GENESIS BANK
INSTITUTE FOR ENTREPRENEURSHIP

ACCOUNTS RECEIVABLE FRAUD: RISKS, RED FLAGS, AND BEST PRACTICES

Many experts say at least two people should always be involved in every key transaction.

Fake sales may be used to cover up stolen or misdirected merchandise.

Accounts Receivable Fraud: Risks, Red Flags, and Best Practices

Every year, businesses across the U.S. lose tens of billions of dollars to employee fraud – and accounts receivable departments are a frequent target.

Unfortunately, the risk of accounts receivable fraud – or "accounts deceivable" – is especially high for small and midsized businesses, which may handle large volumes of delayed payments but lack the resources and personnel to establish robust internal checks and balances.

In this article, we'll look at four common forms of accounts receivable fraud, some warning signs to look out for, and best practices you can implement to protect your company.

Lapping

This method involves diverting customer payments to cover up the theft of previous payments. As the name suggests, this is an ongoing scheme, with Customer B's payment covering Customer A's payment, then Customer C's covering Customer B's, and so on. This can continue

for a prolonged period of time before it's detected – usually by a steady rise in the aging of accounts – or until the loss is finally concealed by falsifying the books another way.

Example: George, an unethical employee at Hopeland Trinkets, Inc., receives a check from a regular customer, Lucille, in the amount of $800. George deposits it in a bank account he's opened for himself under the deceptive name of "Hopeland Treasures." When the next customer payment of $800 comes in, George will credit it to Lucille's account.

Skimming
This is when an employee pockets a cash payment, deposits a check into their own account or otherwise misappropriates inbound funds, and then either leaves the books unbalanced or manipulates them to conceal the theft. This can be accomplished by crediting a customer account and debiting an expense account that's written off annually. A sophisticated swindler might spread the phony debits across multiple accounts so that the transaction is harder to piece together.

Example: George pockets Lucille's check, as above. He credits Lucille's account for $800 and then charges $400 to "advertising" and $400 to "consulting fees."

Fictitious Sales
There are a few different reasons that a dishonorable employee might record nonexistent sales. Individuals who receive commission-based income may pad sales figures to increase their paycheck. Noncommissioned employees may play a longer game, falsifying sales data to make their activities look more profitable so they can angle for a bonus or raise down the road. Alternatively, fake sales may be used to cover up stolen or misdirected merchandise.

Example: George records the sale to Lucille as totaling $1,600 instead of $800. He gets a 2% commission on every sale made, so he's just doubled his earnings even though the company's revenue remains unchanged.

Fraudulent Write-Offs
This can be its own form of accounts receivable fraud, or it can serve as a means to disguise a lapping or skimming scheme. It occurs when an employee falsifies or takes advantage of a customer return, discount, or bad debt. They might enter a write-off on a customer account and then pocket the amount, or they might credit a write-off to an inactive account and then direct the funds to another account they've been stealing from.

Example: George properly deposits and records Lucille's $800 payment. But then he issues a phony 50% refund for "trinkets broken in transit," making a $400 check out to himself.

Red Flags

Accounts receivable fraud isn't always easy to spot, but here are some anomalies to watch for:

- Increased revenues compared to sales, total assets, or shipping costs
- Sudden new activity in a long-dormant bank account
- An excessive number of voids, discounts, returns, or other modifications
- Discrepancies between bank deposits and postings
- Increased expense items or employee reimbursements
- Complaints from customers receiving incorrect nonpayment notices
- An employee with a sudden unwillingness to share job tasks or take time off
- An employee with a much higher-than-expected standard of living

Best Practices

Accounts receivable schemes don't just cause short-term financial loss. They can hurt customers, damage a business's reputation, and lead to severe civil and criminal penalties for those involved. Fortunately, business owners can boost transparency and accountability to avoid employee fraud or catch it before it escalates.

- **Separate accounting functions** among multiple employees. Many experts say at least two people should always be involved in every key transaction. But even small, affordable interventions – like occasionally switching up who opens the mail and who deposits checks – can deter misconduct.
- **Mark all checks *For Deposit Only*** with a stamp, have cash customers pay directly into a lockbox, reconcile cash receipts on a regular basis, issue monthly account statements to customers, and implement other safeguards that make it harder for employees to intercept money or falsify records.
- **Educate employees** about the risks of accounts receivable fraud, how to recognize its warning signs, and how to report it within your organization. Consider setting up a detailed whistleblower procedure so employees can raise the alarm anonymously to a trusted manager, who is not associated with the suspected perpetrator (if possible), without fear of retaliation.

A Financial Partner You Can Trust

Reach out to your financial institution for more tips on safeguarding your money and data.

DISCLAIMER: These training materials are intended as general guidance only and may or may not apply to a particular situation based on the circumstances. The materials do not create any legal rights or impose any legally binding requirements or obligations on Genesis Bank or the Genesis Bank Institute for Entrepreneurship. Genesis Bank and the Genesis Bank Institute for Entrepreneurship make no claims or guarantees regarding the accuracy or timeliness of this information. The content of this training material is not designed or intended to provide authoritative financial, accounting, investment, legal, or other professional advice that may be reasonably relied on by its readers. If expert assistance in any of these areas is required, readers should seek the services of a qualified professional. Reference to any specific organization, commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute an endorsement, recommendation, or preference by Genesis Bank or the Genesis Bank Institute for Entrepreneurship. Copyright © 2022 Genesis Bank. The Genesis Tree Logo is a trademark of Genesis Bank. All rights reserved.

Member FDIC

Interested in more?
Visit **mygenesisbank.com/GBIE**

For more information on how you can get involved with the Institute, please reach out to **Dani Feigin** • Head of Brand Partnerships
E dfeigin@mygenesisbank.com **P** 949.273.1497
A 4675 MacArthur Court, Suite 1600 Newport Beach, CA 92660