Financial institutions can help prevent elder financial exploitation with alerts to trusted contacts

The Consumer Financial Protection Bureau (CFPB) provides voluntary recommendations in this advisory for financial institutions to help them prevent elder financial exploitation with alerts to trusted contacts.

Your institution may already permit, or may someday permit, account holders to designate a trusted contact person for your staff to contact with specific concerns. For example, an account holder may identify a family member or close friend to contact if staff suspects that the account holder may be at risk of financial exploitation. A trusted contact is an emergency financial contact who can step in to help protect the account holder.

This can be a helpful service for account holders and can also signal to consumers that your institution is taking steps to help protect their assets and prevent financial exploitation. This advisory examines how alerts to a trusted contact can be helpful for your institution and your account holders.

How might alerts to a trusted contact help during a suspicious situation?

Lara, a long-time account holder, listed her adult daughter as a trusted contact and provided written

consent for the financial institution to contact her daughter if there is a concern that Lara might be at risk of financial exploitation.

Today, Lara visits a branch to wire a large sum of money to a new friend overseas for an emergency situation, which is uncharacteristic behavior for Lara. The teller asks some questions about the situation and suspects that Lara may be experiencing a scam.

The teller alerts a supervisor, who speaks with Lara further and expresses concerns about the transaction. If a discussion with Lara does not relieve concerns about the threat, financial institution staff could reach out to Lara's daughter about their concerns and encourage her to intervene.

Once she knows about the situation, Lara's daughter might help Lara by:

- Asking questions to help Lara stop and think critically about the situation
- Helping Lara determine whether this is a legitimate transaction
- Explaining to Lara that this sounds like a scam and she should not wire the funds
- Helping Lara to:
  - Find out whether anyone else has accessed Lara's financial information
  - Stop that access
  - File a report with the police or other authorities
- Determining whether Lara needs extra support to manage her money and setting up a fiduciary if necessary
- Discussing how to prevent future problems and how to respond if something like this happens again

Because Lara provided advance consent for her financial institution to alert a trusted contact in case of suspected financial exploitation, Lara's financial institution can help her get more support and potentially prevent her from sending the money.

Note on fiduciaries and representatives:
The Gramm-Leach-Bliley Act (GLBA) permits financial institutions to share information with "persons acting in a fiduciary or representative capacity on behalf of the consumer" without providing the account holder with notice and an opportunity to opt out. For example, if Lara had a court-appointed guardian, under GLBA a financial institution would not need to get Lara's advance consent to share information with that person. See 12 CFR § 1016.15(a)(2)(v).

In 2016, the CFPB released voluntary recommendations for financial institutions that included enabling account holders to consent to sharing information with trusted third parties. **consumerfinance.gov/data-research/research-reports/recommendations-and-report-financial-institutions-preventing-and-responding-elder-financial-exploitation/**

The following voluntary practices may be helpful when considering whether and how to provide alerts to trusted contacts:

Develop clear policies and procedures

- Create a policy that explains when and how your staff can reach out to a trusted contact.
- Establish a procedure for requesting advance consent from account holders to share certain information with a trusted contact when certain situations occur. Offer this option to account holders of all ages.
  - Identify the situations in which your staff may alert the trusted contact. For example, you could alert the trusted contact if you are unable to contact the account holder, if a discussion with the account holder does not relieve staff concerns about the threat of financial exploitation, to confirm the account holder's health status, or to confirm the identity of a new guardian, trustee, executor, or power of attorney holder.
  - You can ask account holders to identify multiple trusted contacts, in case the primary trusted contact is unavailable or is suspected of exploiting the account holder.
- Consider asking account holders to designate a trusted contact at account opening and revisiting

the consent on a regular basis and when certain changes or events occur. For example, you could review the consent if the account holder adds an additional owner to the account, establishes a new power of attorney or trust, or experiences financial exploitation. Or, if an account holder expresses concerns about financial exploitation, you could suggest that they appoint a trusted contact to help protect themselves.

- Account holders may have concerns about privacy, family dynamics, or maintaining financial independence. Develop model language for talking about these issues so consumers can feel more comfortable with choosing a trusted contact. For example, it may be helpful to explain to the account holder that this feature adds an extra layer of security to the account, and clarify that the trusted contact cannot view the account or make any transactions or decisions about the account unless they have some other legal authority, such as guardianship or power of attorney.
- Encourage account holders to talk to their trusted contact to explain that your staff may reach out to them in certain situations.
- Develop model language for the information that staff may disclose in a phone call, in-person conversation, email, or other type of alert to the trusted contact.
- Consider which type of staff person is best qualified to discuss a suspicious situation with the account holder or trusted contact. For example, this could be a staff member who is trained on financial exploitation and communicating with older adults about sensitive issues. It may be helpful to limit access to the trusted contact's information to

The federal Senior Safe Act provides that financial institutions are not liable for reporting suspected elder financial exploitation to covered agencies if the situation meets certain criteria. To establish immunity, the report must be made in good faith and with reasonable care and the employee must have received appropriate training on how to identify and report elder exploitation. The Senior Safe Act also provides individual immunity for certain individuals. The Senior Safe Act applies to depository institutions, credit unions, investment advisers, broker-dealers, insurance companies, insurance agencies, insurance advisers and transfer agents. Senior Safe Act, 12 U.S.C. § 3423(a) (2018).

Banks and credit unions that are interested in implementing trusted contacts may find information on this topic from SEC or FINRA helpful, although the material is targeted for the broker-dealer industry.

FINRA's Rule 4512 (finra.org/rules-guidance/rulebooks/finra-rules/4512) states that firms can alert a trusted contact person and "disclose information about the customer's account to address possible financial exploitation, to confirm the specifics of the customer's current contact information, health status, or the identity of any legal guardian, executor, trustee or holder of a power of attorney, or as otherwise permitted by Rule 2165." For more information about how trusted contacts work in the broker-dealer industry, see finra.org/rules-guidance/guidance/faqs/frequently-asked-questions-regarding-finra-rules-relating-financial-exploitation-seniors.

certain designated staff members, in order to reduce the risk of an inadvertent disclosure of confidential account information.

- Develop a process for what staff should do if the trusted contact is the suspected bad actor. For example, staff could ask the account holder to designate a second trusted contact, and staff could contact Adult Protective Services and/or local law enforcement for assistance.
  - You can note on your trusted contact form that staff members will use their discretion to determine whether to alert the trusted contact in any given situation.

Educate and support your account holders

- Develop concise, plain-language written materials in large, readable fonts about your policies and procedures. This could include a written disclosure you provide to the account holder when they appoint a trusted contact. You could describe the purpose for the consent form, situations when you might reach out to a trusted contact, the type of information staff may disclose to a trusted contact, issues for the consumer to consider when deciding whether to execute the form, and how to choose a suitable trusted contact.
  - A study found that consumers were more likely to appoint a trusted contact when the trusted contact form included three things: a statement about the prevalence of fraud, a statement that most people support the concept of a trusted contact person, and a requirement for the account holder to make an active choice about whether to appoint a trusted contact. osc.gov.on.ca/documents/en/Securities-Category1/rule_20201109_11-790_protecting-aging-investors-through-behavioural-insights.pdf
  - Before implementing a consent form, consider gathering feedback about the draft from older adults and professionals who work with older adults.
- Consider allowing account holders to select specific situations where your staff can reach out to the trusted contact. For example, on the consent form, you could provide a checklist with options they can choose.
- Inform account holders that they have the right to revoke the consent at any time or to execute a new consent and name a different trusted contact.
- Inform account holders that although choosing a trusted contact does not give that person the right to view their account or make any decisions about the account, it is possible that the person could use other methods to try to take advantage of them. Inform them that you will not share information with the trusted contact if your staff reasonably suspects that the trusted

You can download or order CFPB's resources in bulk for free and share them with your account holders. Here are a few examples:

- Managing Someone Else's Money guides for financial caregivers: **consumerfinance.gov/msem**
- Money Smart for Older Adults scam prevention program: **consumerfinance.gov/moneysmart**
- Planning for diminished capacity and illness: **consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/financial-security-as-you-age/planning-for-diminished-capacity-and-illness/**

contact has exploited or will exploit the account holder.

Train and support your staff

- Develop a training culture at your financial institution that incorporates frequent education on elder financial exploitation.
  - Cyclical, recurring training will help integrate awareness of this important topic into daily routines and ensure staff know how to respond when they suspect financial abuse. It may be helpful to walk staff through some common scenarios and discuss how your financial institution could reach out to a trusted contact for help.

    A variety of national, state, and local entities, such as government agencies, nonprofit organizations, and trade groups, offer free trainings to help financial professionals prevent elder financial exploitation.

  - Staff should know how to recognize transactional and behavioral red flags and how to report elder financial exploitation to Adult Protective Services (APS) and/or law enforcement, in accordance with state and federal laws.
  - You can build on your institutional knowledge and celebrate your team by incorporating real stories of incidents in which staff intervened successfully to help an older account holder prevent financial exploitation.
- Develop talking points for your staff to use when asking account holders to choose a trusted contact. It may also be helpful to develop talking points for walking an account holder through the consent form.
- Develop talking points for your staff to use when communicating with an account holder or trusted contact about suspected financial abuse. You may need different talking points for front line staff and supervisors. Make sure staff understand that the trusted contact may decline to get involved in the situation.

The CFPB, Treasury, and FinCEN issued a joint memorandum in 2017 to encourage coordination among financial institutions, law enforcement, and Adult Protective Services (APS) to protect older adults from financial abuse: **consumerfinance.gov/compliance/supervisory-guidance/memorandum-financial-institution-and-law-enforcement-efforts-combat-elder-financial-exploitation/**

In 2019, the CFPB released updated information for financial institutions about reporting elder financial exploitation: **consumerfinance.gov/data-research/research-reports/reporting-suspected-elder-financial-exploitation-financial-institutions-update-2016-advisory-and-recommendations/**

Review state and federal laws

- Review the Gramm-Leach-Bliley Act's notice and opt out requirements.
- State privacy laws and other state and federal laws may impact the account holder's ability to designate a trusted contact, the content of the consent form, or other issues related to the consent. This advisory does not supersede those requirements.

The CFPB, along with several other federal agencies, issued guidance in 2013 to financial institutions to clarify the applicability of privacy provisions of the Gramm-Leach-Bliley Act (GLBA) to reporting suspected financial exploitation of older adults: **consumerfinance.gov/compliance/supervisory-guidance/interagency-guidance-reporting-financial-abuse-older-adults/**

About us

The Consumer Financial Protection Bureau (CFPB) is a 21st century agency that helps consumer finance markets work by making rules more effective, by consistently and fairly enforcing those rules, and by empowering consumers to take more control over their economic lives.

Learn more at consumerfinance.gov

Connect with us

Submit a complaint
consumerfinance.gov/complaint

Tell your story
consumerfinance.gov/your-story

Ask CFPB
consumerfinance.gov/askcfpb

Share your thoughts
facebook.com/cfpb
twitter.com/cfpb

This document includes links and references to third-party resources or content that consumers may find helpful. The Bureau does not control or guarantee the accuracy of this third-party information. By listing these links and references, the Bureau is not endorsing and has not vetted these third parties, the views they express, or the products or services they offer. Other entities and resources also may meet your needs.