detect socially engineered scams.

An effective fraud prevention platform requires the following:

- Comprehensive monitoring across financial accounts, credit, home title, and identity
- Behavioral analytics powered by machine learning to spot subtle changes in how members interact with their accounts—such as unusual withdrawal patterns, abnormal transaction timing, or high-risk transfer behavior
- Alerts with actionable instructions to address issues that have been identified
- User friendly, accessible interfaces



## Know the warning signs of fraud and exploitation

Elder financial exploitation can involve fraud committed by strangers or the improper or illegal use of older adults' funds by people they know. Ensure every member-facing employee of your credit union is aware of these warning signs by routinely sharing this list.

- Large, frequent, or unexplained account withdrawals or transfers
- Withdrawals from dormant accounts
- New joint accounts opened or new names added to existing accounts
- Unexplained credit card charges or new credit card accounts opened
- Frequent non-sufficient fund activity or unpaid bills
- Attempts to wire large sums of money
- Purchases of a large number of gift cards
- Sudden interest in buying cryptocurrency
- Closing CDs or other accounts without regard to penalties
- Suspicious signatures on checks, or checks written as "loans" or "gifts"
- Previously uninvolved relatives or friends taking an interest in a member's finances
- Unexplained transfer of assets to a family member or someone outside the family
- Changes to legal documents or trusted contact designations
- Uncharacteristic new transactions involving cash apps, money transfer services, or online platforms
- The member is accompanied by someone who appears overly controlling
- Multiple declined login attempts or password resets on accounts
- Changes in member behavior or appearance



## Educate members on fraud avoidance

A study by the FINRA Investor Education Foundation found that those who know about a particular type of scam or fraud are 80% less likely to engage with it. That's why keeping members informed about the latest tactics used by scammers can protect them from exploitation.

**Member awareness programs can include:**

- In-branch materials and workshops
- Email newsletters
- Scam simulations and interactive learning tools
- Educational webinars
- Social media campaigns
- Articles and scam alerts on bank websites and in member account dashboards

According to FINRA, people are less likely to be victimized if they have someone with whom they can discuss suspicious offers.

## Monitor for Changes in Cognitive or Behavioral Patterns

Fraud prevention isn't just about watching the money, it's also about watching for changes in the people managing it. One of the most subtle and serious risks to older account holders is cognitive decline, which can make individuals more susceptible to scams, coercion, and financial errors. Credit unions should integrate tools and procedures to monitor for behavioral anomalies that may indicate such decline.

**Key indicators include:**

- Repetitive or confused behavior at the branch or over the phone
- Missed payments by typically diligent members
- Significant changes to spending patterns
- New and unusual account types and peer-two-peer payments
- Difficulty understanding banking processes they previously managed with ease
- Sudden reliance on others for decision-making

By leveraging behavioral analytics and machine learning through a fintech solution, institutions can identify these patterns and prompt soft interventions, such as outreach or involving a trusted contact, before exploitation occurs or continues. Pairing this technology with staff training can help humanize alerts while enhancing protection.

## Leverage trusted contacts



Credit unions should adopt a policy of requesting that members name a trusted contact—a person institutions can reach out to if they notice signs of fraud, exploitation, or cognitive decline. Trusted contacts do not have access to the member's money, but they can serve as an early point of intervention when something seems off.

Naming trusted contacts offers multiple benefits:

- An opportunity to help older adults identify the people who will be their first line of defense against exploitation.
- It supports safer aging without compromising financial independence.
- An opportunity for credit unions to ask members to invite their trusted contacts to a branch to establish a relationship with them and provide them with guidance on protecting their loved ones from fraud and exploitation.



## Offer Member-Side Scam Tools

One example is Carefull ScamCheck, an AI-driven solution that allows users to upload, copy/paste, or forward suspicious texts, emails, or social media messages to receive an instant scam risk rating.

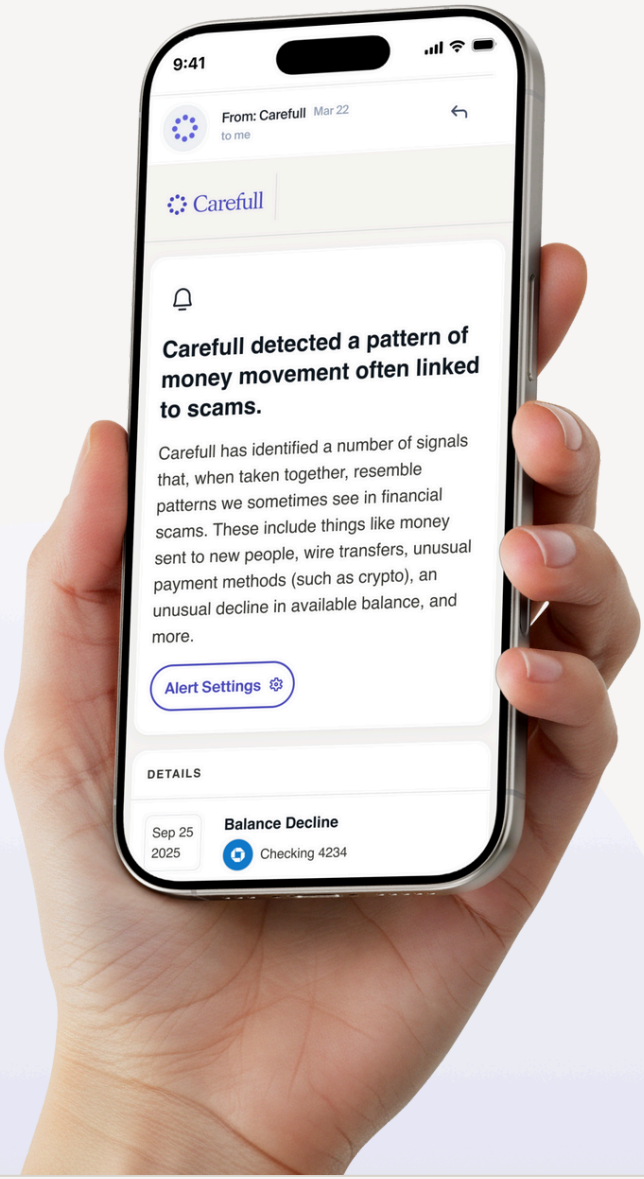
Empowering members with proactive protection tools is essential in the fight against modern fraud tactics. Credit unions should implement member-facing tools that enable members to screen suspicious communications before any damage is done.

These tools provide:

- Immediate feedback on scam likelihood, with reasons why
- Clear next steps, including how to disengage and report the incident
- Educational insight into the techniques and manipulation used

Offering such member-side resources not only protects members but also reduces fraud-related inquiries and enhances the credit union's reputation as a proactive partner in financial safety.

## A platform to protect vulnerable members




Credit unions looking to protect older adults from elder fraud can get a comprehensive solution with Carefull. Carefull is the first digital platform built to protect the daily finances of older adults and to allow for secure sharing and coordination with those they trust. Careful includes:

- 24/7 monitoring of bank, credit card, and investment accounts for signs of fraud, scams, and money mistakes
- Credit, identity, and home title monitoring
- $1 million in identity theft insurance
- Trusted Contacts infrastructure for members to add trusted contacts to their accounts and grant varying levels of view-only permissions
- Carefull ScamCheck, an AI-powered tool that allows users to upload or forward suspicious texts, emails, or messages to receive an instant scam risk assessment and step-by-step resolution guidance
- A military-grade password and document manager that stores sensitive information in one safe, accessible place
- Integrated consumer education that includes timely articles, scam alerts, and weekly activity summary emails—plus, educational webinars for credit union members
- A dedicated care team trained to work with older adults and their families, providing expert guidance on fraud resolution, account questions, digital navigation, and more

Carefull can help reduce financial losses, build trust and give your credit union a competitive advantage while protecting members from irreversible harm.

To learn more about how Carefull can help protect your members from elder fraud request a demo today.
**getcarefull.com**