Preventing Fraud in Joint Account Holder Scenarios

Preventing Fraud from Joint Account Misuse in Lieu of Power of Attorney

Financial institutions increasingly encounter situations where an individual foregoes a formal Power of Attorney (POA) and instead seeks to be added as a joint owner on a vulnerable person's bank account. This tactic can be used to gain unfettered access to funds under the guise of "helping" the primary account holder, often an elderly or incapacitated person. Without proper safeguards, such arrangements may facilitate **financial exploitation**, allowing the new joint owner to legally withdraw or transfer assets for their own benefit.

The stakes are high: older adults who fall victim to this kind of fraud can lose their life savings and financial security. **A recent analysis of bank reports found about $27 billion in suspected elder exploitation in just one year.** Banks and credit unions are uniquely positioned to detect and prevent these abuses; however, they must navigate complex legal, operational, and ethical considerations.

The following report outlines **best practices, key policies, and procedures** that financial institutions can implement to mitigate the risks when individuals attempt to avoid POAs by using joint accounts. Each section provides guidance backed by industry recommendations and regulatory expectations, helping banks protect vulnerable customers while upholding their rights and complying with the law.

Dangers of adding someone as a joint owner of a bank account instead of using a Power of Attorney ⋆ Carol L. Grant, P.A.

7 Things You Need To Know About Adding Someone To Your Bank Accounts

Press Release for Interagency Statement on Elder Fraud FINAL 508C

How Banks and Brokers Can Help Stop Elder Fraud

Financial Protection for Aging Adults & Caregivers

Best Practices for Fraud Prevention

Financial institutions should adopt a proactive, multilayered approach to prevent fraud in scenarios where joint accounts might be misused as a substitute for a POA. **Employee training, customer education, and tailored account features** are cornerstone best practices.

The Consumer Financial Protection Bureau (CFPB) and other regulators have identified several voluntary best practices that have proven effective in combating elder financial exploitation. Key best practices include:

- **Develop a Robust Oversight Program:** Establish strong governance with clear protocols for protecting vulnerable account holders. This means dedicating resources and management attention to elder fraud prevention, and appointing a designated officer or team responsible for oversight.
- Internal protocols should outline how staff should respond if a customer attempts to add a joint owner in lieu of a POA. Effective governance ensures consistent application of safeguards across all branches.
- **Employee Training on Red Flags:** Regularly train frontline staff, managers, and back-office personnel to recognize the warning signs of potential exploitation and to intervene appropriately. Staff should understand that **a new person suddenly asking to be added to an older customer's account** is a common red flag. Behavioral cues examples:

  A caregiver dominating a conversation or an elder customer appearing anxious or confused – **"a caregiver or other individual who shows excessive interest in the older customer's finances, does not allow the customer to speak, or is reluctant to leave their side"** is a classic red flag of undue influence. Training should equip employees with clear action steps for such scenarios, including how to discreetly validate the older person's intent and how to escalate concerns through proper channels. Consider a private conversation (one-on-one) conversation with the account holder and alternative legal forms to use, such as a POA, to allow for assistance with a qualified family member or trust person.

- **Consumer Education and Transparency:** Banks should educate customers – especially seniors and their families – about the **risks of adding a joint account holder instead of using a POA**. Many seniors mistakenly believe joint accounts are a harmless convenience, not realizing they confer equal ownership rights to the other party.
- Financial institutions can provide brochures, seminars, or one-on-one counseling that **highlight the potential pitfalls**: once someone is a joint owner, they can legally withdraw all funds for themselves, override the senior's Will by taking account assets at death, and even expose the account to their personal creditors or lawsuits. Banks are encouraged to explicitly **highlight these risks of joint account access** and to promote safer alternatives.
- For instance, educating customers that a **durable POA allows help with finances without surrendering ownership** can steer them toward a more secure arrangement. In

line with regulatory guidance, offering information on planning for incapacity, **honoring valid POA documents**, and providing protective account features are all part of an age-friendly service model.

- **Offer Safe Account Alternatives:** To reduce the temptation to **use joint accounts improperly**, financial institutions can offer alternative tools for those who need assistance managing accounts. One best practice is to enable **"convenience signer" or authorized user arrangements**, where a trusted person can help with transactions *without* becoming a co-owner. For example, some banks allow adding an **authorized signer or caregiver access** that permits bill payment and monitoring but confers no ownership rights.
- **Huntington Bank's "Caregiver Banking" program is a case in point – it provides account access sharing for a caregiver to view balances, pay bills, and detect fraud. Yet, the caregiver is not a joint owner and bears no legal claim to the funds.**
- **https://www.huntington.com/learn/checking-basics/differences-between-authorized-user-joint-account-power-of-attorney**

- **Similarly, banks can encourage the use of features like automatic bill pay, direct deposit, or bill management services, which minimize the need for another individual to directly access an account. By offering these alternatives, banks give customers safe options to get help with finances without resorting to joint ownership.**
- **Trusted Contact Person Programs:** Implement a **"trusted contact"** designation process for accounts, as encouraged by regulators8. This allows the customer to name a third party (such as a family member or advisor) whom the bank can contact if exploitation is suspected or if the bank is unable to reach the customer. Notably, **Bank of America now lets clients designate a trusted contact** – someone the bank can reach out to to confirm unusual account activity or concerns, without giving that person control over the account.
- Having a trusted contact on file gives the bank an early intervention point: if an elderly customer comes in with a stranger or a distant relative to add them on an account, the bank (with the customer's prior consent) might quietly consult the trusted contact to verify the situation. This practice can deter fraud by bringing another informed party into the loop and is specifically recommended in industry guidance.
- **Data Analytics and Monitoring:** Leverage technology to detect anomalous transactions or account changes that could indicate fraud5. Modern core banking systems can be tuned to flag events like a new joint account holder being added on a senior's account followed by large withdrawals or wire transfers. The AARP's BankSafe initiative and experts have noted that **machine learning and AI can help identify erratic financial activity** that departs from an elder customer's usual patterns. Banks should expand their anti-money laundering (AML) and fraud monitoring rules to incorporate scenarios specific to elder exploitation. For example, set triggers for a surge in account spending after a new signer is added, or repeated ATM withdrawals to the account's daily limit by a non-senior on a senior's account. Early warning systems like these allow banks to **"slow down the**

process" when something looks suspicious, buying time to investigate before irreversible losses occur.

- **Engage in Community Coordination:** As a broader best practice, banks can connect with local elder abuse prevention networks, industry consortiums, and law enforcement partnerships. Sharing information and trends helps develop better protective strategies. Many financial institutions participate in the ABA Foundation's *Safe Banking for Seniors* programs to educate communities and staff. Collaboration with Adult Protective Services (APS) and senior advocacy organizations can enhance a bank's ability to respond effectively when a suspicious joint account addition or transaction is spotted. These outreach efforts not only aid in prevention but also demonstrate the bank's commitment to ethical responsibility in protecting elders.

By adopting these best practices, a financial institution creates a strong front line of defense. Educating customers about the **legal differences between joint accounts and POAs** (and the risks involved) is especially crucial. A power of attorney designates an agent with a fiduciary duty to act in the principal's best interest, whereas a joint account gives the added party an immediate ownership stake with no duty to the original owner. Making sure customers understand this distinction can dissuade them from ill-advised account changes. In fact, **most estate experts advise using a POA rather than adding a joint owner** for exactly these reasons. Ultimately, the bank's goal is to uphold the customer's intent and security – best practices like these help do so by **preventing fraud before it happens** through vigilance, alternatives, and education.

Key Policies for Financial Institutions

In addition to broad best practices, banks should formalize specific policies that institutionalize fraud prevention measures. Clear policies ensure that all employees follow consistent protocols and that the bank complies with legal requirements when handling potential exploitation cases. Below are critical policy elements and guidelines relevant to situations where individuals seek joint account access instead of using a POA:

- **Identity Verification and Documentation Policy: Require rigorous identity verification and authentication for any addition of a joint account holder.** A bank's policy should mandate that **all new joint owners must sign account documents in person at the bank, or provide notarized signatures if an in-person visit isn't possible**. Allowing someone to be added without proper signature verification opens the door to fraud (for example, forged signature cards have been used to siphon funds). A defensible policy, as one banking expert notes, is to insist that *"all those signing signature cards must be present and identified"* – this simple rule could have prevented major losses in fraud cases. Even though Customer Identification Program (CIP) regulations set minimum ID standards, banks should go beyond that for account changes by verifying joint owners with the same rigor as new account openings. This policy protects against unauthorized additions and ensures the bank documents each party's consent to the account arrangement.
- **Elder Financial Exploitation Policy:** Develop a comprehensive policy addressing how the institution prevents and responds to elder financial exploitation. This policy should

incorporate state and federal requirements (e.g. any **mandatory reporting laws** in the bank's operating states) and reflect guidelines from regulators. As part of this, the policy should explicitly cover scenarios of non-POA joint account requests. It might require additional due diligence when an elderly or disabled customer wants to add a non-spouse joint owner, such as manager approval or a cooling-off period to further assess the situation. Importantly, the policy must empower employees to **report suspected exploitation without fear of violating privacy rules**, in line with the federal Senior Safe Act which offers legal immunity for reporting in good faith. Banks should clarify that suspected financial abuse of any customer – even if the transaction is technically authorized – should be treated as suspicious and escalated internally and to authorities as appropriate. The CFPB's guidance urges institutions to **"report all cases of suspected exploitation to relevant federal, state and local authorities, regardless of whether reporting is mandatory."**. Therefore, a strong policy will mandate timely **Suspicious Activity Report (SAR) filings** to FinCEN for suspected elder fraud and direct staff to alert APS or law enforcement per state law10. (**Notably, over 94% of banks already report suspected elder exploitation to APS, according to an ABA survey.)** Defining these reporting steps in policy ensures consistent compliance and quick action when red flags arise.

- **POA Acceptance and Account Authority Policy:** One factor that sometimes leads customers to avoid POAs is difficulty in getting financial institutions to honor those documents. Banks should have a clear, senior-friendly policy for reviewing and accepting valid powers of attorney. This includes training back-office staff to promptly validate POA documents and add the agent to the account in an "agent" capacity (not as owner) with whatever account access is legally granted. The policy should commit to **honoring legally executed POAs** in accordance with state laws, rather than pushing customers toward joint accounts. By making POA acceptance straightforward, banks remove a common excuse for adding a family member as a joint owner. The policy can also provide guidelines for limiting an agent's access if the POA is limited in scope, and for recording the POA in the bank's system so that tellers know an agent is authorized to act. Essentially, ease-of-POA policies encourage the **preferred fiduciary route** and demonstrate the bank's support for responsible financial management.
- **Account Titling and Features Policy:** Financial institutions may consider specialized account titling options as a matter of policy to accommodate customers who need help but want to avoid joint ownership. For example, some states allow "convenience accounts" or "agency accounts" where the second person is listed as an agent for transaction purposes but not as an owner. If permissible, banks should include in their policies whether they offer such accounts and under what conditions. Similarly, policies can promote the use of **beneficiary designations (POD or TOD)** instead of joint survivorship for estate purposes, paired with a POA for day-to-day needs. The bank's product policy could outline that staff should suggest **naming a child as a Payable-on-Death beneficiary and using a POA** rather than adding the child as joint owner, when the goal is estate planning combined with bill-paying help. By having these options clearly defined, employees have concrete solutions to offer that are safer than joint accounts.
- **Transaction Hold and Review Policy:** Where legally allowed, banks should adopt a policy enabling them to **delay or refuse transactions that appear linked to**

exploitation, pending further review. Many U.S. states have enacted "elder financial protection" or **temporary hold laws** that give banks safe harbor to pause disbursements when exploitation is suspected. A policy should spell out the circumstances under which a hold can be placed (e.g. a large withdrawal immediately after adding a new joint owner, or any withdrawal that the customer seems coerced into). It should also detail the required internal approvals and notifications (for instance, notifying the account owner and their trusted contact, as FINRA Rule 2165 requires in the brokerage context). If the bank operates in states without statutory hold authority, the policy might still allow internal holds on certain high-risk transactions, recognizing that the bank must balance risk of customer dissatisfaction or liability. The **American Bankers Association reports** that 50% of banks in states with elder financial hold laws actively use them to protect customers. Banks overwhelmingly support having this ability, and a well-crafted policy ensures it's used consistently and lawfully. The policy should also address how to handle a customer's challenge to a hold and how long holds can last, aligning with any applicable law (many states permit an initial hold of, say, 10–15 business days). By formalizing these procedures, a bank can act decisively when a fraudulent joint-owner scenario crosses into attempted theft.

- **Customer Communication and Consent Policy:** It is wise to implement policies around customer notifications and consent forms for account changes. For example, when an account owner requests to add someone as joint, the bank could have a **mandatory disclosure form** or script that the customer must review, explaining in plain language: *"By making John Doe a joint owner, John will have equal rights to withdraw or use all funds in the account, and ownership of the funds will transfer to him if you die."* This policy-driven practice ensures the customer is confronted with the legal reality (which exploiters might downplay). Some institutions go further and require the customer to sign an acknowledgment of these points. Such documentation not only educates the customer but also serves as evidence that the bank fulfilled its duty to warn. The policy can also state that whenever possible, bank staff should speak **privately with the original customer** (without the would-be joint party present) to confirm the addition is truly what they want and not being done under duress. If the other individual refuses to let the customer speak alone or seems to be coaching answers, employees should treat that as a serious red flag under the bank's exploitation policy. These communication protocols, set by policy, help safeguard the customer's agency and ensure transparency.
- **Compliance with State and Federal Law:** Finally, every policy must be reviewed in light of relevant laws and regulations. Banks must be cognizant of the **varying legal landscape** around elder financial abuse. For instance, some states (like California and Virginia) *mandate* that financial institution employees report suspected elder abuse and provide immunity for doing so. Failure to report in those jurisdictions could expose the bank to penalties. Other states might not mandate reporting but strongly encourage it. The policy should reference the specific obligations in each state of operation and instruct employees accordingly (often via an appendix or state-by-state manual). Additionally, policies should reference federal provisions like the Gramm-Leach-Bliley Act (for privacy) and explicitly note the **Senior Safe Act's protections** for disclosing customer information to authorities in abuse cases. Including legal counsel in policy drafting is important to strike the right balance between proactive intervention and compliance with contract law (e.g., recognizing that a bank generally isn't liable for allowing an

authorized transaction, but could be drawn into litigation if it **"should have known"** of exploitation and did nothing). In sum, aligning policies with legal requirements and safe harbors ensures the bank's fraud prevention efforts are both effective and compliant.

By instituting these policies, banks create an environment where stopping a fraudulent joint account scheme is not just an ad hoc reaction, but a built-in aspect of their operations. Policy measures like mandatory identity verification, formal elder abuse protocols, and transaction hold rights give employees the tools they need to intervene. They also send a clear message that the institution prioritizes ethical standards – protecting vulnerable customers even when doing so might inconvenience a transaction. In practice, strong policies empower staff to act confidently and consistently, closing gaps that fraudsters might otherwise exploit.

Procedures for Handling Joint Account Requests and Suspected Fraud

Having the right policies in place is essential, but **effective procedures** are what bring those policies to life in day-to-day banking operations. Frontline employees need concrete steps to follow from the moment a customer inquires about adding a joint account holder through to ongoing monitoring of the account. Below is a breakdown of recommended procedures that banks should implement to prevent and respond to fraud in scenarios involving joint account access without a POA:

1. **Initial Customer Inquiry – Needs Assessment:** When a customer (often an older adult or their companion) asks to add someone as a joint account holder, the first step is for the employee to gently **probe the customer's needs and rationale**. A well-trained representative will ask questions in a respectful manner to determine if the customer simply needs help managing the account (paying bills, monitoring balances, etc.) or if they intend to gift ownership to the other person. This is a critical juncture to inform the client of alternatives. For example, if the customer says, "My daughter is just going to help me with my finances," the employee should explain that a joint account will make the daughter a co-owner and perhaps suggest, *"We have other options like a power of attorney or convenience signer that might suit your situation without giving up ownership."* This conversation follows the bank's educational best practices and should be documented in the interaction notes. If the customer still wishes to proceed with adding the joint owner, the employee moves to the next steps but remains alert for any signs of confusion or coercion.
2. **Verification of Authority and Capacity:** Before processing the addition, the bank should **assess the account owner's capacity and willingness** in line with training guidelines. If the account owner is present, staff should, whenever possible, speak to them separately to confirm they understand the implications. Any indication that the individual **does not comprehend the decision or is under pressure** (e.g., they cannot answer basic questions about why they want the change, or they defer entirely to the other person) should trigger an immediate pause and escalation per the bank's elder exploitation protocol. Bank procedures should empower employees to delay the transaction if they suspect the customer is not acting freely. In parallel, the bank officer

should **verify whether a valid POA or guardian exists** for the customer. It's not uncommon that a client might already have a designated agent or court-appointed guardian that the branch is unaware of. A quick internal system check and direct query to the customer ("Have you granted power of attorney to anyone to handle your finances?") can surface that information. If a POA is on file, that agent should be involved or at least notified rather than sidestepping the official arrangement. If the customer is **legally incapacitated** (e.g., suffering advanced dementia) and the person with them has no legal authority, the bank should **not proceed with adding a joint owner** – doing so could be facilitating exploitation or could be void if challenged later. In such cases, the procedure is to escalate to a supervisor and likely refer the companion to pursue proper legal guardianship or POA through the courts, rather than the bank making an unauthorized change.

3. **Identity Verification and Documentation for New Owner:** Assuming the request appears legitimate and the customer has capacity, the next step is to perform full Customer Identification Program checks on the prospective joint owner. The bank's procedure must require obtaining government-issued photo ID, Tax ID/Social Security number, date of birth, address, and other CIP-required details from the new owner, just as if they were opening a new account on their own. Both the original customer and the new joint applicant should complete and sign the bank's **account ownership update forms**. As per policy, the **signature of the new joint owner must be verified in person or via notarized form if remote**. The employee should compare signatures with IDs and ensure all paperwork (like a new signature card or account agreement) is properly executed. In practice, many banks now incorporate these steps digitally – for example, by sending a secure link to the second party to provide their information and e-sign after the primary initiates the addition online. Even so, the same verification standards apply. This procedure protects against fraudsters who might otherwise try to add themselves or an accomplice without ever showing their face. It also creates a clear paper trail of the new owner's acknowledgment of account terms.
4. **Customer Acknowledgment of Risks:** As part of the account change process, it is prudent for the bank to require the primary account holder to acknowledge the consequences of adding a joint owner. The procedure can involve reviewing a short checklist or disclosure with the customer, such as: *"By adding this person, (a) they will have equal access and can withdraw money without your permission, (b) your funds could become subject to their debts or legal judgments, and (c) you may not be able to remove them later without their consent."* This aligns with the common issues often unbeknownst to customers. The representative can have the customer sign a form or electronically confirm that they understand these points. Not only does this step educate the client at the very last moment, giving them one more chance to reconsider, it also serves as a safeguard for the bank. It shows the bank took reasonable steps to inform the customer, which could be important if a dispute arises later. In some documented cases, seniors have added a joint owner and later said they didn't realize the person could take all the money; a signed acknowledgment helps prevent that situation or provides clarity that the bank was transparent. If a customer expresses hesitation or surprise during this review, the procedure should allow them to halt or delay the addition without penalty.
5. **Manager or Second-Pair Review (if required):** Many institutions implement a dual-control checkpoint for adding non-spouse joint owners on substantial accounts or for at-

risk clients. Under this procedure, the employee handling the request would notify a supervisor or a centralized risk unit before finalizing the change. The manager might review the documentation and any notes about the interaction (e.g., "Customer seemed unsure, daughter answered for her often"). They could even speak with the customer by phone or in person for a secondary confirmation. The idea is to ensure that one level of frontline staff doesn't miss a red flag – an experienced supervisor might catch subtleties or have additional context (like prior alerts on the account). Such a review is especially warranted if the account has significant balances or if the customer is above a certain age (say, 80+), as the **potential harm is greater**. This step might also include checking the bank's internal fraud databases to see if the new joint person has been involved in any prior suspicious incidents at the bank (for instance, attempting similar with another older customer). Only after this sign-off would the joint addition be approved in the system.

6. **Execution of Account Changes:** Once all verifications and approvals are satisfied, the bank updates the account to add the joint owner. The procedure should automatically trigger certain safeguards: for example, the system might prompt the offer of setting a **notification alert** on the account for large transactions. (CFPB suggests offering such "opt-in account features" for seniors, like alerts or withdrawal limits.) The banker can ask the customer if they would like an email or text alert whenever a withdrawal over a chosen amount occurs, or if they want dual-signature requirements on checks over a threshold (if the bank supports that). Although these are optional, they are additional tools to catch any misuse early. The bank should also confirm whether the customer wants to update any **beneficiary designations** in light of the new setup – sometimes adding a joint owner unintentionally supersedes estate plans, and the bank giving a gentle reminder is a helpful service (as well as a subtle prompt to reconsider if that was not what they intended). Finally, the completion of the change should be clearly logged, and the customer should receive a written confirmation (which might again reiterate the new rights of the joint holder).
7. **Post-Addition Monitoring:** After a joint owner is added, the bank's fraud monitoring systems should **elevate the account's risk profile** for a period of time. Enhanced monitoring procedures might include flagging first-time transactions by the new joint party. If suddenly large sums move out shortly after the account change, that should prompt an immediate review or a courtesy call to the original account holder. For example, if within a month of adding the joint owner, a $50,000 wire is initiated, the procedure could require holding the wire (if possible under law) and contacting the senior customer to confirm they indeed wanted this. This ties into the **"transaction hold" capability** mentioned earlier. Under many state laws, banks can delay suspicious disbursements from an account of an older adult for a short period while an investigation occurs. Internally, banks should use that time to involve their fraud investigators or security department. They may call the customer or the customer's trusted contact to inquire about the transaction. If the new joint owner is attempting to clean out the account against the elder's wishes, this is the last chance to stop it. The bank's procedures should specify who (which department or officer) has the authority to initiate a hold and what documentation is needed. The institution should also be prepared to expedite reports to APS and potentially law enforcement at this stage, since quick action could prevent irreversible losses.

8. **Reporting and Escalation:** Should an employee at any point suspect that the addition of a joint owner or subsequent account activity is fraudulent, they must **escalate the issue immediately** according to the bank's chain of command. Typically, the procedure is to notify the bank's fraud risk unit or elder abuse task force (if one exists) and to file an internal incident report. This internal report often leads to the filing of a SAR with detailed information about the suspected exploiter and the transactions attempted. The bank's legal or compliance team might also reach out directly to APS if state law requires *or* if the bank believes intervention is needed to protect the client (even where not mandated, voluntary reporting is encouraged). Frontline staff should not worry about customer privacy violations when reporting bona fide suspicions – the bank's procedures, bolstered by the Senior Safe Act, protect employees for making good faith reports of elder fraud. All such incidents should be tracked in a case management system. The bank can convene a quick-response team to determine if the joint account should be frozen entirely (which might require legal review given joint owners have rights to the funds). In some situations, the bank's intervention might involve **removing account access** (e.g., disabling online banking or ATM cards) until the matter is resolved. Each step of these actions should be carefully documented, and communications should be maintained with the customer (unless the bank believes the customer is under the control of the abuser, in which case involving APS or law enforcement to visit the customer may be more appropriate).
9. **Follow-Up and Remediation:** If an attempted fraud via joint account was caught in time, the bank's procedure should include follow-up with the affected customer. This might mean working with them to change account numbers, issue them a new debit card, or even close the account and open a fresh one without the fraudulent party. The bank can suggest implementing a true POA at this point if the customer still needs help managing funds – possibly even referring them to legal aid or elder law attorneys for assistance in drafting one. In cases where funds were already taken by a now-joint owner, the bank should advise the customer on their legal options (while the bank itself may not be liable if the transaction was technically authorized, it can still show empathy and provide guidance). The institution might also consider **reparative measures** like reimbursing fees or providing a temporary credit if it appears the bank's oversight contributed to the loss. Additionally, all incidents should be analyzed for lessons learned. The procedures should call for a post-mortem review by the risk management team to determine if any gaps in training or process allowed the situation to progress and update training materials accordingly.

Throughout these steps, **ethical consideration and customer care** are paramount. Bank personnel must strike a balance between protecting the customer and respecting their autonomy. It is a delicate procedure to question someone's financial decisions; hence, the approach is always to express concern for the customer's best interest. Employees are trained to use tactful language, such as, *"Mrs. Smith, our first priority is keeping your money safe. We just want to ensure you understand this change and that it's truly what you want. Would you mind if I asked you a few questions privately? It's something we do for all our senior clients' security."* Such scripts are built into procedures to help staff manage the conversation ethically.

Financial institutions often find themselves in a **"damned if we do, damned if we don't"** predicament. If they intervene by delaying a transaction or refusing an account change, customers might react negatively; yet if they don't intervene and the customer is defrauded, they face blame for not protecting them. Well-crafted procedures, executed with professionalism, aim to minimize frustration by explaining that any extra steps are there to protect the client. Many clients ultimately appreciate these precautions when they understand the reasoning.

In conclusion, detailed procedures from the moment of a joint account request through monitoring and potential intervention form a safety net. By following these procedures, banks can catch and halt many fraud attempts that exploit joint account privileges. Consistency is key: every employee, in every branch, should handle these sensitive situations with the same thoroughness. When procedures are followed diligently, the institution significantly reduces the risk that a bad actor can simply walk an unwary customer into a branch and walk out with access to their money. Instead, fraudsters will encounter a system of checks and safeguards at every turn.

Summary of Recommendations and Benefits

The table below summarizes the key fraud-prevention measures a bank can implement regarding joint accounts and outlines the benefits of each. These recommendations work in concert to protect both the bank and its customers from the risks of avoiding a Power of Attorney by adding joint account holders.

Recommendation	Benefit to Bank & Customer
Rigorous verification for new joint owners	Prevents unauthorized or forged additions to accounts, blocking fraudulent actors at the outset. Ensures only legitimate parties obtain access, reducing liability from wrongful account use.
Employee training on elder fraud red flags	Equips staff to spot and stop suspicious situations (e.g. an overly controlling companion) early. Early detection allows intervention before funds are lost, and consistent responses protect the bank's reputation.
Customer education on POA vs. joint accounts	Informs clients of the legal and financial risks of joint ownership (loss of funds, creditor exposure). Empowers customers to choose safer alternatives, thereby preventing inadvertent self-harm and reducing future disputes.
Offer alternative account access options	Provides convenience (bill payment, monitoring) without granting ownership rights. Protects customers' funds by retaining fiduciary oversight (through POA or view-only access), and deters exploiters who prefer full control.
Trusted contact designation program	Allows bank to confirm suspicious activity with a third party the customer trusts. Facilitates timely intervention if exploitation is suspected, all while respecting privacy rules (pre-consented contact).
Elder abuse reporting & hold policies	Enables the institution to pause questionable withdrawals or new arrangements until verified. Utilizing legal safe harbors to delay

Recommendation	Benefit to Bank & Customer
	transactions prevents irrevocable losses, and robust reporting fulfills legal duties while getting authorities involved quickly.
Ease-of-use for Power of Attorney documents	Encourages customers to use proper legal instruments by assuring their POA will be honored without hassle. Maintains control in the hands of a fiduciary who is obligated to act in the customer's best interest, thereby upholding ethical standards and reducing joint account misuse.
Enhanced monitoring of high-risk accounts	Flags unusual account changes or transactions (e.g. large transfers by a new joint owner) for review. Early alerts give the bank a chance to verify customer intent, stopping potential fraud in progress and minimizing financial damage.
Collaboration with law enforcement/APS	Builds a rapid response network for suspected fraud cases, improving outcomes. Reporting incidents and sharing information shields vulnerable customers, aids investigations, and provides the bank safe harbor protections under laws like the Senior Safe Act.
Clear internal escalation procedures	Guides employees on exactly what to do if they suspect exploitation, ensuring no time is lost. A documented chain of command and action steps lead to efficient case handling, which can be critical in limiting fraud and satisfying regulatory expectations.

Each of these measures contributes to a culture of vigilance and care. Together, they form an integrated strategy to mitigate fraud risk when individuals attempt to circumvent the traditional POA route. By implementing these recommendations, financial institutions can better protect their customers' assets and dignity – fulfilling not just a legal obligation, but a moral one as well – while also protecting themselves from financial loss and reputational harm. In summary, the combination of **preventative education, well-defined policies, and responsive procedures** is the most effective way for banks to address the challenges posed by joint account fraud scenarios. With these safeguards in place, banks can confidently support their customers' needs without giving criminals an easy loophole to exploit.

Bank of America is now the first major bank to allow consumer clients to designate a *trusted* contact. Who is a person the bank can reach out to in cases of suspected financial exploitation, fraud, or if they're unable to reach the account holder.

B of A Trusted Contact:

What This Means for Clients

- A **trusted contact** is someone you authorize the bank to speak with about concerns related to your account.
- They **cannot access your funds or make transactions**, but they can help confirm your well-being or contact details.
- This feature is especially useful for **older adults**, those with health concerns, or anyone who wants an extra layer of protection.

How to Set It Up

Clients can:

- Visit the Bank of America Elder Financial Services page
- Schedule an appointment or use the **beneficiary self-service portal** to add or update a trusted contact

Would you like help drafting a training alert or educational slide that highlights this feature for financial institutions? It's a great fraud prevention tool to spotlight.

A trusted contact is an individual age 18 or older who is identified by you as someone we're able to contact about your account for any of the following reasons:

- To address suspicious financial activity on your account
- To confirm specifics of your current contact information
- To confirm your health status
- To confirm the identity of any legal guardian, executor, trustee or holder of a power of attorney.

A trusted contact is not able to see your balances, gather any information about you, conduct transactions on your behalf or make changes to your account (unlike an account co-owner, who is able to conduct transactions such as deposits and withdrawals).

Designating a trusted contact is easy

Bank of America is the first major bank to allow clients to designate a trusted contact. Simply schedule an appointment to start your request with a financial center associate. Be sure to bring your government-issued photo ID plus contact information (name, address, phone number and email) for the person you want to designate as your trusted contact.

Universal Trusted Contact Form Template

Purpose: This form enables financial institutions to designate a Trusted Contact Person for account holders, allowing the institution to reach out if concerns arise about financial exploitation, unusual activity, or diminished capacity.

Account Holder Information

- **Full Name:** _____
- **Date of Birth:** _____
- **Account Number(s):** _____

Trusted Contact Person Information

- **Full Name:** _____
- **Relationship to Account Holder:** _____
- **Phone Number(s):** _____
- **Email Address:** _____
- **Mailing Address:** _____

Consent & Acknowledgment

I, the account holder, authorize [Institution Name] to contact the Trusted Contact Person listed above if:

- I appear to be subject to fraud, exploitation, or cognitive decline;
- The institution cannot reach me after multiple attempts.
- There is suspicion of third-party control over my account.

This designation does NOT grant the Trusted Contact access to account funds, authorization to make transactions, or the power to act on my behalf.

- **Signature of Account Holder:** _____
- **Date:** _____

For Institution Use Only

- **Received by (Staff Name):** _____
- **Date Received:** _____
- **Verified Identity Documentation:** ☐ Yes ☐ No
- **System Notation Completed:** ☐ Yes ☐ No

This template aligns with FINRA Rule 4512 and CFPB elder protection recommendations. You could customize it with branding or integrate as a module in FRPA workshops to help standardize practices and reduce reliance on joint account workarounds.

When alerting frontline staff or relevant teams that a Trusted Contact has been engaged—or is about to be—your messaging should strike a balance between **clarity, urgency, and discretion**. Here's a structured approach you can adapt for internal fraud alerts, training modules, or policy language:

Sample Trusted Contact Alert Messaging

Subject Line Options (Internal Use)

- "Trusted Contact Outreach Initiated for [Client Last Name] – Suspicious Activity Observed"
- "Escalation Notice: Trusted Contact Designation Activated"
- "Client Unreachable – Trusted Contact Notification Triggered for Review"

Suggested Message Body Template

Summary: Account Holder [Full Name / Account Number] flagged for unusual activity. Unable to confirm legitimacy via standard client outreach protocols.

Action Taken: Per policy guidelines, Trusted Contact [Name] has been notified regarding current concerns involving [brief description: e.g., suspected phishing response, large transfer anomaly, cognitive decline indicators].

Notes:

- No financial authorization granted.
- Communication limited to verification and client wellbeing.
- Case remains open pending client follow-up or additional review.

Next Steps:

- Log contact attempt and response notes in client profile.
- Consider transaction holds or review escalation based on feedback from contact.
- If appropriate, notify Fraud, Elder Services, or Legal for cross-department follow-up.

Tone & Considerations

- **Neutral language** protects customer dignity (avoid "fraud victim" or "decline" terms).
- If customizing for training, include sample triggers like "multiple failed client callbacks" or "withdrawals inconsistent with historic behavior."
- Avoid direct financial details unless required—focus on legitimacy and safety concerns.

Contact Center Script – Trusted Contact Activation

Greeting + Verification: "Hello, thank you for calling [Institution Name]. May I verify your name and the account holder you're calling about today?"

Context Delivery: "We've recently observed activity on [Client Name]'s account that raised some concerns—for example, [insert trigger: suspicious withdrawal, failed outreach attempts, etc.]. For precautionary purposes, we've activated the Trusted Contact protocol."

Privacy + Role Clarification: "As a Trusted Contact, we're reaching out solely to confirm the client's wellbeing. You're not authorized for any transactional access—this call is strictly for verification and safeguarding purposes."

Guided Inquiry Examples:

- "Have you had recent contact with [Client Name]?"
- "Have you noticed any unusual behavior or changes that may impact decision-making?"
- "Is there a known caregiver or third party assisting with finances?"

Next Steps Summary: "Thank you for sharing that. We'll update our internal notes and continue monitoring. If needed, someone from our elder services or fraud prevention team may follow up."

Dashboard Monitoring Checklist – Post Trusted Contact Alert

🔍 Triggered By:

- [ ] Unusual withdrawal pattern
- [ ] Inability to reach client
- [ ] Behavioral concern from staff
- [ ] Caregiver interference

🗂️ Actions Taken:

- [ ] CRM note documented
- [ ] Trusted Contact reached (Y/N)
- [ ] Observations logged
- [ ] Internal escalation flagged (Fraud/Elder/Legal)

⏳ Ongoing Monitoring Timeline:

- [ ] 7-day transaction review
- [ ] Call log trend analysis

- [ ] Re-attempted client contact
- [ ] Legal hold evaluation (if applicable)

Document results. Date, Time, Contacted Party, Voice message and Text sent, results (action to be taken), and FI employee handling the contact, follow-up time frame to reconnect with account holder and /or trusted contact.

_____Prepared by:

John McCullough
FRPA President
612-328-3651
cppcfe@aol.com

Research Topic and Best Practices
Elderly Financial Exploitation: POA VS Joint Accounts and Use of Trusted Contact for FIs
Leading Services for Customers and Members of CU.