

Elder Financial Abuse: Beyond Banks

In today's digital world, advances in technology, mobile devices, and social media have made life more convenient but have also increased financial fraud risks. Financial institutions have long played a key role in protecting customers, but the complexity and scale of modern fraud require broader cooperation. A comprehensive solution must involve financial institutions, social media platforms, telecommunication providers, and government entities working together.

The digital financial landscape demands a collaborative approach, as scammers have become adept at circumventing even the most advanced security measures.

Highlights

- *As mandated reporters of suspected elder financial abuse, banks play a vital role in protecting seniors from financial abuse, but we can't do it alone.*
- *Telecom and social media companies also have a role to play in stopping senior scams since they facilitate the initial point of contact with victims.*
- *Lawmakers can do their part by increasing funding for APS, especially funding contingent on hiring more investigators dedicated to suspected financial abuse cases.*

Improving Telecommunications Security

Many scams originate through phone calls and text messages. Telecom collaborations with financial institutions and regulatory bodies can enhance real-time fraud detection and disrupt fraudulent schemes. To effectively curb financial crimes, telecom providers must also invest in advanced technologies and customer education to identify and prevent phishing, spoofing, and fraudulent messaging. Technologies like Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) improve caller authentication, reducing spoofed calls and verifying the legitimacy of incoming calls.

Addressing Social Media Fraud Risks

Fraudsters have taken to social media to scam senior adults. Unlike financial institutions that comply with Know Your Customer regulations, social platforms typically require minimal verification. Implementing identity verification, such as multi-factor authentication and linking accounts to verified IDs, can help prevent scammers from creating fake profiles.

Collaboration between social media platforms and financial institutions could significantly enhance fraud prevention. Platforms can notify financial institutions of potential scams targeting users, enabling quicker responses to suspicious activities. Implementing enhanced verification for in-app

STATE ISSUE BRIEF: Elder Financial Abuse: Beyond Banks

purchases and sharing information about known fraudulent accounts can further bolster security. Social media companies can lead public awareness campaigns to educate users on common scams and proactive safety measures.

Supporting Adult Protective Services (APS)

The Adult Protective Service (APS) office operated at the county level plays a critical role in protecting vulnerable individuals from financial abuse. However, APS needs more resources to combat this problem. Lawmakers should do their part by increasing funding for APS, especially funding contingent on hiring more investigators dedicated to suspected financial abuse cases. With more resources, APS can improve its capacity to prevent and respond to potential crimes targeting vulnerable populations.

Also, requiring APS to inform mandated reporters of known or suspected financial abuse, like credit unions and banks, about the outcomes of their investigations can help assess the effectiveness of preventative measures deployed by credit unions and banks and assist with adapting strategies based on feedback.

Collaboration among financial institutions, telecommunication providers, social media platforms, and government agencies is essential to fight financial fraud. By working together, stakeholders can create a safer financial ecosystem and protect customers from evolving threats.

####