

Who Commits Fraud and What You Can Do About It

Scam artists and fraudsters have been with us for generations, but they, and their rackets, have become increasingly sophisticated.

Willy Sutton, the accomplished bank robber, was once asked why he robbed banks and he replied: “That’s where the money is.” The same premise applies at your credit union. But it’s not just would-be Willy Suttons you need to be concerned with. Armed robbery, while a risk, is not the only way your credit union can be victimized. It seems like nearly anyone who has the motive, opportunity, and in the case of employees, a sense of justification can get involved with stealing from the credit union, because that is where the money is.

Fraud: Anybody’s (Illgotten) Game

Fraud is an equal opportunity enterprise; there’s a chance for virtually anyone to try to get some of that money for himself or herself. Anyone? Yes. Staff and management have been involved in fraud. Members of their families. Board members. People external to the credit union, such as vendors. With the Internet, the possibilities are endless. Confidence schemes are nothing new. Scam artists and fraudsters have been with us

Case Study: CEO Embezzlement

The CEO of a now-defunct credit union in New England was charged with conspiracy, embezzlement, and tax charges related to shortfalls and missing loan files. At the trial, a former supervisory committee member testified he made a list of missing files during an audit. Among those missing were the CEO’s mortgage and loans under two family members’ names. Other insider loans were incomplete and lacked loan applications and other key paperwork, he said.



for generations, but they, and their rackets, have become increasingly sophisticated. The case studies presented in this chapter show the many variations on a scheme.

Inside Jobs

Let’s start with those who have immediate access: those involved with the internal operations of the credit union. There are seven areas of concern involving internal operations and these will be discussed in detail in this module. From those that are relatively low risk to those that represent a higher exposure to the credit union, the areas are:

1. Cash;
2. Investments;
3. Loans and credit cards;
4. Shares and draft accounts;
5. Dormant accounts;
6. General ledger accounts; and
7. Repossessed collateral.

Outside Sources

External threats to the credit union

Case Study: VP/CFO Embezzlement

A former vice president and chief financial officer of a midwestern credit union was charged with embezzling more than \$339,000 from the credit union. Accused of wiring money from the general account of the credit union to his personal investments accounts to cover stock market losses, he faces two felony charges: embezzlement of more than \$100,000 and embezzlement from a financial institution. If convicted, he could serve 20 years in prison.

can come from nearly any direction, but there are three primary areas of concern: the Internet, forgery and fraudulent deposits, and plastic cards. The Internet, although a powerful tool for all of us, represents a potentially huge source of risk when outsiders access members' accounts or other internal records. Members also are vulnerable to pharming and phishing scams, in which crooks try to capture personal information by sending an e-mail—called **phishing**—or by **pharming**—getting the victim to go to a look-alike Web site, where they gather account numbers and passwords, and then have access to accounts.

Vishing attacks are also on the rise. These scams use telephone systems to get personal information. Because **Voice over Internet Protocol (VoIP)** technology allows for caller identification **spoofing** (trickery that makes a message appear as if it came from an

authorized or legitimate source), vishing can fool even wary consumers into divulging Social Security numbers, passwords, credit card or personal identification numbers.

Forgery and fraudulent deposits are other external sources of fraud. These may involve new members attempting to defraud the credit union or in some scams, thieves who are trying to bilk vulnerable members.

The third area of concern is plastic cards, and this is a growing problem. CUMIS reports losses are up sharply from just a couple of years ago. We will discuss each of these potential sources of fraud in detail in later chapters.

Your Defensive Weapons: Internal Controls

NCUA's Regulation 715—the rules that cover supervisory committees—requires you to ensure that internal controls exist and that they are working as planned.

According to NCUA's Supervisory Committee Guide, internal controls include the staff structure, operating procedures, and other measures within the credit union to:

- Safeguard assets;
- Check the accuracy and reliability of accounting data;
- Promote efficiency; and
- Encourage compliance with board policies.

Simply put, internal controls are a system of checks and balances that can help prevent error or fraud, or identify error or fraud quickly after it occurs.

The NCUA's guide recommends that an internal control structure include

Case Study: Cell Phone Text Scam

Members of a southern credit union were targeted by a cell phone text message scam. Text messages appearing to come from the credit union requested credit, debit, and ATM card information, including the card number, personal identification number, and other personal information. Conveying a sense of urgency, the messages attempted to trick members into disclosing the information by saying that their bill paying service had expired.

Case Study: Sophisticated Scammers Tap HELOCs

Credit unions in the Pacific Northwest and elsewhere were the victims of a sophisticated fraud that involved telephone, fax, or e-mail requests made to the credit union for large-dollar advances on home equity lines of credit. The fraudsters, who had extensive personal information about the members and found ways to circumvent the credit unions' call back verification procedures, requested the money be wire transferred, often to a foreign country.

three elements: the control environment, the accounting system, and the control procedures.

According to the guide, the control environment takes into consideration:

- Management policies and plan;
- Organizational structure;
- Involvement of officials (board and committee);
- Assignment of authority and responsibility;
- Personnel policies; and
- Examinations.

The accounting system's considerations include:

- Quality of the books and record-keeping system;
- Maintenance of accounting

records;

- Financial reporting system; and
- Preparation of accurate financial statements.

The control procedures take into consideration:

- Appropriate transaction authorization;
- Sound segregation of duties;
- Safeguarding of credit union assets—particularly cash, investments, and fixed assets;
- Security access level and controls over the data processing system; and
- Management or supervisory committee periodic reviews and test checks.

Typically, error creates more losses in credit unions than fraud does.

Frauds tend to be relatively small and identified quickly. But error should be a concern because error can result in the biggest write-offs, charge-offs, and losses.

You need to ensure there is a system of controls in place that prevents both

Figure 1.1

Warning Signs

NCUA cites the following as examples of some factors that can contribute to losses:

- One or two people do the work due to limited staff size
- Lack of board-approved policies for lending, investments, borrowing, and operating expenses
- Lack of segregation of duties (no dual controls for key areas such as cash, loans, investments, and shares)
- Lack of mandatory vacation policy that applies for all employees
- Failure to maintain adequate audit trails
- Recordkeeping problems (accounting and financial statements are behind, not reconciled, or materially out-of-balance)
- High level of operating expenses
- Poor loan quality

There are different levels of risk, and as a volunteer, you have a limited amount of time.

errors and fraud, or at the very least, catches them quickly.

A good system of internal controls provides the best protection against both error and fraud. That doesn't mean you, as a member of the supervisory committee, are actually implementing the internal controls. That can be accomplished by an internal auditor or your external auditor. Or it can be a combination of the two.

As a supervisory committee member, it is your job to make sure that somebody is doing it and to make sure it is being done correctly.

There are different levels of risk, and as a volunteer, you have a limited amount of time. So it makes sense that you'll want to spend your time where you have the greatest impact and on the areas of highest risk.



In the next chapters, we examine each of the potential sources of fraud in detail, along with the internal controls that can mitigate losses.