IOFM Institute of Finance & Management

AR Fraud Mitigation Guide

Debra R. Richardson, *Master Data Fraud Expert*

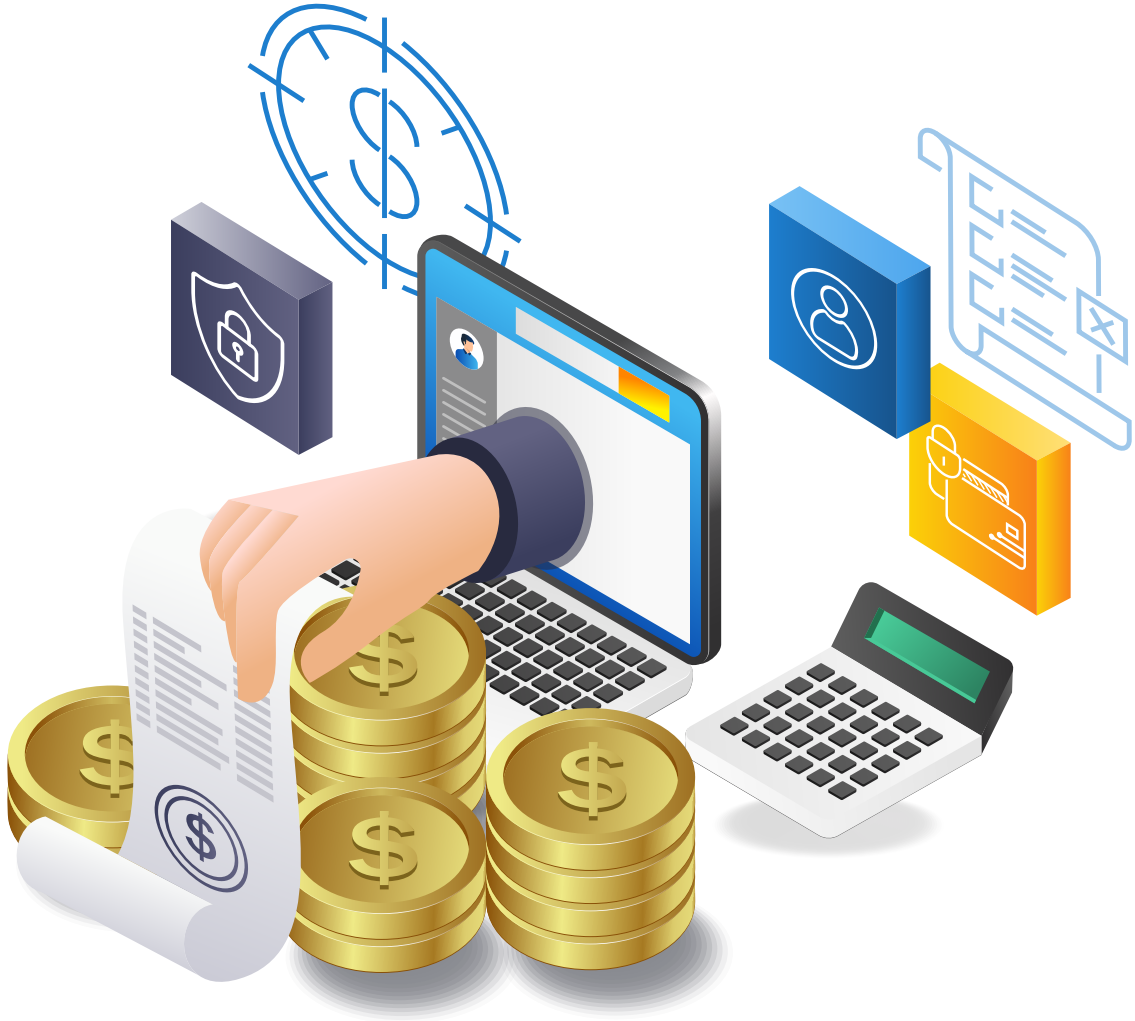

TABLE OF CONTENTS

© 2024 IOFM, Diversified Communications. No part of this publication may be reproduced, stored in a retrieval system or transmitted by any means, electronic or mechanical, without prior written permission of the Institute of Finance & Management.

Accounts receivable fraud is a significant concern for organizations. According to the Association of Certified Fraud Examiners' (ACFE) 2024 Report to the Nations, AR fraud can result in substantial financial damage and requires the need for vigilance and proactive measures.

One shocking revelation from the report is that a considerable percentage of occupational fraud cases (89%) involved asset misappropriation schemes, underscoring the vulnerability of this area within financial operations. Fraudsters are increasingly using sophisticated methods to exploit weaknesses in AR processes.

TYPES OF ACCOUNTS RECEIVABLE FRAUD

False Invoicing

One of the most common forms of AR fraud is false invoicing. This billing scheme occurs when an employee or an external party creates fake invoices, usually under a shell company that has no physical presence but has a mailing address or bank account to accept the payment. While this fraud works better when billing for services since there is no expectation of receipt of product, these invoices may be for goods or services that were never delivered or for inflated amounts.

- **Red Flag:** Invoice company is a shell company
- **Red Flag:** Shell company mailing address is a post office box
- **Red Flag:** Shell company address matches an employee's address

Fictitious Sales

Fictitious sales involve employees reporting non-existent transactions to inflate their commissions or conceal stolen goods. It undermines financial integrity and can severely impact a company's financial statements and operational accuracy.

- **Red Flag:** Mismatches between revenues and actual sales, total assets, or shipping expenses
- **Red Flag:** Increase in long overdue customer accounts

Skimming

Skimming is the theft of cash before it is recorded in the company's accounting system. This type of fraud typically occurs at the point of sale, during cash handling processes or when receiving customer checks to record against their account. It is challenging to detect since the stolen funds are typically never entered into the books. If entered, they are concealed by using a dormant customer account and debiting an expense account that is written off annually.

- **Red Flag:** Discrepancy between the funds deposited in the bank to the amounts recorded
- **Red Flag:** Increase in expense items when compared to forecasted or budgeted amounts
- **Red Flag:** Sudden and unexpected transactional activity in long-dormant bank accounts
- **Red Flag:** High volume of voided transactions, discounts, returns, or other adjustments
- **Red Flag:** Increase in inventory shrinkage ratio following a physical inventory count

© 2024 IOFM, Diversified Communications. No part of this publication may be reproduced, stored in a retrieval system or transmitted by any means, electronic or mechanical, without prior written permission of the Institute of Finance & Management.

Short-Term Skimming - One variation of skimming where employees keep the funds long enough to earn interest from an interest-bearing account or security. They then return the funds, apply it to the customer's account but keep the interest.

Lapping

Lapping is a common method to conceal skimming. It involves the misapplication of customer payments to cover for stolen funds. For example, an employee may divert a payment from one customer for personal use and then use subsequent payments from other customers to cover up the fraud. This creates a cycle of misappropriation that can be difficult to unravel.

- **Red Flag:** Customers complain about receiving notices of non-payment when payment has been sent and recorded in the customer's system
- **Red Flag:** An increase in the accounts receivable turnover ratio indicating customers are paying later than before

Improper Write-Offs

Fraudulent write-offs occur when accounts receivable balances are improperly reduced. An employee might classify a genuine receivable as a bad debt and then personally collect the payment from the customer. This fraud is often overlooked because of its discreet nature.

- **Red Flag:** Write-offs of accounts receivable accounts
- **Red Flag:** Write-offs of lost, stolen, or obsolete inventory
- **Red Flag:** Sudden and unexpected transactional activity in long-dormant bank accounts

FRAUD DETECTION STRATEGIES

The goal of fraud detection strategies is not only to uncover ongoing fraudulent actions but also to deter such activities from occurring in the first place. This involves a comprehensive approach that integrates financial oversight, behavioral analysis, and technological tools to safeguard the integrity of the organization.

Behavioral Red Flags

Employees who embezzle often show behavioral red flags such as sudden wealth, protectiveness over their work, stress, or unusual vendor/customer interactions. They may also refuse to delegate tasks and become defensive when questioned about discrepancies. Vigilance towards these signs, like a noticeable lifestyle change or reluctance to explain financial issues, can help in early fraud detection and prevention within the company.

© 2024 IOFM, Diversified Communications. No part of this publication may be reproduced, stored in a retrieval system or transmitted by any means, electronic or mechanical, without prior written permission of the Institute of Finance & Management.

Regular Reconciliations

Regular reconciliation of AR records with bank statements and customer accounts can help identify discrepancies that may indicate fraud. Any unexplained differences should be investigated promptly.

What to look for:

- Bank Statement Reconciliation
    - Discrepancies between bank deposits and postings
    - Alterations to original bank statement
    - View check images to verify correct payee name and endorsement
- Customer Account Reconciliation
    - Mismatch between customer statement and customer account balance
    - Unexpected write-off or adjustment of customer balance
    - Sudden new activity in long-dormant accounts
- General Ledger Account Reconciliation
    - Increase in expense line item compared to forecast or budget
    - Increase in cost of goods sold and decreases in gross sales
    - Excessive void, discounts, and return transactions

Tip: Periodically have an independent party, like an internal auditor or another department, review the reconciliations. This extra oversight can help spot irregularities or fraud that the accounts receivable team might miss.

Audit Trails

Audit tables track change and deletions of information at the database level, including who performed the transaction, when it occurred, and any changes made. They should also include before and after values. This detailed record-keeping enables organizations to identify anomalies and potentially fraudulent activities, ensuring accountability and enhancing the integrity of financial records.

Tip: Review your audit tables and ensure that key fields are captured on the audit table. This may be overlooked as new fields are added due to automation tools integrated with the system.

Surprise Fraud Audits

Surprise fraud audits of business functions in which fraud is most likely to occur can be effective in both detecting fraud that has already occurred and deterring future fraud. Conducting surprise audits can be an effective way to detect accounts receivable fraud. These audits should be performed by an independent party and should focus on high-risk areas.

Tip: Include in the fraud policy that random tests will be performed to verify that internal controls are not bypassed.

© 2024 IOFM, Diversified Communications. No part of this publication may be reproduced, stored in a retrieval system or transmitted by any means, electronic or mechanical, without prior written permission of the Institute of Finance & Management.

FRAUD PREVENTION STRATEGIES

Fraud prevention strategies encompass practices such as independent audits, detailed audit trails, surprise fraud audits, and the segregation of duties. These measures enhance oversight, ensure accountability, and reduce the likelihood of fraud by dividing responsibilities and maintaining rigorous checks on financial transactions and records.

Segregation of Duties

Segregation of duties prevents accounts receivable fraud by dividing responsibilities among different employees. This ensures that no single person has control over all aspects of a transaction, reducing the risk of unauthorized actions.

Tip: Restrict employee access to all customer accounts, files, and folders to prevent unauthorized changes.

Task	Description	Purpose
Recording and Collection	The employee responsible for recording AR transactions should not be the same employee who collects payments from customers.	Prevent concealment of unauthorized transactions
Authorization and Reconciliation	The employee who authorizes credit sales should not be the one reconciling the accounts receivable ledger.	Detect discrepancies or unauthorized credit sales
Invoice Generation and Payment Processing	The employee who generates and sends invoices to customers should not handle the receipt and processing of payments.	Reduce risk of fraudulent adjustments
Bank Deposits and Account Reconciliation	The employee who deposits customer payments into the bank should not be responsible for reconciling the bank statements.	Ensure accurate recording and accounting of deposits
Customer Account Adjustments and Approval	Any adjustments to customer accounts, such as write-offs or credits, should require approval from a different individual than the one making the adjustments.	Prevent unauthorized changes

Staff Regulations

Implementing strict staff regulations can significantly reduce AR fraud. Clear policies can ensure transparency and accountability. These measures help prevent fraudulent activities, safeguarding the company's financial health.

- **Training** – Training employees on the importance of ethical behavior and the consequences of fraud can help prevent misconduct. Employees should be encouraged to report any suspicious activity and should be aware of the company's whistleblower policy.
- **Background Checks** – Conducting thorough background checks on employees who have access to financial information can help prevent fraud. This includes checking for any previous criminal activity or financial misconduct.
- **Employee Rotation** – Rotating employees' duties periodically within the AR department to enable backfilling of roles.

© 2024 IOFM, Diversified Communications. No part of this publication may be reproduced, stored in a retrieval system or transmitted by any means, electronic or mechanical, without prior written permission of the Institute of Finance & Management.

- **Mandatory Vacations** – Requireing employees take enough time off each year that allows each of their assigned activities to be performed by another team member.
- **Use of Lockboxes** – Implementing lockbox services for customer payments to ensure direct bank deposits.

Tip: Assign at least one or more employees to be trained for every task performed by another employee. This will ensure that each task can be completed by another employee during mandatory vacations.

Use of Technology

Leveraging technology to prevent accounts receivable fraud involves implementing data analytics to detect anomalies, automating reconciliations for accuracy, and employing secure access controls to restrict unauthorized access. Additionally, real-time monitoring and reporting tools can quickly identify suspicious activities, enhancing overall fraud prevention efforts.

- **Matches of employee remittance details to vendor remittance details** – Verify the employee address and bank account number is not the same as a vendor in the vendor master file.
- **Discrepancies between bank deposits and postings** – An indication that the amounts recorded in the AR ledger do not match the actual deposits made into the bank, which could be a sign of fraud.
- **Excessive number of voids, discounts, or returns** – An unusually high number of these transactions can suggest manipulation or fraudulent activities, such as employees voiding sales to steal cash or offering unauthorized discounts.
- **Sudden new activity in long-dormant accounts** – If an account that has been inactive for a long period suddenly shows significant activity, it could be a red flag for fraudulent transactions or errors.

Tip: The Federal Reserve's E-remittance Exchange Pilot is an electronic delivery network that will enable all kinds of businesses to exchange electronic remittance information, or details that describe what is being paid. This will allow for straight through processing without manual intervention, reducing the potential for fraudulent activity with customer accounts.

Bank Security Services

Most banks offer multiple security services that can help prevent fraud. These services verify the legitimacy of payments and authenticate users accessing systems, ensuring that only authorized individuals can conduct transactions and safeguarding against financial misconduct.

- **Positive pay for electronic and check payments** – Banks will match the details of the presented payments to those on a list of legitimate and expected payments.
- **Multifactor authentication tools** – These mechanisms combine two or more methods to validate the identify of the person attempting to access the system.

© 2024 IOFM, Diversified Communications. No part of this publication may be reproduced, stored in a retrieval system or transmitted by any means, electronic or mechanical, without prior written permission of the Institute of Finance & Management.

Employee Hotline

Implementing an employee hotline for tips on internal fraud is a crucial step in fortifying an organization's defenses against financial misconduct. This anonymous reporting system empowers employees to voice concerns without fear of retaliation, thereby promoting a culture of transparency and accountability. The hotline should be accessible 24/7, managed by a third-party service to ensure confidentiality, and integrated with the company's whistleblower policy. Regularly communicating the existence and importance of the hotline to employees can increase its effectiveness, encouraging vigilance and fostering an environment where ethical behavior is the norm.

According to the ACFE 2024 Report to the Nations, 43% of internal fraud cases were discovered based on a tip from a whistleblower. Hotlines are the most common way frauds are detected.

Tip: Create multiple formats for employees to anonymously report suspected fraud. Suggested options include an online entry form or telephone number.

Anti-Fraud Policy

An important part of preventing fraud is a written anti-fraud policy that specifically explains who in an organization manages fraud matters and sends a strong message to employees about the organization's intolerance to fraud.

Recommended sections:

Section	Description
Policy Statement	Commitments to preventing and detecting fraud, zero tolerance for fraudulent activities, importance of integrity and ethical behavior
Scope of Policy	Defines boundaries, specifies who it applies to (employees, contractors, vendors), types of activities covered
Responsibility for Fraud Prevention and Detection	Assigns responsibility to roles within the organization, including management, internal audit, employees
Actions Constituting Fraud	List of actions considered fraudulent, e.g., theft, embezzlement, falsification of records
Non-Fraud Irregularities	Distinguishes between fraud and other irregularities, helps in categorizing issues correctly
Reporting Procedures	Steps to report suspected fraud include: how to report, to whom, and importance of timely reporting
Investigation Responsibilities	Specifies who is responsible for investigating reported fraud (includes internal audit, compliance officers, external investigators)
Authorization for Investigation	Details authority granted to individuals or teams to conduct investigations, ensures necessary access and resources
Confidentiality	Emphasizes the importance of maintaining confidentiality, protects identities of those reporting fraud
Disciplinary Action	Describes potential consequences for individuals found to have committed fraud, including termination, legal action, other penalties

Tip: Before publishing, management should consult with legal counsel to address any necessary legal considerations regarding the policy. This helps ensure consistent handling of allegations and offenders.

© 2024 IOFM, Diversified Communications. No part of this publication may be reproduced, stored in a retrieval system or transmitted by any means, electronic or mechanical, without prior written permission of the Institute of Finance & Management.

Fraud Risk Assessment

Organizations need to complete a fraud risk assessment to identify vulnerabilities, implement effective controls, and mitigate potential losses. For an organization to effectively manage its receivable fraud risks, the fraud risks must first be identified.

Here are the steps of a formal accounts receivable fraud risk assessment:

1. Identify potential inherent fraud risks and schemes.
2. Assess the likelihood of the occurrence of the identified inherent fraud risks.
3. Assess the significance of each inherent fraud risk to the organization.
4. Evaluate which people and departments are most likely to commit fraud.
5. Identify and map existing preventive and detective controls to the relevant fraud risks.
6. Evaluate whether the identified controls are operating effectively and efficiently.
7. Identify, evaluate, and respond to residual fraud risks that need to be mitigated.

This proactive approach helps safeguard assets, maintain financial integrity, and ensure compliance with regulations, ultimately protecting the organization's reputation and fostering a culture of accountability and transparency.

Tip: The Association of Certified Fraud Examiners provides free fraud risk tools under their Fraud Risk Management Guide. This includes a risk assessment and follow-up action templates as a free downloadable Excel resource.

© 2024 IOFM, Diversified Communications. No part of this publication may be reproduced, stored in a retrieval system or transmitted by any means, electronic or mechanical, without prior written permission of the Institute of Finance & Management.

Additional Resources

- Association of Certified Fraud Examiners (ACFE). "2024 Report to the Nations: Global Study on Occupational Fraud and Abuse." https://legacy.acfe.com/report-to-the-nations/2024/
- Association of Certified Fraud Examiners (ACFE). "Fraud Risk Management Tools" https://www.acfe.com/fraud-resources/fraud-risk-tools---coso/tools
- WesBanco. "Accounts Receivable Fraud: Risks, Red Flags, and Best Practices." Last modified September 27, 2023. https://www.wesbanco.com/education-insights/accounts-receivable-fraud-risks-red-flags-and-best-practices/.
- Meaden & Moore. "4 Signs of Accounts Receivable Fraud Schemes" Posted January 2, 2020. https://www.meadenmoore.com/blog/iag/4-signs-of-accounts-receivable-fraud#:~:text=If%20customers%20consistently%20complain%20that%20payments%20have%20been%20misapplied,%20posted
- KPM CPAs & Advisors. "How Surprise Audits Protect Against Fraud". Posted May 31, 2024. https://www.kpmcpa.com/how-surprise-audits-protect-against-fraud/
- The Federal Reserve. "E-remittance Exchange Pilot: Payments Industry Joins Forces to Improve B2B Payments". https://fedpaymentsimprovement.org/news/blog/e-remittance-exchange-pilot-payments-industry-joins-forces-to-improve-b2b-payments/
- Minster Bank. "Accounts Receivable Fraud: Risks, Red Flags, and Best Practices" Posted April 11, 2024. https://www.minsterbank.com/resources/learn/blog/accounts-receivable-fraud-risks-red-flags-and-best-practices/

About the Institute of Finance & Management

Accounting and finance professions have each undergone nothing short of a complete transformation since the Institute of Finance and Management (IOFM) was founded in 1982. Since then our mission has been, and continues to be, to align the resources, events, certifications, and networking opportunities we offer with what companies need from the accounting and finance functions to deliver market leadership. IOFM empowers accounting and finance professionals to maximize the strategic value they offer their employers.

Our enduring commitment to serving the accounting and finance professions is unmatched. IOFM has certified over 25,000 accounting and finance professionals and serves several thousand conference and webinar attendees each year.

IOFM is proud to be recognized as the leading organization in providing training, education and certification programs specifically for professionals in accounts payable, procure-to-pay, accounts receivable and order-to-cash, as well as key tax and compliance resources for global and shared services professionals, controllers, and their finance and administration (F&A) teams.

Learn more at **IOFM.com**

IOFM Institute of Finance & Management

© 2024 IOFM, Diversified Communications. No part of this publication may be reproduced, stored in a retrieval system or transmitted by any means, electronic or mechanical, without prior written permission of the Institute of Finance & Management.