**DRAFT \*\*\*\* Model Policy 2245: Elder and/or Vulnerable Adult Protections \*\*\*\* DRAFT

NOTE: This draft model policy is not intended as nor provided as legal advice. Neither the MCUL & Affiliates nor any of its employees provides legal advice in any capacity. This template will require customization by credit unions to account for their own unique experience, procedures, etc. Informally, inclusion of or reference to specific training programs and reporting procedures, as well as timing of filing any SAR may be advisable. Any policy to be adopted by a credit union should be carefully reviewed by their own legal counsel.**

|  |
| --- |
| **Model Policy Revised Date:** **General Policy Statement:**Credit Unions are in a unique position to detect prevent, and respond to financial exploitation. The primary roles of [[CUname]] (Credit Union) are the protection of its members’ assets and the prevention of financial losses. The Credit Union will take steps to protect members who are vulnerable adults (as defined herein) [as well as \_\_\_\_\_] from covered financial exploitation by training staff to recognize common types and signs of financial exploitation, and to follow established procedures when covered financial exploitation is suspected or detected. The Credit Union may disclose nonpublic personal information to comply with federal, state, or local laws, rules, and other applicable legal requirements, such as state laws that require reporting by financial institutions of suspected abuse. The Credit Union may delay or place a freeze on the transaction(s) or asset(s) relative to the member’s individual or jointly held accounts when covered financial exploitation is suspected or detected. This policy has been revised to comply with Michigan’s Financial Exploitation Prevention Act, MCL 487.2081, *et seq*.**Definitions:**As used in this Policy:1. "Vulnerable adult" means an adult who, because of mental or physical impairment or advanced age, is unable to protect himself or herself from covered financial exploitation.
2. "Financial exploitation" means either of the following:

a) A fraudulent or otherwise illegal, unauthorized, or improper act or process of an individual who uses or attempts to use the financial resources of another individual for monetary or personal benefit, profit, or gain.b) A fraudulent or otherwise illegal, unauthorized, or improper act or process of an individual that results or is intended to result in depriving another individual of rightful access to or use of benefits, resources, belongings, or assets.1. “Covered financial exploitation” means financial exploitation of an individual through deception, manipulation, coercion, intimidation, or improper leveraging of a caregiver relationship.
2. “Caregiver” means a parent or other relative responsible for the health and safety of an individual, or a guardian, conservator, or any other person with legal or fiduciary obligations to an individual.
3. “Law Enforcement Agency” means a police agency of a city, village, township, or county or the Michigan state police.
4. “Adult protective services,” means the office, division, or unit under the department of health and human services that is charged with the investigation of abuse, neglect, or exploitation of vulnerable persons under the social welfare act, 1939 PA 280, MCL 400.1 to 400.119b.

**Guidelines:**1. **ROLE OF BOARD OF DIRECTORS.** The Board of Directors will (1) approve the Credit Union’s written Elder and Vulnerable Adult Protection Policy (“Policy”) and program (“Program”); (2) oversee the development, implementation, and maintenance of the Policy and Program; (3) delegate specific responsibility for the implementation of the Policy and Program; and (4) review reports from management.
2. **ROLE OF MANAGEMENT TEAM.** The management team will (1) oversee the development and implementation of Policy and Program; (2) draft procedures to ensure compliance with the Policy and Program; (3) monitor, evaluate and suggest adjustments to the Policy and Program; (4) ensure that staff are trained on the Policy and Program at least annually; (5) serve as point of contact for any suspected or detected financial exploitation; (6) escalate suspected or detected financial exploitation to the Law Enforcement Liaison for investigation; and (7), report to the Board of Directors 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.

**ROLE OF DESIGNATED LAW ENFORCEMENT LIAISON.** The Board of Directors will designate [Title of Credit Union contact] as Law Enforcement Liaison. This individual will be responsible for (1) investigating any suspected or detected financial exploitation; (2) making required reports to the appropriate Law Enforcement Agency or Adult Protective Services; (3) providing notice to the County Prosecutor in cases where the Law Enforcement Agency or Adult Protective Services has failed to respond to a report filed by the Credit Union, (4) providing notice to the County Prosecutor in cases where the Law Enforcement Agency or Adult Protective Services does not provide required follow-up notifications after a report is filed by the Credit Union with a Law Enforcement Agency or Adult Protective Services; (5) serving as the primary point of contact for financial exploitation investigations conducted by a Law Enforcement Agency and/or Adult Protective Services; (6) reviewing and implementing as needed the content from relevant federal advisory opinions or guidance on elder financial exploitation. and (7) retaining all documentation as required by this Policy.**Training Requirements:**1. **STAFF TRAINING.** The Credit Union will conduct annual training for staff that addresses, at a minimum, the topics outlined in section 2. In the case of newly employed member-facing employees, staff will be trained within 90 days of hire. Training will be appropriate to the job responsibilities of the individual attending the training. The Credit Union will maintain a record of the current employees who have completed the training, including a record of the content of the training, and will make such records available to any agency having examination authority over the Credit Union. The Credit Union will not maintain training records with respect to employees who have left their employment with the Credit Union.
2. **CONTENT OF TRAINING.** The training will cover at a minimum the following topics:
	1. Common types of covered financial exploitation.
	2. Signs of potential covered financial exploitation.
	3. Relevant federal advisory opinions or guidance on elder financial exploitation.
	4. Internal procedures to be followed (i) when covered financial exploitation of a member is suspected or detected based on available facts; (ii) when after an examination or investigation of available facts, covered financial exploitation of a member is no longer suspected; and (iii) for delaying or placing a freeze on the transaction(s) or asset(s) relative to a member’s individually or jointly held accounts when covered financial exploitation is suspected or detected.
	5. Reporting procedures for reporting suspected or detected covered financial exploitation to a Law Enforcement Agency or Adult Protective Services.
	6. The need to protect the privacy and respect the integrity of Credit Union members.
3. **ADDITIONAL TRAINING CONSIDERATIONS.** The training may also include procedures for reporting any other category of affected members, as well as all members at the credit union’s discretion. For example, training may be expanded to include potential human trafficking or foster care fraud examples.
4. **COMMON TYPES OF FINANCIAL EXPLOITATION.** Credit Union staff should be aware of the following types of financial exploitation:
	1. Theft of Income. The most common form of financial exploitation, typically involving less than $1,000 per transaction.
	2. Theft of Assets. This often includes a higher dollar loss and typically involves abuse associated with Powers of Attorney, real estate transactions, investment fraud, identity theft, and/or tax manipulation.
5. **TYPES OF FINANCIAL SCAMS.** Although this is not an exhaustive list, Credit Union staff will be trained on the following types of financial scams:
	1. 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 member’s account. Once the rights are given, the perpetrator uses the funds for personal gain.
	2. 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 assurances that the victims will receive a percentage of assets for their assistance.
	3. Pigeon Drop. The victim or “pigeon” puts up good faith money in the false hope of securing a larger sum of “lost” money, or a more valuable object. The good faith money is lost and the larger sum of money or more valuable object is also lost or does not materialize.
	4. 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.
	5. 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.
	6. Financial Institution Employee Fraud. The perpetrator calls or texts 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.
	7. International Lottery Fraud. Scam operators, often based in Canada, use telephone and direct mail to notify the victim that they have won a lottery. To show good faith, the perpetrator may send the victim 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.
	8. 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.
	9. 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.
	10. Government Grant Scams. The victim is contacted with the claim that the government has chosen the victim to receive a grant. To receive the money, the victim must provide a checking account number and/or other personal information. The perpetrator may electronically debit the victim’s account for a “processing fee,” and the grant money is never received.
	11. 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.
	12. 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.
	13. Stop Foreclosure Scam. There are several versions of this scam. In one version, 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. In a second version, 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. In a third version of this scam, the perpetrator tells the victim to pay the perpetrator a fee to negotiate with the mortgage holder on behalf of the victim to reduce the victim’s mortgage payments or outstanding principal owed on the home. The perpetrator also tells the victim to withhold payment on the mortgage while the perpetrator is supposedly negotiating with the bank. The victim loses the fee to the perpetrator, and the victim’s home moves into foreclosure due to non-payment.
	14. Investment fraud. The perpetrator holds themselves out to the victim to be an investment-advisor or broker-dealer (regardless of whether the perpetrator is licensed or not). The perpetrator tells the victim that they can offer the victim a guaranteed rate of return on a little-known investment opportunity, causing the victim to “invest” large amounts of money with the perpetrator. The perpetrator may provide the victim with homemade account statements, IOUs, or other documents purporting to show that the victim’s investment is earning a high rate of return, when in reality, the perpetrator has spent the victim’s money for the perpetrator’s own personal or business use.
6. **SIGNS OF POTENTIAL FINANCIAL EXPLOITATION.**  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 exploitation:
	1. Signatures seem forged or unusual.
	2. Check numbers are out-of-sync.
	3. A [vulnerable adult] informs staff that funds are “missing” from his or her account.
	4. Abrupt changes in a will or other financial documents.
	5. Requests that account or credit card statements be sent to an address other than the vulnerable adult’s home.
	6. Unusual cash withdrawals from a checking account within a short period of time.
	7. Abrupt increase in credit card activity.
	8. A sudden flurry of bounced checks.
	9. An account shows ATM activity when it is known that the vulnerable adult is physically unable to leave his or her home.
	10. The [vulnerable adult] is accompanied by a third party who encourages the withdrawal of a large sum, whether in cash or otherwise, of may not allow the vulnerable adult to speak.
	11. Abrupt and unexplained change in a financial Power of Attorney; new names added to signature cards; new joint account created.
	12. Discovery of incapacitated [vulnerable adult’s] signature for financial transactions or for title of real or personal property.
	13. Sudden appearance of previously uninvolved relatives claiming rights to manage the [vulnerable adult’s] financial affairs/possessions, including the right to access the [vulnerable adult’s] account information.
	14. [Vulnerable adult] has no knowledge of newly-issued ATM, debit or credit card.
	15. [Vulnerable adult] is confused about account balance or transaction on his or her account.
	16. A caregiver appears to be getting paid too much or too often.
	17. Significant increases in monthly expenses being paid from the account.
	18. [Vulnerable adult] reports concern over having given out personal information.
	19. Unexplained sudden transfer of assets, particularly real property.
	20. Expressed excitement about winning a sweepstakes or lottery, or receiving an inheritance.
	21. Refinance of the [vulnerable adult’s] property resulting in access to significant cash, or with the addition of new owners on the deed, but not on the loan.

**NOTE: Some member commentary has also suggested including items like: Transactions by the family caregiver that do not seem to be in the interest of the member, such as excessive spending on travel, jewelry, or cars; member is reluctant to talk to you about matters he or she usually discusses; member seems nervous, anxious, or fidgety; member avoids eye contact; and member is negative or unresponsive.****Response and Reporting**1. **WHAT TO DO IF FINANCIAL EXPLOITATION IS SUSPECTED OR DETECTED.** Management will develop procedures, and Credit Union staff will be trained to take the following actions when financial exploitation is suspected or detected:
	1. Thoroughly verify the authority of anyone purporting to be acting on the member’s behalf.
	2. Use probing questions to determine the member’s intent regarding a transaction.
	3. Report suspected or detected financial exploitation to direct manager for additional investigation and potential escalation to Law Enforcement Liaison.
2. **WHAT TO DO IF FINANCIAL EXPLOITATION IS WITNESSED.** In some cases, Credit Union staff may witness financial exploitation that requires an immediate response. In these instances, Credit Union staff should:
	1. Seek out the support and advice of their manager or supervisor to properly handle the member situation.
	2. Once safe to do so, Management will follow the steps outlined in 3, to document and report the exploitation.
3. **MANAGEMENT RESPONSE.** Management will develop procedures to ensure proper escalation of suspected or detected covered financial exploitation to the Law Enforcement Liaison. Management may, at their discretion:
	1. For matters determined to be an emergency, or if the covered financial exploitation is actively taking place on-site:
		1. Contact 911.
		2. Notify the Law Enforcement Liaison.
	2. In all situations, contact the Law Enforcement Liaison for assistance and guidance. The Law Enforcement Liaison may be required to contact the Credit Union’s legal counsel for guidance.
	3. Where possible, delay the suspicious transaction and/or freeze the member’s accounts, by advising the member that additional verification of the transaction is required. Any delay and/or freezing of the member’s account must be done in accordance with the terms and conditions of the membership and account agreement. *[Note that if the membership and account agreement does not permit the credit union to delay transactions and/or freeze accounts, then any such action may last no more than 10 days, except where there is a court order to the contrary, or except if a report of suspected or detected covered financial exploitation is being investigated by Adult Protective Services or a Law Enforcement Agency. Credit unions may wish to consult with their legal counsel to determine if an amendment to the membership and account agreement should be made to allow the credit union broad authority to delay transactions and freeze accounts.]*
	4. Escalate activity to the BSA Officer to file a Suspicious Activity Report (SAR), using the term “Elder Financial Exploitation” in the narrative.
	5. The Credit Union may also consider the following when working with members who may be potential victims of financial exploitation:
		1. **[Create][Use]** an "Awareness Document" for large cash withdrawals that appear out of the ordinary, have the member read and sign it prior to the receipt of funds. This form **[does][could]** include the following:
			1. Brief overviews of common fraud schemes.
			2. Warnings that perpetrators of such schemes could present themselves as an FBI agent, financial institution examiner or official, police officer, or detective.
			3. Warnings that members should use caution if they are asked for information about their account, asked to withdraw money to help “catch someone,” or to provide money to show “good faith.”
			4. Notice that the Credit Union does not conduct investigations or verification of accounts by telephone or text message.
			5. Notice that local, state, and federal law enforcement authorities, and financial institution regulatory authorities will not conduct investigations by asking individuals to withdraw cash from their account.
			6. Phone numbers for the appropriate agencies with instructions to members that they should contact their credit union branch, local police department, Adult Protective Services, Attorney General, or the Federal Trade Commission for guidance before they withdraw money.
			7. Reminders that swindlers are almost always friendly, have “honest” faces, and that they target older individuals.
			8. A warning that if a member gives money to a person conducting a scam, it may not be possible for anyone, including law enforcement, the credit union, or the member, to get the member’s money back.
			9. The amount the member has requested, with a request to read and sign the document.
4. **LAW ENFORCEMENT LIAISON RESPONSE.** The Law Enforcement Liaison will develop procedures to follow:
	1. When covered financial exploitation of a member is suspected or detected based on available facts.
	2. When, after examination or investigation of available facts, financial exploitation is no longer suspected.
	3. For delaying or placing a freeze on transactions or assets relative to a member’s accounts if financial exploitation is suspected or detected. Such procedures shall provide for the processing of transactions necessary to preserve the health, safety, or financial well-being of the member during periods of delay or account holds, except where such transactions are related to the suspected or detected covered financial exploitation, or where there is a court order to the contrary.
	4. To report the incident to an appropriate Law Enforcement Agency or Adult Protective Services (in accordance with Adult Protective Services’ procedures or law enforcement procedures, in accord with applicable law or regulation).
	5. To properly complete and submit the required form to the appropriate Prosecutor’s Office in the event a response from Law Enforcement or Adult Protective Services does not occur within required timeframes or is insufficient.
5. **LOSS PREVENTION AND SECURITY.** To protect the member and their assets, management will develop procedures to take the following loss prevention and security steps when financial exploitation is detected or suspected:
	1. Take prompt protective action on accounts by placing delays or freezes holds or restraints in accordance with the terms and conditions of the membership agreement. During periods where the Credit Union has implemented a delay or account freeze, the Credit Union may still process transactions necessary to preserve the health, safety, or financial well-being of the member, except where such transactions are related to the suspected or detected covered financial exploitation, or where there is a court order to the contrary.
	2. Follow normal prevention and recovery steps to follow the money as needed.
	3. Make a report to the local Adult Protective Services or Law Enforcement Agency. Reports must contain the name of the victim, a description of the suspected or detected covered financial exploitation, and a designated contact for notices. Provide investigative research and services as needed to Adult Protectives Services or the Law Enforcement Agency.
	4. Continue to monitor the account during legal proceedings, if any, as necessary.
	5. Document file of outcome.

**NOTE: As noted above, per informal regulator suggestions the credit union may wish to reference following procedures for the filing of Suspicious Activity Reports, etc. under federal law or regulation in this section.****Continuing Education**To remain vigilant in protecting credit union members, this Policy and training will continue to be revised. Additionally, the following resources provide information about new and emerging trends:1. Department of Attorney General – Consumer Protection [https://www.michigan.gov/ag/0,4534,7-359-97937---,00.html]
2. AARP.org – Scams and Frauds <https://www.aarp.org/money/scams-fraud/?intcmp=GLBNAV-SL-MON-CONP>
3. FinCEN Advisories - <https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets>
4. Federal Trade Commission – Consumer Information <https://www.consumer.ftc.gov/features/scam-alerts>

**Additional Resources**1. County Prosecutor Electronic Directory [Prosecuting Attorneys Association of Michigan (PAAM) [https://www.michigan.gov/mdhhs/0,5885,7-339-71548\_54783\_54853\_54856-277574--,00.html](https://www.michigan.gov/mdhhs/0%2C5885%2C7-339-71548_54783_54853_54856-277574--%2C00.html)]
2. Adult Protective Services [855-444-3911 [https://www.michigan.gov/mdhhs/0,5885,7-339-73971\_7119---,00.html](https://www.michigan.gov/mdhhs/0%2C5885%2C7-339-73971_7119---%2C00.html)]
3. Attorney General [517-335-7622]
4. Local Law Enforcement Agency [CU regional contact]
 |
|  |

U:\All Department Share\Elder Abuse Task Force\Committees\Law Enforcement\Financial Exploitation Preventation Act Implementation\2021-06-10 Kieran DRAFT Model FEPA Policy DRAFT for TEAM AG w kab commenpts.docx