Elder Financial Abuse and Exploitation

Arkansas Tool Kit

Educating credit unions about elder financial abuse and exploitation is an initiative of REAL Solutions and the Cornerstone Credit Union League.
## Elder Financial Abuse and Exploitation

### Tool Kit Checklist

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EFAE Mission, Initiative, National Statistics, and Implementation</td>
</tr>
<tr>
<td>2</td>
<td>Important Facts for Credit Unions (includes Arkansas statutes)</td>
</tr>
<tr>
<td>3</td>
<td>Arkansas APS Document</td>
</tr>
<tr>
<td>4</td>
<td>Who Reports? Arkansas APS Document</td>
</tr>
<tr>
<td>5</td>
<td>Department of the Treasury—FinCEN Advisory</td>
</tr>
<tr>
<td>6</td>
<td>The Campaign against Financial Crimes: Reporting Suspicious Activity Q&amp;A</td>
</tr>
<tr>
<td>7</td>
<td>Sample Suspected Activity Report (SAR) for FinCEN</td>
</tr>
<tr>
<td>8</td>
<td>Model Policy 2245 (Sample EFAE Policy) from Policy Pro</td>
</tr>
<tr>
<td>9</td>
<td>Policy Pro Memo and How to Access</td>
</tr>
<tr>
<td>10</td>
<td>EFAE Posters</td>
</tr>
<tr>
<td>11</td>
<td>What to Do and Who to Call</td>
</tr>
<tr>
<td>12</td>
<td>Resources</td>
</tr>
</tbody>
</table>
Mission
To inform and educate credit unions in Arkansas, Oklahoma, and Texas about elder financial abuse and exploitation—what it is, how to identify it, and what to do about it.

Why the Focus on Elder Financial Abuse and Exploitation?
Elder abuse is a serious problem that is on the rise, including its subset, financial abuse and exploitation. Credit unions need to be concerned about financial abuse and exploitation (EFAE) in their elderly members, since they are the most likely victims of this crime. By state law, credit union employees are required to report cases of suspected EFAE or face penalties.

Credit unions must be trained to:
- identify suspected abuse,
- fill out appropriate agency incident forms, and
- report incidents to appropriate authorities.

Financial Abuse and Exploitation Defined
In general, elder abuse refers to intentional or neglectful acts that lead to, or may lead to, harm of a vulnerable older adult. Physical abuse, neglect, emotional or psychological abuse, verbal abuse and threats, financial abuse and exploitation, sexual abuse, and abandonment are considered forms of elder abuse. In many states, self-neglect is also considered mistreatment.

Financial exploitation may be further defined as "the illegal or improper act or process of a caretaker, family member, or other individual who has an ongoing relationship with the elderly or disabled person using the resources of an elderly or disabled person for monetary or personal benefit, profit, or gain without the informed consent of the elderly or disabled person."
# National Statistics on Elder Abuse

*Source: National Center on Elder Abuse, Bureau of Justice Statistics*

*Research Date: 9.12.2012*

<table>
<thead>
<tr>
<th>Elderly Abuse Statistics</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of elderly abuse cases in 2010</td>
<td>5,961,568</td>
</tr>
<tr>
<td>Percent of elderly population abused in 2010</td>
<td>9.5 %</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Demographics of Elderly Abuse Victims</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percent of female elder abuse victims</td>
<td>67.3 %</td>
</tr>
<tr>
<td>Median age of elder abuse victims</td>
<td>77.9</td>
</tr>
<tr>
<td>Percent of white victims</td>
<td>66.4 %</td>
</tr>
<tr>
<td>Percent of black victims</td>
<td>18.7 %</td>
</tr>
<tr>
<td>Percent of Hispanic victims</td>
<td>10.4 %</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Breakdown of Reported Elder Abuse Cases</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neglect</td>
<td>58.5 %</td>
</tr>
<tr>
<td>Physical Abuse</td>
<td>15.7 %</td>
</tr>
<tr>
<td><strong>Financial Exploitation</strong></td>
<td><strong>12.3 %</strong></td>
</tr>
<tr>
<td>Emotional Abuse</td>
<td>7.3 %</td>
</tr>
<tr>
<td>Sexual Abuse</td>
<td>0.04 %</td>
</tr>
<tr>
<td>All other types</td>
<td>5.1 %</td>
</tr>
<tr>
<td>Unknown</td>
<td>0.06 %</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Family Perpetrated Elderly Abuse</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Percent of Adult Protective Service cases that involve elderly abuse</td>
<td>68 %</td>
</tr>
<tr>
<td>Percent of elderly abuse perpetrated by adult children or spouses</td>
<td>66 %</td>
</tr>
<tr>
<td>Percent of murder victims over 60 who were killed by their own offspring</td>
<td>42 %</td>
</tr>
<tr>
<td>Percent of murder victims over 60 who were killed by their spouses</td>
<td>24 %</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nursing Home Abuse</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Percent of nursing homes that lack adequate staff to properly care for patients</td>
<td>91 %</td>
</tr>
<tr>
<td>Percent of nursing homes that have been in violation of elderly abuse laws</td>
<td>36 %</td>
</tr>
</tbody>
</table>
Preventing Elder Financial Abuse and Exploitation
Is Everyone's Business!

Important Facts for Credit Unions

Older Americans hold a high concentration of wealth as compared to the general population. In the instances where elderly individuals experience declining cognitive or physical abilities, they may find themselves more reliant on specific individuals for their physical wellbeing, financial management, and social interaction. While anyone can be a victim of a financial crime such as identity theft, embezzlement, and fraudulent schemes, certain elderly individuals may be particularly vulnerable.

Financial institutions may become aware of persons or entities perpetrating illicit activity against the elderly through monitoring transaction activity that is not consistent with expected behavior; or they may become aware of such scams through direct interactions with elderly customers who are being financially exploited. Credit union staff should evaluate indicators of potential financial exploitation in combination with other red flags and expected transaction activity conducted by or on behalf of the elder.

Abuse and exploitation of the elderly is statutorily defined at the state level, but the National Center on Elder Abuse defines financial exploitation this way: “the illegal taking, misuse, or concealment of funds, property, or assets of a vulnerable elder.”

State law (HR Code) requires that Adult Protective Services be contacted, if "during the scope of a person's employment, knowledge of possible abuse is occurring, even in cases where professional communications are generally held confidential."

In addition, the Financial Crimes Enforcement Agency (FinCEN) requires that a Suspicious Activity Report (SAR) be filed, in the case of elder financial abuse and exploitation. Read the advisory here: www.fincen.gov/statutes_regs/guidance/html/fin-2011-a003.html.

FinCEN's advisory contains examples of "red flags" based on activity identified by various state and federal agencies and provides a common narrative term that will assist law enforcement in better identifying suspected cases of financial exploitation of the elderly reported in SARs.

The Arkansas Statutes
Arkansas Reporting of Elder Abuse
Arkansas Code Annotated (A.C.A.)

Excerpts from A.C.A. Title 12: Law
Subchapter 17: The Adult and Long-term Care Facility Resident and Maltreatment Act
A.C.A. 12-12-1703: Definitions

(5) “Endangered person” means:
   (A) A person eighteen (18) years of age or older who:
       (i) is found to be in a situation or condition that poses a danger to himself or herself; and
(ii) Demonstrates a lack of capacity to comprehend the nature and consequences of remaining in that situation or condition; or

(B) A long-term care facility resident or an Arkansas State Hospital resident who:
   (i) Is found to be in a situation or condition that poses an imminent risk of death or serious bodily harm to the long-term care facility resident; and
   (ii) Demonstrates a lack of capacity to comprehend the nature and consequences of remaining in that situation or condition;

(6) “Exploitation” means the:
   (A) Illegal or unauthorized use or management of an endangered person’s or an impaired person’s funds, assets, or property;
   (B) Use of an adult endangered person’s or an adult impaired person’s power of attorney or guardianship for the profit or advantage of one’s own self or another;
   (C) The fraudulent or otherwise illegal, unauthorized, or improper act or process of a person, including a caregiver or fiduciary, that uses the resources of an endangered person, impaired person, or long-term care facility resident for monetary or personal benefit, profit, or gain, or that results in depriving the endangered person, impaired person, or long-term care facility resident of rightful access to or use of benefits, resources, belongings, or assets; or
   (D) Misappropriation of property of a long-term care facility resident, that is, the deliberate misplacement, exploitation, or wrongful, temporary, or permanent use of a long-term care facility resident’s belongings or money without the long-term care facility resident’s consent;

(9)
   (A) “Impaired person” means a person eighteen (18) years of age or older who as a result of mental or physical impairment is unable to protect himself or herself from abuse, sexual abuse, neglect, or exploitation.
   (B) For purposes of this subchapter, a long-term care facility resident is presumed to be an impaired person.
   (C) For purposes of this subchapter, a person who has a representative payee appointed for the person by the Social Security Administration or another authorized agency is presumed to be an impaired person in relation to adult maltreatment through financial exploitation;

(13) “Maltreated adult” means an adult who has been abused, exploited, neglected, physically abused, or sexually abused;

(14) “Maltreated person” means a person, regardless of age, who has been abused, exploited, neglected, physically abused, or sexually abused;

A.C.A. 12-12-1708: Persons Required to Report Adult or Long-term Care Facility Resident Maltreatment

(a)

(1) Whenever any of the following persons has observed or has reasonable cause to suspect that an endangered person or an impaired person has been subjected to conditions or circumstances that constitute adult maltreatment or long-term care facility resident
maltreatment, the person shall immediately report or cause a report to be made in accordance with the provisions of this section:

(A) A physician;
(B) A surgeon;
(C) A coroner;
(D) A dentist;
(E) A dental hygienist;
(F) An osteopath;
(G) A resident intern;
(H) A nurse;
(I) A member of a hospital's personnel who is engaged in the administration, examination, care, or treatment of persons;
(J) A social worker;
(K) A case manager;
(L) A home health worker;
(M) A mental health professional;
(N) A peace officer;
(O) A law enforcement officer;
(P) A facility administrator or owner;
(Q) An employee in a facility;
(R) An employee of the Department of Human Services;
(S) A firefighter;
(T) An emergency medical technician;
(U) An employee of a bank or other financial institution;
(V) An employee of the United States Postal Service;
(W) An employee or a volunteer of a program or an organization funded partially or wholly by the department who enters the home of or has contact with an elderly person;
(X) A person associated with the care and treatment of animals, such as animal control officers and humane society officials;
(Y) An employee who enforces code requirements for a city, township, or municipality;
or
(Z) Any clergy member, including without limitation, a minister, a priest, a rabbi, an accredited Christian Science practitioner, or any other similar functionary of a religious organization, or an individual reasonably believed to be a minister, a priest, a rabbi, an accredited Christian Science practitioner, or any other similar functionary of a religious organization by the person consulting him or her, except to the extent he or she:
   (i) Has acquired knowledge of suspected maltreatment through communications required to be kept confidential pursuant to the religious discipline of the relevant denomination or faith; or
   (ii) Received the knowledge of the suspected maltreatment from the offender in the context of a statement of admission.

(2) Whenever a person is required to report under this subchapter in his or her capacity as a member of the staff, an employee in or owner of a facility, or an employee of the department, he or she shall immediately notify the person in charge of the institution, facility, or agency, or that person’s designated agent, who shall then become responsible for making a report or cause a report to be made within twenty-four (24) hours or on the next business day, whichever is earlier.
(3) In addition to those persons and officials required to report suspected maltreatment, any other person may make a report if the person has observed an adult or long-term care facility resident being maltreated or has reasonable cause to suspect that an adult or long-term care facility resident has been maltreated.

Penalties A.C.A. 5-28-110

§ 5-28-110. Penalties

(a) Any person or caregiver required by the Adult and Long-Term Care Facility Resident Maltreatment Act, § 12-12-1701 et seq., to report a case of suspected adult maltreatment or long-term care facility resident maltreatment who purposely fails to do so is:
   (1) Guilty of a Class B misdemeanor; and
   (2) Civilly liable for damages proximately caused by the failure.

(b) Any person, official, or institution willfully making a false notification by the Adult and Long-Term Care Facility Resident Maltreatment Act, § 12-12-1701 et seq., knowing the allegation to be false, is guilty of:
   (1) Class A misdemeanor; or
   (2) Class D felony if the person, official, or institution has been previously convicted of making a false allegation.

(c) Any person who willfully permits and any other person who encourages the release of data or information contained in the adult and long-term care facility maltreatment central registry to a person to whom disclosure is not permitted under this section is guilty of a Class A misdemeanor.

(d) Any person required to report a death as the result of suspected adult maltreatment or long-term care facility resident maltreatment who knowingly fails to make a report immediately to the appropriate coroner is guilty of a Class C misdemeanor.

(e) Any person required to report suspected adult maltreatment or long-term care facility resident maltreatment who knowingly fails to make a report within twenty-four (24) hours or on the next business day, whichever is earlier, is guilty of a Class C misdemeanor.

Safe Harbor

A.C.A. § 12-12-1713

§ 12-12-1713. Immunity for investigation participants

(a) Any person, official, or institution acting in good faith in the making of a report, the taking of a photograph, or the removal of a maltreated person under this subchapter shall have immunity from liability and suit for damages, civil or criminal, that otherwise might result by reason of those actions.

(b) The good faith of any person required to report a case of adult maltreatment or long-term care facility resident maltreatment shall be presumed.

Adult Protective Services
Call 1-800-482-8049
http://www.aradultprotection.com/
1-800-482-8049 - Adult Abuse Hotline

What we Do.

- **Who**
  Who are we talking about
- **APS History**
  How APS Services Evolved
- **Self Neglect**
  Self Neglect
- **Dementia**
  Dementia
- **Families and Dementia**
  Families and Dementia
- **Staff**
  Adult Protection Staff
- **Who Reports**
  Anyone or Mandated?

---

Insignificant
as a beached shell
I feel
the indifferent succession
of days
monotonous as ocean waves.

---

-- Lynn Kozma

**Aging is a natural process, abuse is not.** In spite of the
headway that has been made in explaining how and why elder
abuse occurs, it still remains a poorly understood problem in
our state. No simple definition can encompass its many
aspects. Elder mistreatment may be an act of commission
(abuse) or omission (neglect). It may be an intentional act,
that is, a conscious attempt to inflict suffering, or it may be
unintentional because of inadequate knowledge, infirmity, or
laziness on the part of the person responsible. Now is the time
to stop it...Stop ignoring the abuse and neglect....**You can
make a difference!**

**Endangered and Impaired Adults/Who Are We Talking About?**
**How Adult Protective Services Evolved**
**Self-Neglect**
**Dementia**
**Families Coping with Dementia**
**Guard the future - respect the Past**

**Adult Protective Services Staff**

*Back to the Division of Aging and Adult Services website*
1-800-482-8049 - Adult Abuse Hotline

What we Do.

Who
Who are we talking about

APS History
How APS Services Evolved

Self Neglect
Self Neglect

Dementia
Dementia

Families and Dementia
Families and Dementia

Staff
Adult Protection Staff

Who Reports
Anyone or Mandated?

Who Reports?

Anyone can report, however, *mandated reporters are required by law* to report suspected abuse, neglect, or exploitation of endangered or impaired adults.

**ACA 12-12-1708** lists the persons required to report abuse, stating:

(a)(1) Whenever any of the following has observed or has reasonable cause to suspect that an endangered or impaired adult has been subjected to conditions or circumstances which would reasonable result in abuse, sexual abuse, neglect, or exploitation, as defined in this chapter, he or she shall immediately report or cause a report to be made in accordance with the provisions of this section:

- Physician
- Surgeon
- Coroner
- Dentist
- Dental hygienist
- Osteopath
- Resident intern
• A nurse
• Hospital personnel engaged in administration, examination, care, or treatment of persons
• Social worker
• Case manager
• A home health worker
• Mental health professional
• Peace officer
• Law enforcement officer
• Facility administrator or owner
• Employee of a facility
• Employee of the Department of Human Services
• Firefighter
• Emergency medical technician
• An employee of a bank or other financial institution

(2) Whenever a person is required to report under this chapter in his or her capacity as a member of the staff, an employee in a facility, or an employee of the department, he or she shall immediately notify the person in charge of the institution, facility, or agency, or that person’s designated agent, who shall then become responsible for making a report or cause a report to be made.

(3) In addition to those persons and officials required to report suspected adult abuse, sexual abuse, or neglect, any other person may make a report if the person has reasonable cause to suspect that an adult has been abused, neglected, or exploited, as defined in this chapter.

(b)(1) A report required under this chapter shall be made to the central registry (800-482-8049) by the receiving agency for abused or neglected adults not residing in long-term care facilities.

(2) A report for abused or neglected adults residing in a long-term care facility shall be made immediately to the local law enforcement agency for the jurisdiction in which the facility is located and to the Office of Long-Term Care of the Division of Medical Services of the Department of Human Services, pursuant to regulations of that office.
(3) The office shall notify this central registry and the office of the Attorney General.

(c) No privilege of contract shall relieve anyone required by this subchapter to make notification of the requirement of making notification.

Amended 2006
The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to assist the financial industry in reporting instances of financial exploitation of the elderly, a form of elder abuse. Financial institutions can play a key role in addressing elder financial exploitation due to the nature of the client relationship. Often, financial institutions are quick to suspect elder financial exploitation based on bank personnel familiarity with their elderly customers. The valuable role financial institutions can play in alerting appropriate authorities to suspected elder financial exploitation has received increased attention at the state level; this focus is consistent with an upward trend at the federal level in Suspicious Activity Reports (SARs) describing instances of suspected elder financial exploitation. Analysis of SARs reporting elder financial exploitation can provide critical information about specific frauds and potential trends, and can highlight abuses perpetrated against the elderly.

This advisory contains examples of “red flags” based on activity identified by various state and federal agencies and provides a common narrative term that will assist law enforcement in better identifying suspected cases of financial exploitation of the elderly reported in SARs.

Older Americans hold a high concentration of wealth as compared to the general population. In the instances where elderly individuals experience declining cognitive or physical abilities, they may find themselves more reliant on specific individuals for their physical well-being, financial management, and social interaction. While anyone can be a victim of a financial crime such as identity theft, embezzlement, and fraudulent schemes, certain elderly individuals may be particularly vulnerable.

**Potential Indicators of Elder Financial Exploitation**

The following red flags could indicate the existence of elder financial exploitation. This list of red flags identifies only possible signs of illicit activity. Financial institutions

---

1 A buse and exploitation of the elderly is statutorily defined at the state level. The National Center on Elder Abuse offers the following definition of exploitation as a type of elder abuse: “the illegal taking, misuse, or concealment of funds, property, or assets of a vulnerable elder.”

2 Bank Secrecy Act data reflects increasing use of terms related to elder financial exploitation/abuse in SAR narratives.
should evaluate indicators of potential financial exploitation in combination with other red flags and expected transaction activity being conducted by or on behalf of the elder. Additional investigation and analysis may be necessary to determine if the activity is suspicious.

Financial institutions may become aware of persons or entities perpetrating illicit activity against the elderly through monitoring transaction activity that is not consistent with expected behavior. In addition, financial institutions may become aware of such scams through their direct interactions with elderly customers who are being financially exploited. In many cases, branch personnel familiarity with specific victim customers may lead to identification of anomalous activity that could alert bank personnel to initiate a review of the customer activity.

• Erratic or unusual banking transactions, or changes in banking patterns:
  o Frequent large withdrawals, including daily maximum currency withdrawals from an ATM;
  o Sudden Non-Sufficient Fund activity;
  o Uncharacteristic nonpayment for services, which may indicate a loss of funds or access to funds;
  o Debit transactions that are inconsistent for the elder;
  o Uncharacteristic attempts to wire large sums of money;
  o Closing of CDs or accounts without regard to penalties.

• Interactions with customers or caregivers:
  o A caregiver or other individual shows excessive interest in the elder’s finances or assets, does not allow the elder to speak for himself, or is reluctant to leave the elder’s side during conversations;
  o The elder shows an unusual degree of fear or submissiveness toward a caregiver, or expresses a fear of eviction or nursing home placement if money is not given to a caretaker;
  o The financial institution is unable to speak directly with the elder, despite repeated attempts to contact him or her;
  o A new caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of the elder without proper documentation;
  o The customer moves away from existing relationships and toward new associations with other “friends” or strangers;
  o The elderly individual’s financial management changes suddenly, such as through a change of power of attorney to a different family member or a new individual;
The elderly customer lacks knowledge about his or her financial status, or shows a sudden reluctance to discuss financial matters.

**Suspicious Activity Reporting**

SARs continue to be a valuable avenue for financial institutions to report elder financial exploitation. Consistent with the standard for reporting suspicious activity as provided for in 31 CFR Part 103 (future 31 CFR Chapter X), if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, the financial institution should then file a Suspicious Activity Report.3

In order to assist law enforcement in its effort to target instances of financial exploitation of the elderly, FinCEN requests that financial institutions select the appropriate characterization of suspicious activity in the Suspicious Activity Information section of the SAR form and include the term “elder financial exploitation” in the narrative portion of all relevant SARs filed. The narrative should also include an explanation of why the institution knows, suspects, or has reason to suspect that the activity is suspicious. It is important to note that the potential victim of elder financial exploitation should not be reported as the subject of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.

Elder abuse, including financial exploitation, is generally reported and investigated at the local level, with Adult Protective Services, District Attorney’s offices, sheriff’s offices, and police departments taking key roles. We emphasize that filers should continue to report all forms of elder abuse according to institutional policies and the requirements of state and local laws and regulations, where applicable. Financial institutions may wish to consider how their AML programs can complement their policies on reporting elder financial exploitation at the local and state level.

Financial institutions with questions or comments regarding this Advisory should contact FinCEN's Regulatory Helpline at 800-949-2732.

---

3 Financial institutions shall file with FinCEN to the extent and in the manner required a report of any suspicious transaction relevant to a possible violation of law or regulation. A financial institution may also file with FinCEN a Suspicious Activity Report with respect to any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by FinCEN regulations. See, e.g., 31 CFR § 103.18(a) (future 31 CFR § 1020.320(a)).
REPORTING SUSPICIOUS ACTIVITY:
Q&A FOR MONEY SERVICES BUSINESSES

As of January 1, 2002, certain money services businesses (MSBs) became obligated under the Bank Secrecy Act to report suspicious activity to the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN). Following are answers to frequently asked questions about this requirement.

**To which businesses does this rule apply?**

This rule applies to any business that:

- Provides **money transfers** in any amount; or
- Issues, sells, or redeems **money orders** or **traveler’s checks** in an amount greater than $1,000 for the same customer on the same day in either instrument, or
- Provides **currency dealing or exchange** in an amount greater than $1,000 for the same customer on the same day in either activity.

**What is suspicious activity?**

Suspicious activity is any transaction or pattern of transactions that the MSB knows, suspects or has reason to suspect meets any of the following four conditions:

- **Involves funds from an illegal activity**, or attempts to hide funds raised from illegal activity.
- **Appears to be an attempt to evade Bank Secrecy Act requirements**, such as filing of a Currency Transaction Report (CTR), by breaking a large transaction into smaller amounts.
- **Seems to have no business or other lawful purpose** and available facts provide no reasonable explanation.
- **Involves use of the money services business to facilitate criminal activity.**

**Must all suspicious activity be reported?**

Suspicious activity, as described above, must be reported if it involves transactions or attempted transactions at or above a certain amount:

- **$2,000 or more** --- for transactions conducted or attempted by, at or through an affected money services business, the threshold of $2,000 applies;
- **$5,000 or more** --- for transactions identified by issuers of money orders or traveler’s checks from a review of clearance records or other similar records of instruments that have been sold or processed, the threshold of $5,000 applies.

**How does a business report suspicious activity?**

Suspicious Activity Report by MSB forms are available at [www.msb.gov](http://www.msb.gov) or by calling the IRS forms distribution center at 1-800-829-3676. Completed forms should be sent to: Detroit Computing Center, ATTN: SAR-MSB, P.O. Box 33117, Detroit, MI 48232-5980.

**Other reporting requirements:**

1. **Deadline:** MSBs have 30 calendar days to file a Suspicious Activity Report after becoming aware of a suspicious transaction.
2. **Urgency:** If a situation seems to require urgent attention, the MSB should immediately notify the appropriate law enforcement authority, as well as file the required form.
3. **Confidentiality:** It is against the law to inform anyone other than an appropriate law enforcement or supervisory agency that a Suspicious Activity Report has been filed.
4. **Liability:** The law protects MSBs that report suspicious activity from civil liability.

**For More Information**

Free materials are available to help MSBs learn more about the requirement to report suspicious activity. To order, please visit [www.msb.gov](http://www.msb.gov) or call 1-800-386-6329.

This guidance is intended to explain only general issues about the SAR requirement for MSBs, under 31 CFR Part 103. The guidance does not replace or supercede the regulation.
Suspicious Activity Report

Filing name

*1 Type of filing
(Check all that apply)

- Initial report
- Correct/Amend prior report
- Continuing activity report
- Joint report

Prior report Document Control Number/BSA Identifier

Attachment

Under penalties of perjury, I declare that I have examined this transmittal, including accompanying documents, and to the best of my knowledge and belief it is correct and complete. In the case of documents without recipient's identifying numbers, I have complied with the requirements of the law in attempting to secure such numbers from the receipts. I declare that this filing represents all Documents filed during this reporting period except for those transactions reported on paper.

Sign with PIN
Part IV Filing Institution Contact Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>82</td>
<td>Type of financial institution</td>
</tr>
<tr>
<td>78</td>
<td>Primary federal regulator</td>
</tr>
<tr>
<td>79</td>
<td>Filer name (Holding company, lead financial institution, or agency, if applicable)</td>
</tr>
<tr>
<td>80</td>
<td>TIN</td>
</tr>
<tr>
<td>81</td>
<td>TIN type</td>
</tr>
<tr>
<td>83</td>
<td>Type of Securities and Futures institution or individual filing this report - check box(es) for functions that apply to this report</td>
</tr>
<tr>
<td>84</td>
<td>Financial institution identification Type</td>
</tr>
<tr>
<td>85</td>
<td>Address</td>
</tr>
<tr>
<td>86</td>
<td>City</td>
</tr>
<tr>
<td>87</td>
<td>State</td>
</tr>
<tr>
<td>88</td>
<td>ZIP/Postal Code</td>
</tr>
<tr>
<td>89</td>
<td>Country</td>
</tr>
<tr>
<td>90</td>
<td>Alternate name, e.g., AKA - individual or trade name, DBA - entity</td>
</tr>
<tr>
<td>91</td>
<td>Internal control/file number</td>
</tr>
<tr>
<td>92</td>
<td>LE contact agency</td>
</tr>
<tr>
<td>93</td>
<td>LE contact name</td>
</tr>
<tr>
<td>94</td>
<td>LE contact phone number (Include Area Code) Ext.</td>
</tr>
<tr>
<td>95</td>
<td>LE contact date</td>
</tr>
<tr>
<td>96</td>
<td>Filing institution contact office</td>
</tr>
<tr>
<td>97</td>
<td>Filing institution contact phone number (Include Area Code) Ext.</td>
</tr>
<tr>
<td>98</td>
<td>Date filed (Date filed will be auto-populated when the form is signed.)</td>
</tr>
</tbody>
</table>
### Part III Information about Financial Institution Where Activity Occurred

<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>47</strong> Type of financial institution</td>
<td></td>
</tr>
<tr>
<td><strong>48</strong> Primary federal regulator</td>
<td></td>
</tr>
<tr>
<td><strong>49</strong> Type of gaming institution</td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="https://example.com/checkbox-options.png" alt="Checkbox Options" /></td>
</tr>
<tr>
<td><strong>50</strong> Type of Securities and Futures institution or individual where activity occurred</td>
<td><img src="https://example.com/checkbox-options.png" alt="Checkbox Options" /></td>
</tr>
<tr>
<td><strong>51</strong> Financial institution identification</td>
<td></td>
</tr>
<tr>
<td><strong>52</strong> Financial institution's role in transaction</td>
<td></td>
</tr>
<tr>
<td><strong>53</strong> Legal name of financial institution</td>
<td><img src="https://example.com/unknown.png" alt="Unknown" /></td>
</tr>
<tr>
<td><strong>54</strong> Alternate Name, e.g., AKA - individual or trade name, DBA - entity</td>
<td></td>
</tr>
<tr>
<td><strong>55</strong> TIN</td>
<td><img src="https://example.com/unknown.png" alt="Unknown" /></td>
</tr>
<tr>
<td><strong>56</strong> TIN type</td>
<td></td>
</tr>
<tr>
<td><strong>57</strong> Address</td>
<td><img src="https://example.com/unknown.png" alt="Unknown" /></td>
</tr>
<tr>
<td><strong>58</strong> City</td>
<td><img src="https://example.com/unknown.png" alt="Unknown" /></td>
</tr>
<tr>
<td><strong>59</strong> State</td>
<td></td>
</tr>
<tr>
<td><strong>60</strong> ZIP/Postal Code</td>
<td><img src="https://example.com/unknown.png" alt="Unknown" /></td>
</tr>
<tr>
<td><strong>61</strong> Country</td>
<td><img src="https://example.com/unknown.png" alt="Unknown" /></td>
</tr>
<tr>
<td><strong>62</strong> Internal control/file number</td>
<td></td>
</tr>
<tr>
<td><strong>63</strong> Loss to financial institution</td>
<td>$ .00</td>
</tr>
</tbody>
</table>

#### Branch where activity occurred information

**If no branch activity involved, check this box [ ]**

<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>64</strong> Branch's role in transaction</td>
<td><img src="https://example.com/checkbox-options.png" alt="Checkbox Options" /></td>
</tr>
<tr>
<td><strong>65</strong> Address of branch or office where activity occurred</td>
<td></td>
</tr>
<tr>
<td><strong>67</strong> City</td>
<td></td>
</tr>
<tr>
<td><strong>68</strong> State</td>
<td></td>
</tr>
<tr>
<td><strong>66 RSSD Number</strong></td>
<td></td>
</tr>
<tr>
<td><strong>69</strong> ZIP/Postal Code</td>
<td></td>
</tr>
<tr>
<td><strong>70</strong> Country</td>
<td></td>
</tr>
</tbody>
</table>
**Part I Subject Information**

1 of 1

2. Check:  
   - [ ] if entity,  
   - [ ] if all critical* subject information is unavailable (Does not include item 24)

3. Individual's last name or entity's legal name: [ ] Unknown

4. First name: [ ] Unknown

5. Middle name/initial:  
   - [ ] Suffix:  
   - [ ] Gender:  

6. Date of birth: [ ] Unknown

6a. Alternate name, e.g., AKA - individual or trade name, DBA - entity:  

7. Occupation or type of business:  

7a. NAICS Code:  

13. TIN: [ ] Unknown

14. TIN type:  

18. Phone number:  
   - [ ] Ext.:  
   - [ ] 17 Type:  

19. E-mail address:  

19a Website (URL) address:  

20. Corroborative statement to filer? [ ]  
   - [ ] 25 Subject's role in suspicious activity:  

**Subject Address Information**

8. Address: [ ] Unknown

9. City: [ ] Unknown

10. State: [ ] Unknown

11. ZIP/Postal Code: [ ] Unknown

12. Country: [ ] Unknown

15. Form of identification for subject: [ ] Unknown  
   - [ ] Type:  
   - [ ] Number:  
   - [ ] Issuing State:  
   - [ ] Country:  

21. Relationship of the subject to an institution listed in Part III or IV (check all that apply)
   
a. Institution TIN:  
   
b. Accountant  
   - [ ] Attorney  
   - [ ] Director  
   - [ ] Officer  
   - [ ] Owner or Controlling Shareholder  
   - [ ] Other  
   
c. Agent  
   - [ ] Borrower  
   - [ ] Employee  
   - [ ] No relationship to institution  
   - [ ] Other  
   
d. Appraiser  
   - [ ] Customer  
   - [ ] No relationship to institution  
   - [ ] Other  

22. Status of relationship:  

23. Action date:  

24. Financial institution TIN and account number(s) affected that are related to subject:  
   - [ ] No known accounts involved  
   - [ ] Non-US Financial Institution  
   - [ ] Closed? Yes  

Page 4 of 7
### Part II Suspicious Activity Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>Amount involved in this report</td>
</tr>
<tr>
<td>27</td>
<td>Date range of suspicious activity</td>
</tr>
<tr>
<td>28</td>
<td>Cumulative amount (only applicable when &quot;Continuing activity report&quot; is checked in Item 1)</td>
</tr>
</tbody>
</table>

#### When completing Item 29 through 38, check all that apply

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>Structuring</td>
</tr>
<tr>
<td>a</td>
<td>Alters transaction to avoid BSA recordkeeping requirement</td>
</tr>
<tr>
<td>b</td>
<td>Alters transaction to avoid CTR requirement</td>
</tr>
<tr>
<td>c</td>
<td>Customer cancels transaction to avoid BSA reporting and recordkeeping requirements</td>
</tr>
<tr>
<td>d</td>
<td>Multiple transactions below BSA recordkeeping threshold</td>
</tr>
<tr>
<td>e</td>
<td>Multiple transactions below CTR threshold</td>
</tr>
<tr>
<td>f</td>
<td>Suspicious inquiry by customer regarding BSA reporting or recordkeeping requirements</td>
</tr>
<tr>
<td>z</td>
<td>Other</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Terrorist Financing</td>
</tr>
<tr>
<td>a</td>
<td>Known or suspected terrorist/terrorist organization</td>
</tr>
<tr>
<td>z</td>
<td>Other</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>Fraud (Type)</td>
</tr>
<tr>
<td>a</td>
<td>ACH</td>
</tr>
<tr>
<td>b</td>
<td>Business loan</td>
</tr>
<tr>
<td>c</td>
<td>Check</td>
</tr>
<tr>
<td>d</td>
<td>Consumer loan</td>
</tr>
<tr>
<td>e</td>
<td>Credit/Debit card</td>
</tr>
<tr>
<td>f</td>
<td>Healthcare</td>
</tr>
<tr>
<td>g</td>
<td>Mail</td>
</tr>
<tr>
<td>h</td>
<td>Mass-marketing</td>
</tr>
<tr>
<td>i</td>
<td>Pyramid scheme</td>
</tr>
<tr>
<td>j</td>
<td>Wire</td>
</tr>
<tr>
<td>z</td>
<td>Other</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>Casinos</td>
</tr>
<tr>
<td>a</td>
<td>Inquiry about end of business day</td>
</tr>
<tr>
<td>b</td>
<td>Minimal gaming with large transactions</td>
</tr>
<tr>
<td>c</td>
<td>Suspicious intra-casino funds transfers</td>
</tr>
<tr>
<td>d</td>
<td>Suspicious use of counter checks or markers</td>
</tr>
<tr>
<td>z</td>
<td>Other</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>a</td>
<td>Exchange small bills for large bills or vice versa</td>
</tr>
<tr>
<td>b</td>
<td>Suspicion concerning the physical condition of funds</td>
</tr>
<tr>
<td>c</td>
<td>Suspicion concerning the source of funds</td>
</tr>
<tr>
<td>d</td>
<td>Suspicious designation of beneficiaries, assignees or joint owners</td>
</tr>
<tr>
<td>e</td>
<td>Suspicious EFT/wire transfers</td>
</tr>
<tr>
<td>f</td>
<td>Suspicious exchange of currencies</td>
</tr>
<tr>
<td>g</td>
<td>Suspicious receipt of government payments/benefits</td>
</tr>
<tr>
<td>h</td>
<td>Suspicious use of multiple accounts</td>
</tr>
<tr>
<td>i</td>
<td>Suspicious use of noncash monetary instruments</td>
</tr>
<tr>
<td>j</td>
<td>Suspicious use of third-party transactors (straw-man)</td>
</tr>
<tr>
<td>k</td>
<td>Trade Based Money Laundering/Black Market Peso Exchange</td>
</tr>
<tr>
<td>l</td>
<td>Transaction out of pattern for customer(s)</td>
</tr>
<tr>
<td>z</td>
<td>Other</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
<td>Identification/Documentation</td>
</tr>
<tr>
<td>a</td>
<td>Changes spelling or arrangement of name</td>
</tr>
<tr>
<td>b</td>
<td>Multiple individuals with same or similar identities</td>
</tr>
<tr>
<td>c</td>
<td>Provided questionable or false documentation</td>
</tr>
<tr>
<td>d</td>
<td>Refused or avoided request for documentation</td>
</tr>
<tr>
<td>e</td>
<td>Single individual with multiple identities</td>
</tr>
<tr>
<td>z</td>
<td>Other</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>Other Suspicious Activities</td>
</tr>
<tr>
<td>a</td>
<td>Account takeover</td>
</tr>
<tr>
<td>b</td>
<td>Bribery or gratuity</td>
</tr>
<tr>
<td>c</td>
<td>Counterfeit instruments</td>
</tr>
<tr>
<td>d</td>
<td>Elder financial exploitation</td>
</tr>
<tr>
<td>e</td>
<td>Embezzlement/theft/disappearance of funds</td>
</tr>
<tr>
<td>f</td>
<td>Forgeries</td>
</tr>
<tr>
<td>g</td>
<td>Identity theft</td>
</tr>
<tr>
<td>h</td>
<td>Little or no concern for product performance penalties, fees, or tax consequences</td>
</tr>
<tr>
<td>i</td>
<td>Misuse of &quot;free look&quot;/cooling-offright of rescission</td>
</tr>
<tr>
<td>j</td>
<td>Misuse of position or self-dealing</td>
</tr>
<tr>
<td>k</td>
<td>Suspected public/private corruption (domestic)</td>
</tr>
<tr>
<td>l</td>
<td>Suspected public/private corruption (foreign)</td>
</tr>
<tr>
<td>m</td>
<td>Suspected use of informal value transfer system</td>
</tr>
<tr>
<td>n</td>
<td>Suspected use of multiple transaction locations</td>
</tr>
<tr>
<td>o</td>
<td>Transaction with no apparent economic, business, or lawful purpose</td>
</tr>
<tr>
<td>p</td>
<td>Two or more individuals working together</td>
</tr>
<tr>
<td>q</td>
<td>Unauthorized electronic intrusion</td>
</tr>
<tr>
<td>r</td>
<td>Unlicensed or unregistered MSB</td>
</tr>
<tr>
<td>z</td>
<td>Other</td>
</tr>
</tbody>
</table>
### 36 Insurance

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Excessive insurance</td>
<td>e</td>
<td>Suspicious termination of policy or contract</td>
</tr>
<tr>
<td>b</td>
<td>Excessive or unusual cash borrowing against policy/annuity</td>
<td>f</td>
<td>Unclear or no insurable interest</td>
</tr>
<tr>
<td>c</td>
<td>Proceeds sent to or received from unrelated third party</td>
<td>z</td>
<td>Other</td>
</tr>
<tr>
<td>d</td>
<td>Suspicious life settlement sales insurance (e.g., STOLI's, Viaticals)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 37 Securities/Futures/Options

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Insider trading</td>
<td>d</td>
<td>Unauthorized pooling</td>
</tr>
<tr>
<td>b</td>
<td>Market manipulation/wash trading</td>
<td>z</td>
<td>Other</td>
</tr>
<tr>
<td>c</td>
<td>Misappropriation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 38 Mortgage Fraud

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Appraisal fraud</td>
<td>d</td>
<td>Reverse mortgage fraud</td>
</tr>
<tr>
<td>b</td>
<td>Foreclosure fraud</td>
<td>z</td>
<td>Other</td>
</tr>
<tr>
<td>c</td>
<td>Loan Modification fraud</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 39 Were any of the following product type(s) involved in the suspicious activity? (Check all that apply)

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Bonds/Notes</td>
<td>g</td>
<td>Futures/Options on futures</td>
<td>m</td>
<td>Options on securities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>Commercial mortgage</td>
<td>h</td>
<td>Hedge fund</td>
<td>n</td>
<td>Penny stocks/Microcap securities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>Commercial paper</td>
<td>i</td>
<td>Home equity loan</td>
<td>o</td>
<td>Prepaid access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td>Credit card</td>
<td>j</td>
<td>Home equity line of credit</td>
<td>p</td>
<td>Residential mortgage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e</td>
<td>Debit card</td>
<td>k</td>
<td>Insurance/Annuity products</td>
<td>q</td>
<td>Security futures products</td>
<td></td>
<td></td>
</tr>
<tr>
<td>f</td>
<td>Forex transactions</td>
<td>l</td>
<td>Mutual fund</td>
<td>r</td>
<td>Stocks</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>s</td>
<td>Swap, hybrid, or other derivatives</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>z</td>
<td>Other (List below)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 40 Were any of the following instrument type(s)/payment mechanism(s) involved in the suspicious activity? (Check all that apply)

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Bank/Cashier's check</td>
<td>d</td>
<td>Gaming instruments</td>
<td>g</td>
<td>Personal/Business check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>Foreign currency</td>
<td>e</td>
<td>Government payment</td>
<td>h</td>
<td>Travelers checks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>Funds transfer</td>
<td>f</td>
<td>Money orders</td>
<td>i</td>
<td>U.S. Currency</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>z</td>
</tr>
</tbody>
</table>

### 41 Commodity type (If applicable)

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

### 42 Product/Instrument description (If needed)

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

### 43 Market where traded

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

### 44 IP address (If available)

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

### 45 CUSIP® number

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>
Part V  Suspicious Activity Information - Narrative*
Model Policy 2245
Protecting the Elderly and Vulnerable from Fraud

General Policy Statement
Credit unions are in a unique position to detect and prevent financial exploitation and fraud. The primary roles of the Credit Union are the protection of its members’ assets and the prevention of financial losses. The Credit Union will take steps to protect elderly and vulnerable members from financial exploitation and fraud by training staff to recognize the types of financial scams, the red flags of potential abuse and what to do when fraud is suspected.

Guidelines:

1. **ROLE OF BOARD OF DIRECTORS.** The Board of Directors will (1) approve the credit union’s written Elderly and Vulnerable Protection policy and program; and (2) oversee the development, implementation, and maintenance of the Credit Union’s program, including assigning specific responsibility for its implementation, and reviewing reports from management.

2. **ROLE OF MANAGEMENT TEAM.** The management team will (1) oversee the development and implementation of the Elderly and Vulnerable Protection program; (2) draft procedures to ensure compliance with the program; (3) monitor, evaluate and suggest adjustments to the program; (4) ensure that staff are trained on these issues at least annually; and (5) brief the Board of Directors of the Credit Union at least annually on the status of the program. In addition to the annual report, the Board of Directors may allow the management team the option to provide [2245-1] reports.

3. **TYPES OF FINANCIAL EXPLOITATION.** Credit Union staff should be aware of the following types of financial exploitation:
   - **Theft of Income.** The most common form of financial fraud and exploitation, typically involving less than $1,000 per transaction.
   - **Theft of Assets.** This is often more expensive and typically involves abuse associated with Powers of Attorney, real estate transactions, identity theft or tax manipulation.

4. **TYPES OF FINANCIAL SCAMS.** Although this is not an exhaustive list, Credit Union staff will be trained to be aware of the following types of financial scams:
   - **Power of Attorney Fraud.** The perpetrator obtains a Limited or Special Power of Attorney, which specifies that legal rights are given to manage the funds in the account. Once the rights are given, the perpetrator uses the funds for personal gain.
   - **Advance Fee Fraud or “419” Fraud.** Named after the relevant section of the Nigerian Criminal Code, this fraud involves a multitude of schemes and scams – mail, e-mail, fax and telephone promises that the victims will receive a percentage for their assistance in the scheme proposed in the correspondence.
C. **Pigeon Drop.** The victim puts up “good faith” money in the false hope of sharing the proceeds of an apparently large sum of cash or item(s) of worth which are “found” in the presence of the victim.

D. **Financial Institution Examiner Fraud.** The victim believes that he or she is assisting authorities to gain evidence leading to the apprehension of a financial institution employee or examiner that is committing a crime. The victim is asked to provide cash to bait the crooked employee. The cash is then seized as evidence by the “authorities” to be returned to the victim after the case.

E. **Inheritance Scams.** Victims receive mail from an “estate locator” or “research specialist” purporting an unclaimed inheritance, refund or escheatment. The victim is lured into sending a fee to receive information about how to obtain the purported asset.

F. **Financial Institution Employee Fraud.** The perpetrator calls the victim pretending to be a security officer from the victim’s financial institution. The perpetrator advises the victim that there is a system problem or internal investigation being conducted. The victim is asked to provide his or her Social Security number for “verification purposes” before the conversation continues. The number is then used for identity theft or other illegal activity.

G. **International Lottery Fraud.** Scam operators, often based in Canada, use telephone and direct mail to notify victims that they have won a lottery. To show good faith, the perpetrator may send the victims a check. The victim is then instructed to deposit the check and immediately send (via wire) the money back to the lottery committee. The perpetrator will create a “sense of urgency,” compelling the victim to send the money before the check, which is counterfeit, is returned. The victim is typically instructed to pay taxes, attorney’s fees, and exchange rate differences in order to receive the rest of the prize. These lottery solicitations violate U.S. law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail.

H. **Fake Prizes.** A perpetrator claims the victim has won a nonexistent prize and either asks the person to send a check to pay the taxes or obtains the credit card or checking account number to pay for shipping and handling charges.

I. **Internet Sales or Online Auction Fraud.** The perpetrator agrees to buy an item for sale over the Internet or in an online auction. The seller is told that he or she will be sent an official check (e.g., cashier’s check) via overnight mail. When the check arrives, it is several hundred or thousand dollars more than the agreed-upon selling price. The seller is instructed to deposit the check and refund the overpayment. The official check is later returned as a counterfeit but the refund has already been sent. The seller is left with a loss, potentially of both the merchandise and the refund.

J. **Government Grant Scams.** Victims are called with the claim that the government has chosen their family to receive a grant. In order to receive the money, victims must provide their checking account number and/or other personal information. The perpetrator may electronically debit the victim’s account for a processing fee, but the grant money is never received.

K. **Spoofing.** An unauthorized website mimics a legitimate website for the purpose of deceiving consumers. Consumers are lured to the site and asked to log in, thereby providing the perpetrator with authentication information that the perpetrator can use at the victim’s legitimate financial institution’s website to perform unauthorized transactions.
L. **Phishing/Vishing/Smishing.** Technology or social engineering is used to entice victims to supply personal information (i.e., account numbers, login IDs, passwords, and other verifiable information) that can then be exploited for fraudulent purposes, including identity theft. These scams are most often perpetrated through mass e-mails, spoofed websites, phone calls or text messages.

M. **Stop Foreclosure Scam.** The perpetrator claims to be able to instantly stop foreclosure proceedings on the victim’s real property. The scam often involves the victim deeding the property to the perpetrator who says that the victim will be allowed to rent the property until some predetermined future date when the victim’s credit will have been repaired, and the property will be deeded back to the victim without cost. Alternatively, the perpetrator may offer the victim a loan to bridge his or her delinquent payments, perhaps even with cash back. Once the paperwork is reviewed, the victim finds that his or her property was deeded to the perpetrator. A new loan may have been taken out with an inflated property value with cash back to the perpetrator, who now owns the property. The property very quickly falls back into foreclosure and the victim/tenant is evicted.

5. **ROLE OF CREDIT UNION STAFF.** Although this is not an exhaustive list, Credit Union staff will be trained to spot the following red flags that are often associated with financial scams:
   A. Signatures seem forged or unusual.
   B. Check numbers are out of sync.
   C. A vulnerable adult informs staff that funds are “missing” from his or her account.
   D. Abrupt changes in a will or other financial documents.
   E. It is requested that account or credit card statements are to be sent to an address other than the vulnerable adult’s home.
   F. Unusual cash withdrawals from a checking account within a short period of time.
   G. Abrupt increase in credit card activity.
   H. A sudden flurry of bounced checks.
   I. An account shows ATM activity when it is known that the vulnerable adult is physically unable to leave his or her home.
   J. The vulnerable adult is accompanied by a third party who encourages the withdrawal of a large sum of cash, and may not allow the vulnerable adult to speak.
   K. Abrupt and unexplained change in a financial Power of Attorney; new names added to signature cards; new joint account created.
   L. Discovery of incapacitated vulnerable adult’s signature for financial transactions or for title of real or personal property.
   M. Sudden appearance of previously uninvolved relatives claiming rights to the adult’s affairs and possessions.
   N. Adult has no knowledge of newly-issued ATM, debit or credit card.
   O. Adult is confused about account balance or transaction on his or her account.
   P. A caregiver appears to be getting paid too much or too often.
   Q. Significant increases in monthly expenses being paid from the account.
   R. Adult reports concern over having given out personal information to a solicitor over the phone.
   S. Unexplained sudden transfer of assets, particularly real property.
   T. Expressed excitement about winning a sweepstakes, lottery or inheritance.
   U. Refinance of the adult’s property, with significant cash out, or with the addition of new owners on the deed, but not on the loan.
6. **WHAT TO DO IF FRAUD IS SUSPECTED.** Management will develop procedures, and Credit Union staff will be trained to take the following actions when fraud is suspected:

   A. Carefully verify anyone’s authority who is acting on the member’s behalf.
   
   B. Use probing questions to determine the member’s intent regarding a transaction.
   
   C. For large cash withdrawals that appear out of the ordinary, have the member sign an “awareness document,” and ask the member to sign it prior to the receipt of funds. This form could include the following:
      
      i. Brief overviews of common fraud schemes.
      
      ii. Warnings that perpetrators of such schemes could present themselves as an FBI agent, financial institution examiner or official, police officer, or detective.
      
      iii. Warnings that members should use caution if they are asked for information about their account, or asked to withdraw money to help “catch someone,” or provide money to show “good faith.”
      
      iv. Notice that the Credit Union does not conduct investigations or verification of accounts by telephone, nor will local, state or federal law enforcement authorities, financial institution regulatory authorities or officials conduct investigations by asking individuals to withdraw cash from their account for any reason.
      
      v. Phone numbers for the appropriate agencies, if any of the circumstances listed about are in evidence, with instructions to members that they should contact their branch, local police department, Adult Protective Services or the Federal Trade Commission to investigate before they withdraw money.
      
      vi. Reminders that swindlers are almost always friendly and have “honest” faces and that they particularly tend to take advantage of older individuals.
      
      vii. The amount the member has requested, with a request to read and sign the document.

   D. Delay the suspicious transaction, if possible, by advising the member that additional verification of the transaction is required.
   
   E. Contact management for assistance and guidance. Management may be required to contact the credit union’s legal counsel for such assistance.
   
   F. File a Suspicious Activity Report (SAR), using the term “Elder Financial Exploitation” in the narrative.
   
   G. Report the incident to law enforcement following the credit union’s normal protocol.

7. **LOSS PREVENTION AND SECURITY.** Management will develop procedures, and Credit Union staff will be trained to take the following loss prevention and security steps when financial fraud occurs or is suspected:

   A. Document the situation.
   
   B. File a SAR, using the term “Elder Financial Exploitation” in the narrative
   
   C. Take immediate protective action on accounts by placing holds or restraints and follow normal prevention and recovery steps to follow the money as needed.
   
   D. Make a verbal report to the local Adult Protective Services and provide investigative research and services as needed.
   
   E. Continue to monitor the account during legal proceedings, of necessary.
   
   F. Document files of final outcome.

*Content of this policy is derived from the "BITs Fraud Protection Toolkit Preventing the Elderly and Vulnerable from Financial Fraud and Exploitation."*
CU PolicyPro

Cornerstone Credit Union League has partnered with CU Solutions Group and InfoSight to provide a new compliance product to all credit unions members as dues supported service. This is another benefit of your Cornerstone membership.

CU PolicyPro is an online operations policy manual that contains a comprehensive suite of more than 200 model policies which have been researched, developed, and written specifically for credit unions by regulatory experts. CU PolicyPro not only includes the model policy content, but a full policy content management system (CMS) that allows credit unions to customize any model content to fit the credit union’s own operations. The publishing tool allows multiple policies to be compiled into one printable document that can be posted in read-only format on the site for staff, board, or examiners to view.

Features and Benefits:

- CU PolicyPro is web based, allowing 24/7 access from any computer
- Model policies can easily be added, removed, or customized
- Existing credit union policies can be copied into the system
- System supports multiple users with varying levels of access
- Semi-annual updates provided
- Fully compliant with NCUA regulations
- Offsite backup
- New and advanced user training is available
- CU Solutions Group is available to assist with questions related to technical support, content, or general best practices and tips for using the manual.

Registration Process

- Each credit union will receive its own “manual” so registration is required.
- Only one person should register from each credit union. This person will be designated as the “primary admin” user for the credit union. The primary admin user will have the ability to add additional staff as users who will then be able to access the credit union’s CU PolicyPro manual.
- To learn more about CU PolicyPro, please click here. Please make sure to fill in the "exact" full spelling of your credit union name for verification.
- Two-to-three days after registration, you’ll receive a welcome email packet from the CU Solutions Group, which will include login and training information.

Free Online Video Training for New Users

- To get started, take advantage of the free on-demand video training, which you can access on the CU PolicyPro site's "New User Training" section.

If you have any questions about CU PolicyPro, please contact Nathan Behncke, at (512) 853-8514, or email nbehhcke@cornerstoneleague.coop for more information.
If it’s not your money, it’s a crime.

Signs of elder financial abuse and exploitation:

- Sudden changes in credit union account or practices
- Unexplained or unexpected withdrawal of large sums of money
- The inclusion of additional names on an elderly person's signature card
- Unfamiliar person accompanying customer to withdraw a large sum of money
- Adding names to an account signature card
- Unauthorized withdrawal of funds using ATM card
- Abrupt changes in financial documents
- Unexplained purchases
- Abuse of funds by person with a power of attorney
- Unexplained loss of funds or valuable possessions
- Unpaid bills, despite having adequate money
- Sudden appearance of previously uninvolved relatives claiming rights to a person's affairs and possessions
- Unexplained sudden transfer of assets

What can you do about it?

Report abuse. Call 800-252-5400

Preventing financial exploitation is everyone’s business.

Adult Protective Services
Texas Department of Family and Protective Services
everyonebusiness.org
May is Elder Abuse Prevention Month

Preventing financial exploitation is everyone’s business.

Elders throughout the U.S. lose an estimated $2.6 billion or more annually due to elder financial abuse and exploitation—funds that could have been used to pay for basic needs such as housing, food, and medical care.

Department of Health & Human Services Administration on Aging

What can **YOU** do about it?

Report abuse. Call 800-252-5400

Adult Protective Services
Texas Department of Family and Protective Services
everyonesbusiness.org

Educating credit unions about elder financial abuse is an initiative of REAL Solutions and the Cornerstone Credit Union League.
June 15th

World Elder Abuse Awareness Day

Preventing financial exploitation is everyone’s business.

What if your caregiver took your money—money you needed for living expenses?

What would you do if all of your savings disappeared?

While seniors 60 and older make up 15% of the U.S. population, they account for roughly 30% of fraud victims. Americans over age 65 lost $2.9 billion in 2010—a 12% increase from 2008.

Financial institutions may be the first line of defense in preventing elder financial exploitation. Know your responsibilities when it comes to identifying and protecting your members’ assets.

What can YOU do about it?

Report abuse.
Call 800-252-5400
Adult Protective Services
Texas Department of Family & Protective Services
everyonesbusiness.org

Real Solutions
Cornerstone

Educating credit unions about elder financial abuse is an initiative of REAL Solutions and the Texas Credit Union League.
Elder Financial Abuse and Exploitation

What to Do

1. Tell your supervisor.

2. Complete a Suspicious Activity Report (SAR).
   * Go online to FinCEN to retrieve the SAR form.

Who to Call

1. Call your local law enforcement office:
   #______________________________

2. Call your state adult protective services or office of the attorney general:
   #______________________________

Questions? Contact Paula Upchurch at REAL Solutions
832.407.7965 or 800.442.5762, Ext. 6822
pupchurch@tcul.coop
Resources
Your Quick Reference Guide

American Society on Aging
800-537-9728
asaging.org

Arkansas Adult Protective Services
Adult Abuse Hotline: 800-482-8049
aradultprotection.com

Arkansas Attorney General
Consumer Protection
501-682-2341
800-482-8982
ArkansasAG.gov
GotYourBackArkansas.org
arkansasag.gov/programs/seniors

Arkansas Elder Abuse
arkansasag.gov/programs/seniors/elder-abuse

Elder Justice Coalition
1612 K Street, NW, Suite 400
Washington, DC 20006
Phone: 202-682-4140
elderjusticecoalition.com/

Financial Crimes Enforcement Network (FinCEN)
Law Enforcement General Info: 703-905-3591
fincen.gov

Legal Hotline for Older Texans
800-622-2520
tls.org

National Center on Elder Abuse
202-898-2586
ncea.aoa.gov

National Council on the Aging
800-424-9046
ncoa.org

National Fraud Information Center
800-876-7060
fraud.org

Oklahoma Attorney General
Consumer Protection
405-521-3646
oag.state.ok.us/

Oklahoma Adult Protective Services
After-Hours Abuse Hotline: 800-522-3511
okdhs.org/programsandservices/aging/default.htm

Older Americans Month
"Unleash the Power of Age"
olderamericansmonth.acl.gov

Texas Attorney General
Consumer Protection
800-621-0508
oag.state.tx.us
800-252-8011
texasattorneygeneral.gov/elder/index.shtml

Texas Adult Protective Services (APS)
(Texas DFPS)
24/7 Abuse Hotline: 800-252-5400
dfps.state.tx.us/everyonesbusiness/default.asp
Make a report on TDFPS secure website:
txabusehotline.org

U.S. Administration on Aging
202-619-0724
aoa.dhhs.gov