2 Practical Ways For Banks To Battle Elder Financial Abuse

By **Michael Krebs, Daniel Hartman and Nick Stabile** (March 10, 2025)

Michael Krebs

Daniel Hartman

Nick Stabile

On Dec. 4, five federal financial regulatory agencies,[1] the Financial Crimes Enforcement Network and state financial regulators issued an interagency statement on elder financial exploitation.

The purpose of the statement was to provide depository institutions with examples of risk management practices that can be effective in identifying, preventing and responding to elder financial exploitation.[2]

Importantly, the statement does not replace any existing guidance on this issue, nor does it create any new compliance standards on this topic. Instead, the statement is meant to raise awareness of the issue of elder financial exploitation.

To that end, it provides a useful catalog of resources and techniques that many depository institutions currently employ, including governance and oversight, employee training, transaction holds, so-called trusted contact systems for account holders, law enforcement engagement, and consumer awareness.

As baby boomers age and criminal groups around the world use advanced technologies like AI to create complex scams, it is increasingly important for banks and credit unions to adopt and improve best-in-class methods to prevent elder financial exploitation.

Today's scams are increasingly difficult to detect and combat, and are nearly impossible to reverse once they have ensnared a victim.

Based on our industry experience, we believe two of the techniques highlighted in the statement have the greatest potential to be most practically effective.

First, encouraging older account holders to establish trusted contacts, when paired with complementary account terms and conditions, will permit a depository institution to pump the brakes if a trusted contact has not been specified, cannot be contacted, or cannot confirm to the depository institution that a proposed payment or funds transfer evidently is for a legitimate purpose.

Second, encouraging collective action by the depository industry to timely share warnings about the latest scams with their customers and to sponsor engaging public service announcements across various media platforms can promote customer awareness of online financial scams.

Background

Many have a story of an older loved one facing one of these schemes.

For example, using AI, criminals can scour the internet to develop a profile of someone and

create an uncanny imitation of their voice, and then call pretending to be a loved one in a desperate situation in which they need money immediately. They claim they've been falsely arrested and need bail money now, emphasizing that their parents can't know about the situation.

But, if older customers are already familiar with these types of scams, they know techniques to mitigate the risk and begin probing the caller with questions only the loved one could answer.

Elder financial exploitation is an ever-growing problem. The statement notes that, according to AARP, older Americans fall victim to financial exploitation to the tune of $28.3 billion annually.

FinCEN says that financial institutions filed 155,415 reports of suspicious activity involving financial exploitation from June 2022 to June 2023.[3] The statement defines elder financial exploitation as "the illegal use of an older adult's funds or other resources for the benefit of an unauthorized recipient."

FinCEN, on the other hand, distinguishes between two types of elder financial exploitation: (1) theft by the transfer of assets by an older person to a trusted person; or (2) scams where the older person transfers assets to a stranger or imposter for something promised but not received.[4] This article focuses on the latter.

In addition to so-called person-in-need scams like the emergency phone call from a family member anxiously pleading for money, older customers face a myriad of other online threats.

For example, an older customer could be convinced that they have won a sweepstakes and that they must send either money or their financial account information to receive their winnings.

Or, someone may be told that their bank account has been associated with a heinous crime such as child pornography and, to avoid having their funds blocked indefinitely, the customer must withdraw all of their deposits from the bank and transfer the funds to a "federal locker" (which of course has never existed), often by physically handing cash or gold coins to criminals posing as government employees.

Another type of scam that emerged during the pandemic is so-called errand helper scams, in which a scammer offers to run errands but instead goes on a shopping spree with the credit or debit card provided.[5]

Elder homeowners may also face high-pressure sales tactics to enter into reverse mortgages to purchase an annuity or to use the proceeds for other imprudent or unnecessary purposes.[6] These are just a few of many sophisticated fraud scams developing every day and gaining the attention of federal, state and local government agencies and law enforcement.

Importantly, older people of all demographics are subject to these types of schemes. A recent series of investigative articles published in The Washington Post found that susceptibility to elder financial exploitation does not arise solely, or even primarily, from cognitive decline.

Rather, elder financial exploitation is so prominent because older people, as a group, have

the greatest amount of financial assets, usually from years of saving for retirement and accumulating equity in their homes.[7] Schemes are becoming so sophisticated that they can trick even highly educated and cognitively keen individuals.

Combine the wealth amassed by the older generations with a confluence of factors increasing the risk of exploitation, and you have the early stages of a crisis. Those factors include the following:

- The prevalence of assets held in online accounts and subject to faster withdrawal increases the risk of fraud. Scams often result in electronic overseas transfers where funds are whisked away, laundered and quickly emptied from foreign bank accounts before the fraud is even detected.

- Fraudsters are increasingly using AI to more quickly create plausible narratives to ingratiate themselves with older people and steal their funds.

- Michael Hsu, former acting comptroller of the currency, pointed out that voice replications, deepfakes and other sophisticated tricks are used to lure family members into transferring funds to impostors.[8]

- Families are more mobile than ever, and a close family member may no longer be down the street or across town, but might be in a different state, time zone or even country. This is leading to a more isolated older population and contributing to older customers being more vulnerable to fraud.

- Scammers are increasingly confident that they will not be reported to law enforcement until they have completed a scam and an individual's funds are irretrievable. Scammers know that in many cases the dollar amount of the fraud will fall below law enforcement's financial threshold to pursue an investigation, or, even if the stolen dollar amount is substantial, a general lack of investigative resources to address the volume of reports will often inhibit enforcement and successful prosecution.

We believe depository institutions are earnestly looking for ways to help their customers better protect themselves from becoming victims of financial exploitation. Their objective should be not only to help their account holders preserve their assets, but to also help reduce the risk of fraud-related consumer protection claims, which can lead to significant legal and regulatory costs and scrutiny.

There are important steps depository institutions can take to help combat the risk of elder financial exploitation and reduce the risk of loss to their customers and to themselves.

Key Strategies to Fight Exploitation: Trusted Contacts and Raising Customer Awareness

Two of the most important strategies highlighted in the statement, both of which are relatively inexpensive to implement, are (1) encouraging customers to identify trusted contacts, and (2) proactively and rapidly raising customer awareness of the types of scams then in circulation.

Trusted Contacts

Depository institutions can follow the example of brokerage firms and encourage every customer above a certain age to specify one or more family members or other contacts as trusted contacts on their accounts. Depository institutions should consider adding guardrails to their account terms to help customers protect themselves as they age.

The account terms would permit the depository institution to rely on the trusted contact if they are unable to reach the customer or otherwise believe the customer is potentially falling victim to a scam.[9]

Ideally, the trusted contact should be someone who does not have authority to make transactions in or directly benefit from the customer's account, although it could be a joint account owner or child who already has power of attorney for a parent.

As part of this policy, depository institutions could modify account terms to expressly permit, but not require, the depository institution to decline, delay, freeze or reverse a payment or funds transfer under certain circumstances.

These circumstances could include suspicion of fraud even when the account holder has authorized the transaction, unless a trusted contact confirms to the depository institution that the trusted contact has spoken directly with the account holder and reasonably believes the activity is not part of a fraud.

Depository institutions must be mindful to implement and administer such a policy fairly and consistently across any relevant accounts. Furthermore, it would be reasonable for the documentation implementing the arrangement to exculpate a trusted contact who acts in good faith.

Depository institutions should anticipate that some older customers may view the imposition of the trusted contact arrangement as an unreasonable infringement on the customer's financial autonomy, or that not every older customer will have a trusted contact.

In those instances, the depository institution can explain that the purpose of the trusted contact arrangement and complementary account terms is to help a customer establish safeguards to protect their assets before they are under the influence of scammers, and that the customer will retain the ultimate authority to close the account and withdraw their funds if that's their final decision.

Consumer Awareness

In terms of educating customers, depository institutions can build upon the Federal Trade Commission's Pass It On education campaign by employing multimedia techniques and modern social media distribution.

The campaign provided materials that respected older customers' life experiences, but also provided resources about fraud they could pass on to family and friends and other potential trusted contacts.[10]

Since elder fraud is so prevalent across the industry, trade associations could organize working groups to collaborate and share details of current scams aimed at older customers. This would come at a relatively low and distributed cost to depository institutions.

Recognizing that customers often become numb to additional written disclosures, trade associations and participating institutions should use all available multimedia and marketing tools to create informative, engaging content that people will remember and share. Content creators should maximize distribution by relying both on traditional and new media.

The depository industry could complement the warnings of specific ongoing or recent online scams by sponsoring high-profile public service announcements across all various media platforms, using well-regarded contemporaries of the intended audience.

Picture Harrison Ford, Oprah Winfrey, Jennifer Lopez, Nick Saban or Laura Bush raising awareness in a plainspoken, no-nonsense manner about reducing your risk of being victimized by online scams.

Conclusion

Depository institutions can take proactive and targeted steps to implement trusted contact account protections and raise consumer awareness of fraud.

These strategies are relatively inexpensive and have the potential to positively alter the trajectory of online elder financial exploitation. Merely adhering to consumer protection law and utilizing Bank Secrecy Act/anti-money laundering tools like suspicious activity reporting of elder fraud — while still important — is unlikely to change the status quo.

More and more customers are entering their older years while facing newer and more sophisticated scams that are harder to detect and evade.

The industry and regulators alike are keenly aware of these issues, but to meaningfully reduce the incidence of online elder financial exploitation, the industry will require continuous monitoring for new threats to older adults and a nimbleness and readiness to counter them.

Michael Krebs is a member and chairs the banking and financial services practice group at Nutter McClennen & Fish LLP.

Daniel Hartman is of counsel at the firm.

Nick Stabile is a partner at the firm.

Nutter partners Caitlin Glynn and Daniel Mulhern, and of counsel Matthew Hanaghan, contributed to this article.

[1] The Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration, and the Office of the Comptroller of the Currency.

[2] Interagency Statement on Elder Financial Exploitation (Dec 2024), available

at https://www.fincen.gov/sites/default/files/2024-12/Interagency-Statement-on-EFE-FINAL-508C.pdf.

[3] Id.

[4] Id., at FN 5.

[5] Consumer Financial Protection Bureau and Federal Deposit Insurance Corporation, COVID-19 Scams and Planning Tips (June 2021), available at https://files.consumerfinance.gov/f/documents/cfpb_covid-19-scams-and-planning-tips_2021-06.pdf.

[6] Office of the Inspector General, US Department of Housing and Urban Development, Reverse Mortgage Schemes – Fraud Bulletin (Apr. 9, 2013), available at https://www.hudoig.gov/fraud-prevention/reverse-mortgage-schemes-fraud-bulletin.

[7] Michelle Singletary, Enter the 'Ether,' Where Scammers Weaponize your Emotions, The Washington Post, December 2, 2024, available at https://www.washingtonpost.com/business/interactive/2024/scammer-method-weaponize-emotions-steal-victims/.

[8] Acting Comptroller of the Currency Michael J. Hsu, Remarks for the Financial Literacy and Education Commission's Public Meeting: Banks' Role in Addressing Fraud Against Consumers (July 10, 2024), available at https://occ.gov/news-issuances/speeches/2024/pub-speech-2024-75.pdf.

[9] Statement, at 4.

[10] See generally, https://consumer.ftc.gov/features/pass-it-on.