"The Ultimate Betrayal"
Elder Abuse & Financial Exploitation of Elderly Members

By: Franklin Drake
fdrake@smithdebnamlaw.com

Introduction: As our population ages, so does the membership of many CUs. Ageing members may become cognitively impaired, isolated, baffled by computer-driven banking practices and increasingly dependent on caretakers and family members. At the same time, they can cling to 20th-century conventions of personal privacy and a fierce desire to maintain their independence. Result: too many seniors become vulnerable to too-frequent financial exploitation. Estimates are that only 1 in 44 incidents of financial abuse are officially documented. Fully 90% of financial abusers of the elderly are not strangers; they are family members or "trusted others". What are earmarks of financial abuse? What duty does the CU owe to the elderly or disabled member? How is any duty best performed? What about privacy restrictions and potential liability for mistakes? *Read on.*

I. **JUST WHAT IS IT?** "Financial exploitation" of the elderly, in the eyes of law has a broad definition in federal statues, but state statutes may define it more narrowly.

A. One broadly useful definition of financial exploitation is found in the federal "Elder Justice Act of 2009", 42 USC §1397j(8). It is:

"the fraudulent or otherwise illegal, unauthorized, or improper act or process of and individual, *including a caregiver or fiduciary,* that uses the resources of an elder for monetary or personal benefit, profit or gain, or that results in depriving an elder of benefits, resources, belongings or assets." [Emphasis added].

B. Who qualifies as an "elder"? Under the same federal statute, anyone over age 60 (42 USC §1397j(5)).

C. However, any CU protocol addressing financial exploitation should be equally applied to *both* elders *and* those mentally or physically disabled members who are dependent on the care of others to conduct their business with you.

1. Elders can be ferociously protective of their privacy and personal independence and may be mentally **UN**impaired until their demise, but any policy should be uniformly applied by age, to avoid any appearance of discriminatory practices.

2. Mere physical disability alone does not create any presumption of special vulnerability to financial exploitation, but resultant physical isolation or loss of communication capacities can, when reliance on caregivers for all daily life functions is a result.

D. In contrast to federal law, state laws may define elders and the disabled somewhat differently, *e.g.,* age 65 or older (NCGS §108A-112 *et seq.,* S.C. Code §43-35-10(11)). Get your own local counsel to provide your state's statutory definition.

E. Some common forms of financial exploitation, usually by family and caregivers:

1. Outright theft of property – *e.g.,* "in anticipation of inheritance."

2. Misuse of a victim's income or assets or both, frequently in violation of some existing fiduciary duty. Greed can overcome guilt.

3. Forging checks and withdrawals without consent.

4. Fraudulent acquisition and/or use of powers of attorney ("POAs").

5. Changes in access to accounts, access to safe deposit boxes or ownership of certificates of deposit ("CDs").

II. **WHAT DOES FINANCIAL EXPLOITATION LOOK LIKE?** Similar to another famous example, most readers "know it when they see it." Some earmarks and examples of financial exploitation of the elderly or disabled:

A. Uncharacteristic *banking behavior* by a new or existing member:

1. Sudden appearance of a *new* member who is elderly or disabled, accompanied by 3rd person or represented via POA, with significant assets, complex financial structures, or requests for unusual services (*e.,g.,* out-of-US wire transfers.) Is the exploiter shifting a victim's accounts from a suspicious CU to a new institution?

2. Frequent, numerous changes of accounts from one branch to another within the same CU (to escape suspicious branch personnel);

3. Changes in and frequencies of account withdrawals;

4. Large withdrawals or balance transfers from recently-opened joint accounts or previously inactive accounts;

5. Increased and frequent ATM withdrawals when the member is isolated or home-bound AND has not accessed an ATM recently;

6. Sophisticated usage of web-based functions and services by elderly members who own rotary-dial phones or who have never demonstrated such computer skills in the past.

7. Increases in overdraft fees, unpaid statements, unpaid bills specially when someone else has been designated to make payments.

8. Monthly statements re-directed to addresses other than the elder's, multiple change-of-address requests, or return of undelivered mail.

9. Suspicious signatures on checks, endorsements, withdrawal slips, loan applications, etc., indicating a possible forgery, signature of blank documents or inconsistent handwriting (for those CUs whose members still engage in paper-based transactions.)

10. Sudden secured debt increases, especially if associated with a mortgage on previously un-mortgaged property, or a second mortgage.

11. Unusual increase in credit card transactions, especially for electronics, music, website "memberships" & similar products that an elder or disabled person would not need.

12. Repeated claims of lost checkbooks, lost or forgotten PINs, unauthorized withdrawals and disbursements.

13. Large, repeated financial gifts or contributions to new, unusual or unknown charitable institutions.

14. Sudden, unexplained account closure by longtime elderly members, including multiple accounts, government-benefit accounts, or early withdrawal of Certificates of Deposit despite the financial consequences.

15. Request for unusual banking services by an existing member (*e.g.*, wire transfers, foreign currency exchange into USD, authorization for auto-withdrawals by non-US entities).

B. Suspicious or anomalous *personal behavior* by the elder, the disabled person, or associated third parties, including for example:

1. Branch visits accompanied by a stranger, caregiver, or family member, especially when that 3rd party demonstrates an inappropriate interest in the depositor's financial matters, or the depositor appears nervous, afraid, intimidated, or reluctant to speak for themselves, or;

2. ANY degree of apparent coercion into any transactions by any third party, in the presence or hearing of your employee(s);

3. CTR-worthy cash withdrawals, whether by the depositor directly or indirectly through any third party, with or without a valid POA;

4. Unwillingness or reluctance of the 3rd party to allow the depositor to speak separately or in private with your employees, or other similar isolation of the depositor from direct contacts by phone or in person;

5. Inability of the depositor to answer substantive questions about the financial transaction, to sign required paperwork or to understand the consequences of their requests.

6. Depositor's expressions of fearfulness of institutionalization, foreclosure or eviction, especially when their property is not mortgaged.

7. Concern or confusion over "missing funds" in deposit accounts;

8. Excessively large "reimbursements" or "gifts" to caregivers or new friends, especially when requested remotely or in writing rather than in person;

9. Personal appearance of neglect in daily needs or insufficient care give their financial status (*e.g.*, soiled, odiferous, neglected appearance, nutritional deficiencies, etc.)

C. Suspicious or unusual documents or financial arrangements with or by 3rd parties, including:

1. POAs recently signed or re-issued, or attorney-in-fact re-designation, by depositors who appear confused or befuddled.

2. Refusal or reluctance by any attorney-in-fact on a POA to register the POA, or to prove their own identity, or to sign a notarized "Affidavit of Attorney-in-Fact" (see attached example) to validate their right to exercise the POA;

3. Sudden changes in wills, POAs, authorizations for entry into safe-deposit boxes, authorized signers on deposit accounts; re-designation of deposit account pay-on-death beneficiaries as account co-depositors;

4. New loans by third parties using POAs or using the depositor as a co-signer, where there is no obvious benefit to the elderly or disabled depositor;

5. New caregivers, or relatives or "friends" suddenly try to conduct financial transactions on the depositor's behalf, without proper documentation, or without ID.

6. Repeat presentation of multi-party checks endorsed in blank by the depositor, or of checks signed by the depositor but made payable in a different handwriting, or of checks made payable to "Cash".

7. Any other act, omission or practice that just "smells wrong". If it seems SAR-worthy, it is worthy of scrutiny for exploitation.

III. IS YOUR INSTITUTION LIABLE FOR ACCEPTANCE OF AN EXPLOITIVE OR MISUSED POWER OF ATTORNEY?

A. One of the most commonly-available devices to financially exploit elders and the disabled is the POA. Easily found on Internet websites for free download, all an exploiter needs is a cooperative Notary Public, and (s)he can easily secure *carte blanche* access to the victim's entire financial portfolio and existence.

B. Not all POAs are exploitative, and not all attorneys-in-fact are exploiters, but common sense and prudent practice dictate any financial institution adopt and use a uniform policy of what to honor, what to require and when to refuse a POA.

C. Require all POAs first to be read by qualified persons (at least management and at best your counsel) to verify the grant of banking authority and the proper form.

1. No presenter of a POA can initially expect immediate cooperation or assent by your CU. All POAs are subject to verification.

2. All attorneys-in-fact are subject to ID and OFAC check at the outset.

D. Verify that the POA has been notarized. A POA is worthless without a notary. Beware "military POAs" – *i.e.,* POAs bearing a military (or consular or embassy) notarization. Military POAs must be accepted without requirement of any particular format or prior courthouse registration, provided that banking functions are granting within it. *See,* 10 USC §1044(b) *et seq.*

1. Except with military POAs, seek a signed "Affidavit of Attorney-in-Fact" from the presenter, to be signed in the CU and notarized. *See attached example.*

2. Some states allow the CU to require the execution of such an Affidavit as a condition of honoring the POA, and allow refusal to honor the POA without it.

a. An "amateur" scoundrel may think twice before becoming both a thief *and* a perjurer, or just take the POA elsewhere.

b. Acquisition of the Affidavit can afford immunity to third parties or to the depositor of the CU, if the attorney-in-fact uses the POA to exploit the depositor. Check with your local counsel.

E. Except with military POAs, require the POA first be filed in the appropriate county courthouse as a condition precedent to honoring it. Local counsel can advise you on the correct filing point(s).

F. Provided the CU has no independent knowledge the POA was fraudulently obtained, or that the grantor has since died, or that the grantor has revoked the POA or changed designated attorneys-in-fact, it can usually be confident it will not be liable for relying in good faith on the POA

IV. **PREPARE NOW FOR FINANCIAL EXPLOITATION YOU WILL DISCOVER LATER**

A. Adopt a Board-approved policy to offer to protect all senior and disabled depositors from the risk of financial exploitation by 3rd parties, family members, and care-givers while maintaining their financial privacy.

1. Apply the policy to all elders and all vulnerable adults.

a. An "elder" should be age-defined according to your state's definition in its elder-protection statutes. (*E.g.* age 65 or older in NC (NCGS §108A-112)). In the absence of a state statute, consider the federal definition of 60 or older (See above).

b. A vulnerable adult should be defined any person over the age of 18, who has a physical or mental condition which substantially impairs the person from adequately providing for his or her own care or protection. More specifically, this should include any person who is impaired in the ability to provide for his or her own care or protection, due to physical, mental or emotional dysfunction.

2. Provide a letter allowing the depositor's designation of at least one (and preferably two) other individuals you may alert in the future, if you find or suspect financial exploitation of the elderly or disabled depositor is occurring, or has occurred. *See attached example.*

    a. Opportunity should be offered universally to every *new* elderly or vulnerable adult depositor upon joining, and every *existing* and future member on their "elder-qualifying birthday.

    b. Opportunity should be offered universally to every new depositor who appears to be disabled or a vulnerable person, and every existing depositor if they become so in the future.

    c. Opportunity can also be offered to anyone else who asks for it.

    d. Two named persons are better than one, since one of the named persons may be (or become) the exploiter.

3. Letter should be provided in paper format, so signatures can be verified *i.e.* signed in-person or signed remotely and notarized.) If it is completed electronically, require electronic notarization, to reduce the risk of a connivance by an exploiter.

4. Depositors cannot be required to complete a form and cannot be denied services merely because they refuse to complete a form, but you can caution them that if they later wish to change or withdraw a completed form, you will take special care at that time to verify no coercion or exploitation is occurring.

5. Provide the opportunity to vulnerable elders or the disabled in person, privately and in isolation from caregivers and other family members. Any refusal to allow such by those 3rd parties is suspicious, SAR-worthy behavior in itself.

B. Adopt a Board-approved policy, procedure and protocol of how to regard internally all suspicious behavior in the accounts of elders and the disabled, to include:

1. Employee training (especially of front-line CSR/MSR's & tellers) on how to spot and interpret evidence of financial exploitation of elders and the disabled, and inclusion in employee training and policy manuals.

2. An immediate internal report to management of any suspected financial exploitation, whether in-person, electronic, remote, via 3rd party or otherwise.

3. Authority to suspend any activity on account(s), block ATM cards, block credit card charges, hold withdrawal requests pending verification of legitimacy.

4. Sacrifice of speed of service for sureness of result. Slow down the transaction, and refer the applicant(s) up the chain of command. If they become angry or abusive, suspicion should be increased.

5. Abundant nosey questions. Require direct, specific answers. Implausible explanations or reasons by depositors and especially from 3rd parties are unacceptable.

6. If the depositor is accompanied by a 3rd party, question the depositor in private. Then, in private, ask the depositor to reiterate his request, to see if he makes sense the second time.

7. If the 3rd party is alone with a POA, or is communicating by telephone, ask to communicate directly with the depositor unless (s)he is unavailable (*e.g.*, comatose). Any excuse should increase suspicion.

8. Verification of authority and all signatures for authenticity.

9. For complete account closures, early redemption of CDs, etc., especially remotely, require written management authority in advance.

C. Establish the boundaries of allowed or required reporting to authorities within your own state's statutes, in advance.

1. All 50 states have adopted statutory standards that address financial exploitation of the elderly and other vulnerable persons. They are broadly similar, but differ in particulars.

    a. Seek local counsel's legal opinion of the content and provisions of the laws of your state, and all the state(s) where your branch(es) can be found.

    b. Most state statutes contain "safe harbor" provisions, which exempt reports of financial exploitation from privacy restrictions.

2. The vast majority of states (46 of 50) *require* rather than simply allow such reports to authorities, and sometimes to designated trusted persons. Regardless of your location, assume some sort of report to police authority(ies) is required. Get your local counsel to tell you when, how where.

3. Place in your favorites the contact info for your state's Adult Protective Services offices (or equivalent) and local law enforcement. Be ready to report, when the need arises. See www.eldercare.gov to locate easily APS offices by ZIP Code nationally. The APS office where the depositor lives is the correct one, not the one closest to your offices.

    a. Establish what level of internal management approval is required before reporting can occur.

    b. Establish alternative chains of command, so approval or reporting is not vulnerable to vacations, absences or unoccupied position(s) of critical management members.

V. FINANCIAL EXPLOITATION IS FOUND OR SUSPECTED. NOW WHAT?

A. Take comfort in the (somewhat qualified) words of CFPB Director Richard Cordray:

"Reporting suspected elder financial abuse to the appropriate authorities is typically the right thing to do and generally will not violate the Gramm-Leach-Bliley Act".

B. In 2013, the CFPB, NCUA & 6 other federal regulators issued a joint 5-page "Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults". *See attached.*

1. In the Guidance, the CFPB & others take pains to assure depositary institutions that they have no need to fear regulatory wrath for reporting actual or suspected financial exploitation of elders.

2. Examples of exploitation in the Guidance are reflected in those above.

C. No privacy requirement of Gramm-Leach-Bliley (GLB) applies to restrict reporting to correct authorities or to Adult Protective Services. Take even greater comfort in 31 USC §5318(g)(3)(A), on the question of liability to anyone for disclosure of such NPI of consumers:

"Any financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency or makes a disclosure pursuant to this subsection or any other authority, and any director, officer, employee, or agent of such institution who makes or requires another to make any such disclosure, *shall not be liable to any person under any law or regulation* of the United States, any constitution, law or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement) for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." [Emphasis added.]

D. GLB also permits disclosure of NPI to protect against or to prevent actual or potential fraud, unauthorized transactions, claims or other liability. Simply put, *GLB allows reports of real or suspected financial exploitation as an exception to privacy restrictions.*

E. Federal Right to Financial Privacy Act (12 USC §3401 *et seq.*) is applicable to all CUs regardless of charter (§3401(1)) and to all CU members and their authorized representatives under POAs (§3405(5)).

1. The Act expressly allows a financial institution to volunteer any information to federal authorities which may be relevant to even a *possible* violation of "any statute or regulation." 12 USC §3403(c)). That can include names and the nature of suspected illegal acts.

2. No prior notice of the disclosure to the depositor by the financial institution is required. The notice requirement is on the government, not on you.

3. The Act immunizes the disclosing institution from liability to the depositor and to third parties.

F. Even if the suspicion proves *incorrect*, a person who, acting "in good faith," reports should be immune from civil or criminal liability in an action related to the report, under states' laws.

G. State statutes normally contain substantially similar "immunity from liability" provisions, so absolute certainty should not be needed for a report. (*see, e.g.,* S.C. Code § 43-35-75(A), NCGS §108A-117(3)).

H. Expect to make at least a triple report, and possibly a 4-way report:

1. If the depositor has granted the CU advance permission to notify specific persons (s)he has provided in response to your "birthday letter" above, report the abuse to those designees (unless one of them is the exploiter).

2. Report to local law enforcement or the local District Attorney / Prosecutor. It is not necessary to report initially in complete or

specific detail, but do the research, have the dossier ready to hand over and tell the D.A. your homework is already done. That may increase the likelihood the D.A. will follow up for the details.

3. Report to local Adult Protective Services, using whatever contact info and whichever forms you had researched in advance. Often APS investigators are at least as diligent as police investigators can be.

4. File a SAR. Any financial exploitation is probably SAR-worthy.

I. Beware that 46 states have *mandatory* reporting requirements, which carry specific criminal or administrative penalties for an intentional failure to report. Refer to those penalties if any future depositor is found to have suffered a "false alarm". Even if your institution is not found criminally negligent in failure to report abuse, expect an exception on an examiner's report if (s)he concludes the CU should have made a report of clear abuse.

A. Once the reports are made, your duty is performed, and it falls to the authorities (local or federal or both) to follow up. The likeliest pressure-point is the APS offices. You may pester both the police and APS at will with follow-ups.

B. Can a CU flatly refuse services to an abuser or exploiter? YES, if it has the courage of its convictions. In addition, it can notify the suspect and/or the member that it intends to make a report to local authorities and to APS (but must NOT disclose any SAR filing).

1. If the refusal and report were justified, no liability results

2. If the refusal and report proved to be "false alarm" (this time), the depositor may be grateful and stay, or may be resentful, close all accounts and depart. In either event, the CU has resolved the issue.

3. There is no universal immunization from spurious civil Complaints from annoyed depositors, but the likelihood of any Court awarding damages for a report of potential elder abuse seem remote.

PRUDENT PRACTICE, PROPER REGARD FOR THE SAFETY OF DEPOSITORS, A UNIFORM POLICY AND UNIFORM APPLICATION ARE THE WISEST COURSE TO MINIMIZE EXPOSURE OF VULNERABLE MEMBERS TO FINANCIAL EXPLOITATION.

[Credit Union Letterhead]
[Date]

[Older Adult CU Member Name]
[Member Address]
[City, State, ZIP]

Re: Helping to protect our older and disabled members from financial exploitation [Insert state statute here].

Dear [Member Name]:

Your credit union is committed to protecting our senior members from the risk of financial exploitation. We offer you the opportunity to provide us with a list of persons who you trust, and to allow us to contact them if we suspect you ever become the victim of financial exploitation. Sometimes, third parties can try to take advantage of the trust and good will of seniors. Sometimes, seniors can become disabled, impaired and vulnerable to mistreatment by others. Now is the time to take steps to protect your future security. We want to make it easy.

We invite you to provide us now with a list of trusted family members or friends below. In the future, if we suspect you are being exploited financially, we can alert you *and* those you may list below. *Your participation in this program is purely voluntary*. You may change or remove any name(s) at any time, upon verified request to us. You may choose to list no one. We will always comply with your wishes in this matter.

We will keep any response to this letter that you send us entirely confidential, just as we do with all your other personal information. You may ask to participate in this program at any time in the future. We have enclosed a pre-addressed, stamped envelope for your convenient reply.

We hope we hear from you soon.

Sincerely,

[Your] Credit Union

[ ] If my Credit Union ever suspects I may have become a victim of financial exploitation, I ask that the following be notified of the nature of the exploitation and any other related information needed to protect me:

_____ _____ _____
_____ _____ _____
_____ _____ _____

I understand that I can change, remove or add to any of the above, at any time.

_____
[Member's Signature]
Date: _____