



LOWERING THE HIGH COST of Internal FRAUD

How policies, culture and training work together to improve fraud detection and prevention

By Jennifer Roland Cadiente



It's a continual problem, but one that many of us don't like to think about: internal fraud. Why do we avoid it? Sometimes we don't want to admit that we made a hiring mistake or that our policies didn't protect us. But employee fraud happens, and the results can seriously hurt the credit union.

A 2014 report from the Association of Certified Fraud Examiners (ACFE) showed that financial institutions had the highest rate of internal

fraud among the industries they analyzed — 17.8 percent of the total cases reported. According to a review of the data by Ray Birch for CUToday.info, there have been fluctuations in the annual number of internal fraud cases and the dollar amounts involved, but overall, it has remained relatively steady since this ACFE study.

One particularly concerning piece of information, though, is the number of times internal fraud has caused credit unions to fail. For example, Birch pointed out that in 2015, employee fraud was a key contributor to 69 percent of credit union failures.

So how do we work to prevent internal fraud and mitigate losses to the credit union? A combination of policy strategies, cultural changes and training.

The Costs of Internal Fraud Go Beyond Cash

The ACFE study found the median reported dollar cost of internal fraud in financial institutions to be \$200,000, and these losses are likely to be covered by insurance. But hard dollar costs are only part of the picture.

Sabrina Waner, senior vice president and chief financial officer at Allegiance Credit Union in Oklahoma City, points out the burden on staff time that gathering information and evidence of internal fraud can have, especially for small credit unions. There were two cases of internal fraud while she was working at a previous credit union. Because they were small — the staff numbered between seven and 14 when the two fraud cases happened — and she was a vice president who was responsible for the accounting functions, much of the burden of documentation fell on her shoulders. “We weren’t big enough to hire an auditor or an audit firm to come in and pull all that information,” she says. “I spent a year of my life making sure we had documentation of every transaction, every piece of paper and every policy, then going through the trial and testifying in court.”

Ryan Ross, senior vice president and chief risk officer at Pen Air Federal Credit Union in Pensacola, Fla., had a similar experience with one fraud case in which a staff member was skimming off the top of cash shipments. In this case, it took a year and a half of working with the local district attorney and the FBI to get the case to court. “The time I put in just myself, pulling video footage and working with the FBI to see where she was in the branch and see if we could catch her doing it, [was substantial],” he says.

Additionally, credit unions may suffer reputational loss. “When you start reporting things to law enforcement and regulators, that becomes public record,” says Jon Crawford, security manager at Apple Federal Credit Union in Fairfax, Va. And in cases involving large sums of money or senior staff, local media can find a



refreshing take to an interesting story whenever there is a new development in that long investigation timeline. This can be an ongoing issue, repelling new members until the story blows over. To combat this potential risk, give your credit union spokesperson information they can discuss with media that underscores how the credit union’s policies, procedures and internal auditing helped them find this internal fraud. It also helps to highlight relationships with law enforcement to protect member assets and prosecute anyone who commits fraud. Prosecution of employees who commit fraud, says Crawford, “sends a message that fraud will not be tolerated and

the assets of the members of Apple Federal Credit Union will be protected at all costs.”

Strong Policies Are Critical

Internal auditing and policies and procedures help prevent and uncover internal fraud.

Two of the most important, according to Michael J. Carroll, assistant vice president of internal audit at Apple Federal Credit Union, are dual control and segregation of duties. “As long as you’re segregating duties properly, it’s going to make it very difficult for one employee to complete a fraudulent transaction from beginning to end.”



“We count cash at the end of shifts and do surprise cash counts.”

— SABRINA WANER, SENIOR VICE PRESIDENT AND CHIEF FINANCIAL OFFICER, ALLEGIANCE CREDIT UNION



“We tell our employees, ‘If you see anything that is against Pen Air’s policies and procedures, inform us. We will safeguard your identity.’”

— RYAN ROSS, SENIOR VICE PRESIDENT AND CHIEF RISK OFFICER, PEN AIR FEDERAL CREDIT UNION

Also important are tiered approval limits on specific types of transactions, says Ross.

Carroll also suggests credit unions of all sizes outsource some of their auditing functions and a review of policies — “having a fresh set of eyes look at your controls is extremely important.”

Waner points to the importance of internal audits, especially in preventing fraud at the teller level. “We count cash at the end of shifts and do surprise cash counts,” she says, “and we really don’t have any employee losses.” She also notes that they often find issues when employees are taking their required 40 hours off or when they’re rotating in new employees.

“Someone will say, ‘This just doesn’t look right,’” she says, and that gives the credit union the opportunity to investigate and see whether there is any fraudulent activity.

Technology tools can help prevent fraud. For example, Ross says Pen Air recently launched RSA keys, a secure ID to log in to computers. “It’s a key fob that’s based on you, and the numbers change every 60 seconds. There’s never a password to log on. That keeps others from being able to guess your password and get into your computer.” Of course, this works only when employees log off their workstations when leaving, so it is important to emphasize this procedure. Waner mentions a specific case in which an employee used another employee’s workstation and teller

number to cash fraudulent checks, and it took about a month to get the proof they needed of that activity.

Ross also points out that cash isn’t the only area to monitor. Mileage logs and credit charges are given extra scrutiny by supervisors at Pen Air. Additionally, call center calls are recorded, file maintenance records track account changes, and all new memberships and accounts go through quality assurance reviews.

Culture Is Key to Catching and Preventing Fraud

Giving employees the opportunity to speak up when they see something unethical is a key component of a fraud-preventing culture.

Pen Air Federal Credit Union includes a whistleblower procedure in the employee handbook. Says Ross, “We tell our employees, ‘If you see anything that is against Pen Air’s policies and procedures, inform us. We will safeguard your identity.’” They also ask employees to sign a commitment card to show that they are living the credit union’s culture of honesty and integrity.

Employee onboarding is an important moment for setting culture. Waner says all new employees at her credit union meet every member of senior leadership during their orientation. “From the get-go, employees visit with the vice presidents and the president, and they get to know who we all are,” she says. “And I talk about fraud and let them know that our culture is open and we depend on them to alert us — if there is something suspicious, you need to tell someone.” That openness has paid off. Waner says Allegiance employees report suspicious activity directly to human resources, rather than the ethics hotline they’ve set up.

At Apple Federal Credit Union, open access to leadership continues after new employee orientation with branch visits from the CEO and the head of human resources (its “chief people officer”) and town hall meetings at which the credit union comes together to hear from senior management. Additionally, they provide





AI OASIS

Don't waste time and resources with
obsolete behavior-based and rule-based tools.

Join the United AI Network™ today!

The United AI Network™ empowers numerous financial institutions worldwide to instantly eliminate all types of risks, losses, and damages. The United AI Network™ uses the following patented AI-powered Officers to protect financial institutions:

- PATRIOT OFFICER® - the #1 BSA/AML/U.S. PATRIOT Act solution
- GUARDIAN OFFICER® - the #1 Fraud Prevention solution
- CHAMPION OFFICER® - the #1 Consumer Protection solution
- ENQUIRER OFFICER® - the #1 Financial Crimes Elimination solution

