Family First Credit Union

Protecting the Elderly and Vulnerable from Financial Abuse

Revised June 29, 2017

General Policy Statement:

Credit Unions are in a unique position to detect and prevent financial exploitation and fraud. The primary roles of Family First Credit Union are the protection of its members' assets and the prevention of financial losses. The Credit Union will take steps to protect elderly (over 62 years of age) and vulnerable (generally described as individuals over the age of 18 who lack the physical and mental capability to care for themselves) 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. 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.

Guidelines:

1. **Role of the 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.

3. **Types of Financial Exploitation.** Credit Union staff should be aware of the following types of financial exploitation:

    A. **Theft of Income.** The most common form of financial fraud and exploitation, typically involving less than $1,000 per transaction.

    B. **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:

    A. **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.

    B. **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" falsely claiming an unclaimed inheritance, refund or escheatment. The victim is lured into sending a fee to receive information about how to obtain the alleged 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. Create an "Awareness Document" and 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 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. Complete an Unusual Activity Report and give to the Compliance department who will 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. Complete the Unusual Activity Report and turn in to the Compliance department.

C. File a SAR, using the term "Elder Financial Exploitation" in the narrative

D. Take immediate protective action on accounts by placing holds or restraints and follow normal prevention and recovery steps to follow the money as needed.

E. Make a verbal report to the local Adult Protective Services and provide investigative research and services as needed.

F. Continue to monitor the account during legal proceedings, of necessary.

G. Document files of final outcome.