

Expert Opinion

Halting Occupational Fraud

Unfortunately, credit unions remain an accessible and desirable target for internal fraud perpetrators.

By Shannon Walker | July 24, 2023 at 04:24 PM











Trending Stories

- 1 **CUNA and NAFCU Planning to Merge Next Year**
- 2 **League CEOs React to Historic CUNA-NAFCU Merger News**
- 3 **PCCU Takes Another Hit From Former Cannabis CUSO**
- 4 **Earnings Fall for Top 10 Credit Unions in Q2**
- 5 **Man Who Used a Can to Allegedly Rob a CU Ends Up in the Can ... Twice**

Occupational fraud is the most common and costly type of fraud, resulting in billions of revenue dollars lost each year. Unfortunately, credit unions remain an accessible and desirable target for many occupational fraudsters. At the beginning of 2023, the NCUA reported that the risk of fraud within credit unions remains elevated. In fact, in the last quarter of 2022, financial institutions experienced a 53% increase in fraudulent activity, and credit unions experienced a 70% increase in total fraud activity for the year, according to a Pindrop study. The most common type of occupational fraud is asset misappropriation at the executive level, but organizations can be targeted by an employee at any level.

To help mitigate and discourage fraud attempts, credit unions must understand how they are vulnerable to attacks and what measures they can take to prevent occupational fraud. When occupational fraud does occur, leadership must hold those responsible accountable and apply a transparent approach to stakeholder relations to ensure their reputation remains intact.

Understanding Different Types of Frauds

Asset misappropriation: Occupational fraud generally refers to fraudulent actions carried out by a person against their employer, usually for financial gain. These actions frequently involve the individual abusing their position and authority inside the company to their own advantage and to the detriment of their employer. Asset misappropriation is the first and

most common type of fraud, which entails misappropriating or stealing an organization's resources. Examples include:

- Pocketing cash;
- Inflating expenses;
- Stealing merchandise or tangible property; and
- Abusing corporate resources for one's own benefit.

Corruption: This is another common type of occupational fraud that utilizes decision-making powers to divert gains to themselves or the company. Employees may target outside sources to help their corrupt tactics. For example, bribery and product substitution are common methods for reverting profits back into their own pockets. Here, it is common for employees in client and supplier-facing positions to commit fraud.

Financial statement fraud: This is the third category that falls under the umbrella of occupational fraud. Usually, this type of fraud will be committed by someone in a position of power privileged to the financial statements and documents of the organization. In these cases, the employee may alter a balance sheet or cash flow statement, effectively falsifying the financial statements so the resulting documents appear in their favor. While these cases are uncommon, they have historically been used to make companies appear more attractive to investors or by individuals looking to justify a raise from their boss.

Asset misappropriation, corruption and financial statement fraud are all somewhat intertwined. Often various instances of corruption may fall under one of the other two categories and vice versa. Discerning and understanding the different types of occupational fraud will help your organization be better suited to deal with cases that arise and implement prevention measures to protect the company.

Preventative Measures for Mitigation of Occupational Fraud

Preventative measures are crucial for the mitigation of occupational fraud in any organization. Preventing fraud must start the second employees walk through the door. Thorough background checks implemented in the hiring process can help screen potential employees for any past illegal behavior. Thus, a crucial prevention measure is eliminating at-risk prospects before they are onboarded and privy to information that can be used against the organization.

Next, it is vital to have strong internal controls to squash the plans of any prospective fraudster. A lack of internal controls is common in credit unions, especially in smaller organizations that have developed a family-like operation that may suffer from overtrust of good character. Having processes and policies to control access to sensitive information that could be used illicitly will be crucial for preventing all types of occupational fraud. This involves limiting access only to those who need it for their job functions and monitoring this access closely. Physical and software-based security will be crucial for this. For

example, advancements in biometric technology can provide advanced security measures for traditionally password-protected documents.

Additionally, financial documents should be carefully audited and never edited by those who may be incentivized to commit financial statement fraud. Alongside these internal controls, regular internal and external auditing should be conducted to detect any suspicious activities.

Importance of Fraud Reporting Tools for Credit Unions

When it comes to reporting illicit activity that happens within the credit union, your employees are often your eyes and ears. More often than not, employees will witness or suspect a fraudster before senior management catches wind. However, they may be silenced or fear retaliation for what they witness. It is essential to implement anonymous reporting mechanisms so that your employees remain committed to maintaining ethical standards and can speak up about any wrongdoing they witness. Most commonly, organizations will use either a hotline or intake form that can be audited internally or externally and ensure concerns are brought to the attention of senior management in a timely manner.

With any reporting mechanism, a comprehensive anti-retaliation policy is essential to protect those who speak up against potential fraud, ensuring they will not face backlash. With this, all employees should be trained to ensure compliance with these policies and reinforce the importance of ethical conduct within the organization. When implemented and enforced, such measures can significantly reduce the incidence and impact of occupational fraud.

Dealing With Cases of Occupational Fraud

Dealing with occupational fraud at credit unions necessitates a thorough strategy that includes alerting all relevant parties, limiting access to information during investigations, being open with staff, appreciating those who come forward and holding those who violate rules publicly accountable to set an example. When necessary, executives and senior management, regulatory authorities and human resources personnel must all be involved to assess the circumstances properly.

What to Expect During the Investigation Process

During investigations, it is vital to limit access to sensitive information to maintain the integrity of the process. This includes restricting access to relevant documentation, financial records and electronic systems to prevent tampering with evidence and safeguard the investigation's integrity.

Credit unions must also prioritize transparency with their employees and members when necessary. If the investigation warrants external press, you want to jump at the opportunity to ease members' minds and protect your organization's brand. Sharing information about the ongoing investigation, its progress and any necessary actions being taken demonstrates the organization's commitment to addressing the issue. Open communication helps foster trust and assures employees that appropriate measures are being implemented to prevent similar incidents in the future.

If another employee helped uncover the fraud, expressing gratitude for their actions is crucial. By acknowledging and appreciating their bravery in speaking up, your organization

will be an environment that encourages the reporting of wrongdoing. Even if their identity is kept anonymous, showing appreciation for whistleblowers encourages others to follow suit, thereby helping to identify and prevent fraudulent activities.

Finally, it is imperative to hold individuals accountable for breaking policies related to occupational fraud. No matter how senior the individual is, no one can be protected from the law. By taking firm action and terminating the employment of wrongdoers, credit unions not only deter potential fraudsters but also safeguard their organization's reputation and maintain the trust of their members.

Best Practices Moving Forward

Occupational fraud remains a significant threat to credit unions everywhere and has historically resulted in both huge financial losses and reputational damage. To mitigate this risk, credit unions must understand the different types of occupational fraud and implement preventive measures including, but not limited to, background checks, strong internal controls, regular auditing and anti-fraud policies.

The next step is creating a transparent, ethical culture that promotes anti-fraud rhetoric. Anonymous reporting mechanisms and anti-retaliation policies will help to empower employees to report suspicions. Open communication with stakeholders and credit union members during investigations helps foster trust and demonstrates a commitment to addressing fraud. Holding individuals accountable, regardless of their position, will deter future potential fraudsters and protect the organization's reputation.

The next step is creating a transparent, ethical culture that promotes anti-fraud rhetoric. Anonymous reporting mechanisms and anti-retaliation policies will help to empower employees to report suspicions. Open communication with stakeholders and credit union members during investigations helps foster trust and demonstrates a commitment to addressing fraud. Holding individuals accountable, regardless of their position, will deter future potential fraudsters and protect the organization's reputation.



Shannon Walker Founder and President [**WhistleBlower Security Inc.**](#)
West Vancouver, British Columbia, Canada

NOT FOR REPRINT

© 2023 ALM Global, LLC, All Rights Reserved. Request academic re-use from www.copyright.com. All other uses, submit a request to asset-and-logo-licensing@alm.com. For more information visit [Asset & Logo Licensing](#).

Shannon Walker
