Fraud Awareness Policy Best Practices

This document includes a template structure for a Fraud Awareness Policy that a credit union may utilize to reinforce their position related to fraud activity, and the controls in place that assist in the identification and restriction of fraudulent activity. The policy can be a helpful tool to both identify and make available to all employees all of the policies and procedures in place that address anti-fraud activities within the credit union. It can also be used as a vehicle for regular review and formal acknowledgment by all staff of their understanding of the policies and procedures, and their agreement to comply with all of the policies and procedures.

I. Purpose

The purpose section should provide a broad and general explanation of the reason why the credit union has and maintains a fraud awareness policy. Implementing a requirement for employees to annually review and sign a standalone Anti-Fraud Policy reinforces the credit union's commitment to ethical conduct, fraud prevention, and accountability. While an employee handbook or general employment policy may address standards of conduct, a dedicated Anti-Fraud Policy places specific emphasis on each employee's responsibility to prevent, detect, and promptly report suspected fraud, theft, misconduct, or other unethical behavior. An annual acknowledgment confirms that employees understand the credit union's fraud prevention expectations, reporting procedures, confidentiality requirements, and the consequences of policy violations. Aligning the Anti-Fraud Policy with the credit union's employment policies promotes consistency, supports a strong culture of integrity, demonstrates management's commitment to internal controls, and provides evidence to auditors, regulators, and examiners that fraud awareness and employee accountability are reinforced on an ongoing basis.

II. Scope

The scope section defines who and what is covered by the policy. It establishes the boundaries of the policy and helps employees, management, and auditors understand when the policy applies and who is responsible for complying with its requirements. A clearly defined scope reduces ambiguity and promotes consistent application throughout the credit union.

When developing the scope of a policy, the credit union should consider including:

- Who is covered by the policy (e.g., directors, committee members, employees, temporary staff, contractors, vendors, and volunteers).
- What activities are covered (e.g., member transactions, lending, electronic services, cash handling, information security, fraud prevention, or vendor management).
- What locations are covered (e.g., branches, administrative offices, remote work environments, shared service centers, and digital platforms).
- What systems, products, or services are covered (e.g., online banking, mobile banking, debit and credit cards, wire transfers, ACH transactions, ATMs, and member account services).
- Any exceptions or exclusions to the policy, including circumstances where other policies, procedures, laws, or regulations take precedence.
- Third-party applicability, if appropriate, includes service providers or business partners performing functions on behalf of the credit union.

A well-written scope should be broad enough to ensure comprehensive coverage while being specific enough to clearly identify the individuals, activities, products, services, and operations subject to the policy's requirements.

III. Policy

The policy section will include the details of the credit union's policy related to fraud awareness and anti-fraud efforts. The policy can include more detail to include dishonest acts, but not limited to, theft, embezzlement, misappropriation of funds or assets, fraud, forgery, falsification or alteration of records or documents, unauthorized transactions, identity theft, check fraud, misuse of credit union property or confidential information, bribery, kickbacks, conflicts of interest, misuse of authority or position, intentional misrepresentation, concealment of material information, and any other act of deception or misconduct intended to obtain an improper benefit or cause financial, operational, legal, or reputational harm to the credit union, its members, employees, or other stakeholders. A list is intended to provide examples and is not all-inclusive. Any act involving dishonesty, deception, unethical conduct, or violation of applicable laws, regulations, or credit union policies may be considered a dishonest act under this policy. It may also make sense to reference the credit unions individual fraud prevention policies and procedures within this section.

- **Member Account Misconduct**

✓ Accessing member accounts without a legitimate business purpose.
✓ Viewing accounts belonging to family members, friends, neighbors, coworkers, public officials, celebrities, or other individuals without authorization.
✓ Changing member phone numbers, email addresses, mailing addresses, passwords, or account settings without proper authorization.
✓ Processing transactions on member accounts without authorization.

- **Cash Theft and Transaction Manipulation**

✓ Stealing cash from teller drawers, vaults, ATMs, ITMs, night depositories, or cash recyclers.
✓ Manipulating transaction records to conceal shortages.
✓ Reversing transactions without proper authority.
✓ Falsifying balancing records or settlement reports.

- **Loan Fraud**

✓ Falsifying loan documentation, income information, collateral values, or underwriting information.
✓ Approving loans outside delegated authority.
✓ Creating fictitious loans or diverting loan proceeds.
✓ Assisting members in providing false information.

- **Wire Transfer, ACH, and Payment Fraud**

✓ Processing transactions without required approvals.
✓ Circumventing dual-control procedures.
✓ Creating unauthorized ACH transactions or wire transfers.

- ✓ Altering payment instructions without authorization.

- **Debit Card, Credit Card, and Digital Banking Fraud**
- ✓ Issuing cards without authorization.
- ✓ Activating cards for unauthorized individuals.
- ✓ Increasing limits or changing controls without proper approval.
- ✓ Assisting individuals in bypassing security procedures.

- **Expense and Payroll Fraud**
- ✓ Falsifying time records.
- ✓ Claiming reimbursement for personal expenses.
- ✓ Submitting duplicate expense reports.
- ✓ Receiving payment for hours not worked.

- **Vendor and Procurement Fraud**
- ✓ Accepting kickbacks, gifts, favors, or personal benefits in exchange for business decisions.
- ✓ Creating fictitious vendors or approving fraudulent invoices.
- ✓ Directing business to vendors for personal gain.

- **Information Security Violations**
- ✓ Sharing passwords, tokens, authentication credentials, or system access.
- ✓ Accessing systems beyond assigned authority.
- ✓ Downloading, copying, transmitting, or removing confidential information without authorization.
- ✓ Destroying, altering, or concealing records related to an investigation.

- **Failure to Report Fraud**
- ✓ Ignoring known or suspected fraud.

- ✓ Assisting another employee in concealing misconduct.
- ✓ Failing to report suspicious activity, control violations, or unethical conduct.

IV. Annual Employee Acknowledgement

The Acknowledgment section explains/defines the process by which employes will be required to review and acknowledge the policy and on what cadence. By having an employee sign and acknowledge a standalone fraud awareness policy, it reinforces that fraud will not be tolerated, below are some items to consider in the employee acknowledgement:

- I acknowledge that I have received, read, and understand the Credit Union's Anti-Fraud & Ethical Conduct Policy.
- I understand that fraud, theft, dishonesty, misuse of member information, misuse of Credit Union assets, or violations of internal controls will not be tolerated.
- I agree to comply with this policy and understand my obligation to report suspected fraud, misconduct, or unethical behavior.

V. Resource

https://ncua.gov/regulation-supervision/regulatory-compliance-resources/fraud-prevention-resources