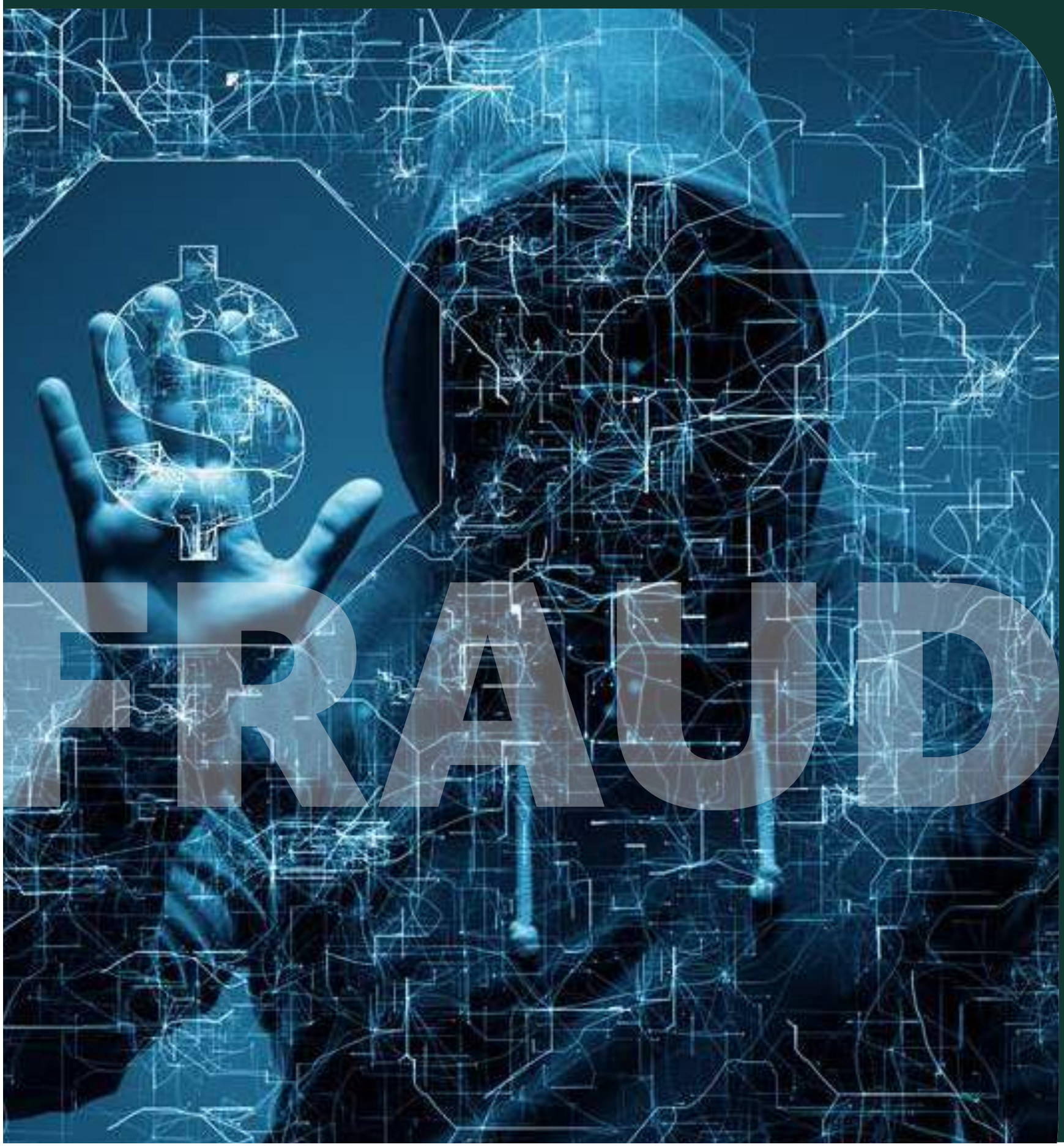
rillion

White Paper

Top 6 Action Steps to Reduce Payments Fraud



Reducing P2P Fraud

Despite organizations recognizing the threat and actively implementing controls to reduce payments fraud, tactics are becoming more sophisticated and success more frequent.

According to the 2019 AFP Payments Fraud and Control Survey, “more than 80 percent of financial professionals report that their organizations were targeted by fraudsters in 2018, the largest percentage since the Association of Financial Professionals® (AFP) began tracking such activity” in 2005.

Unsurprisingly, one of the reasons fraud has hit new heights may be that there has been a strong period of growth – and disruption. As rapid growth boosts the number of transactions a company handles, and disruption causes a certain amount of uncertainty, new opportunities to commit fraud arise.

Controls are often bypassed or overridden as current staff struggle to manage increased workloads, while new hires take advantage of lax recruitment practices put in place to fill positions quickly.

While only four percent of perpetrators have a prior fraud conviction, businesses may be infiltrated for the express purpose of conducting fraudulent activities.

The Association of Certified Fraud Examiners (ACFE) found that occupational fraud (using one’s occupation for personal gain) cost businesses over $7 billion in just 21-months.

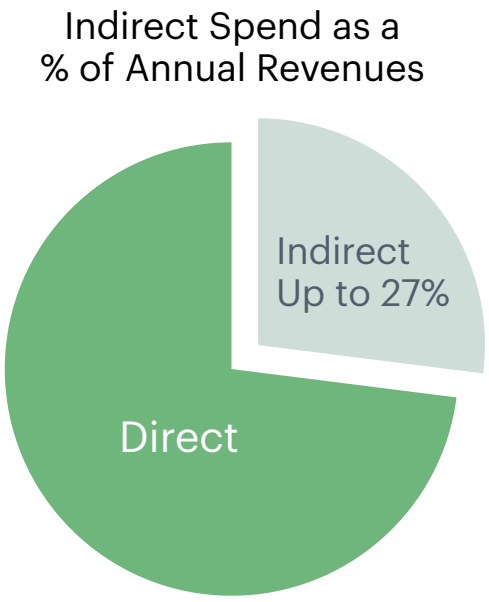
At an average of $130,000 per case and an elapsed time of 16 months before a scheme is discovered, an estimated 50% of fraud cases can be directly attributed to a lack of internal controls.

This highlights the need for businesses to increase focus on protecting their bottom line by implementing and maintaining controls - especially during periods of growth or disruption where oversight of indirect spend tends to be less rigid.

Managing indirect vs. direct spend

Both direct and indirect spend is critical to business operations. Direct spend—direct cost or direct procurement— involves spending related to the goods, materials, and services directly related to the production of products and/or services offered by a business.

Indirect spend, on the other hand, refers to administrative or internal expenses incurred to operate the company. These may include the costs associated with facilities, utilities, office equipment and supplies, travel expenses, and similar items.



While most companies use sophisticated enterprise resource planning (ERP) and supply chain management (SCM) software to monitor and control their direct spend, it's in the area of indirect spend that cost control and risk mitigation are often overlooked.

Generally accounting for 15-27% of a company's total revenue, indirect spend is where the majority of occupational fraud takes place.

Exposing fraud across purchase to pay (P2P) functions

According to the ACFE report, small businesses lose—for each case—almost twice as much to fraud as do large companies, at a median loss of $200,000 per incident.

Employees who have been with their company for more than five years tend to defraud them of twice the amount as employees with less than five years' tenure.

Since the fear of bad publicity often prevents companies from pressing charges, the majority of these businesses rarely—if ever—recoup their losses.

While not all P2P fraud reaches the heights of Evaldas Rimasauskas and his compatriots who tricked Google and Facebook into wiring them over $100 million between 2013 and 2015 with a business e-mail compromise (BEC), fraud can have a significant impact on a business, no matter the size.

Here are some examples:

The superintendent and the wife

In one Massachusetts' school, the superintendent conspired with his wife to defraud the school system. While she formed a distributorship for office and cleaning supplies, he used his position to ensure all procurement went through her business. She took the orders, bought the goods from Home Depot and Office Depot, and marked them up by 20%.

If not for the sharp eyes and courage of another school employee who saw her delivering supplies to the school, the fraud may have continued for much longer.

The shipping manager and the packaging company

When a consumer goods company terminated a product line requiring specific packaging, the shipping manager falsified orders. When the boxes arrived, he sent them for recycling and pocketed the income.

Eventually, he got greedy, plotting with the packaging company to stop shipping the boxes and splitting the profits. The mistake he made was arriving at work in a Porsche, triggering an investigation.

The manager and the accountant

Between 2011 and 2013, the manager of a large healthcare organization—with over 500 locations and thousands of SKUs—colluded with an accounting clerk, defrauding the institution of over $1.4 million.

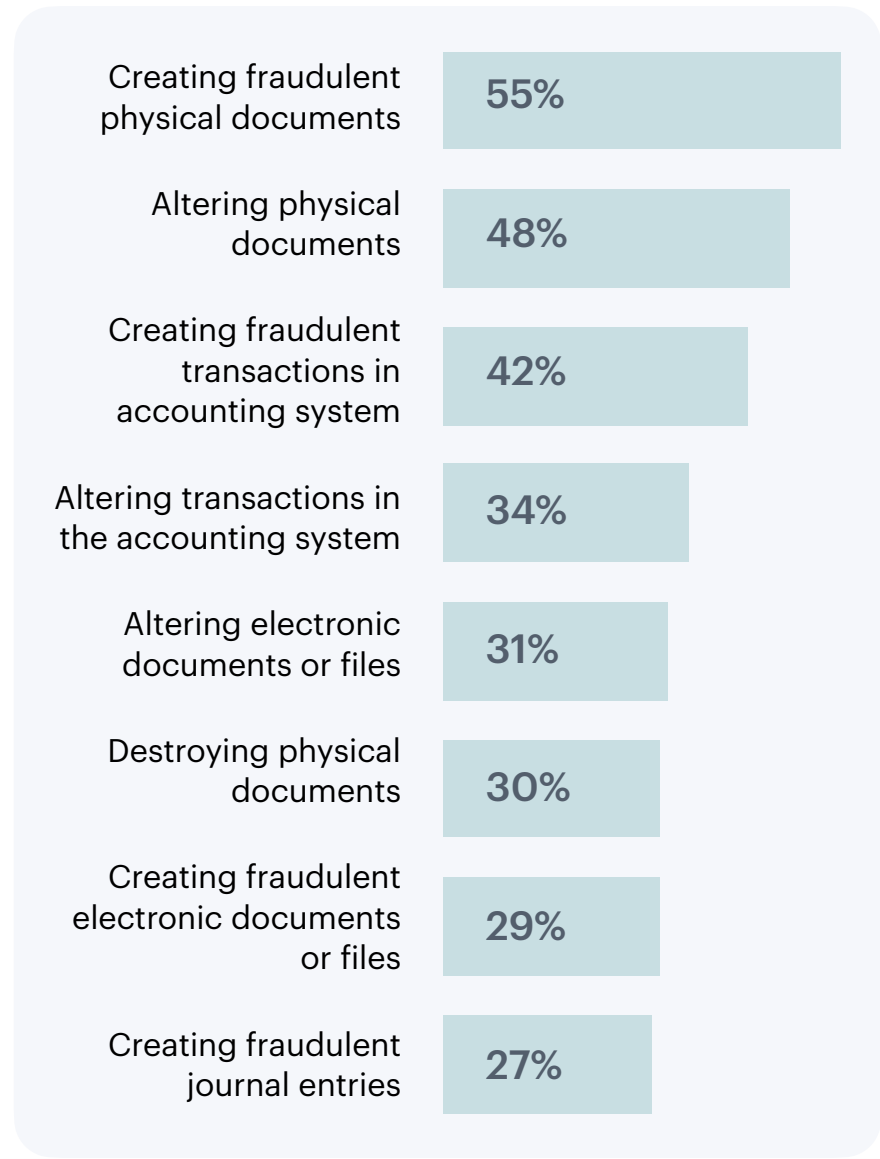
They set up a phantom company tied to an ACH account and invoiced varying amounts under $10,000 (the audit threshold) in no specific pattern with different vendor numbers.

It was only after both the employees had left the company that late payment demands were researched and the fraud discovered.

It's interesting to note that while fraud by owners or executives comprises only a relatively small percentage—19%—of all cases of fraud, the average loss per case amounts to $850,000.

Identifying attempts to conceal fraud

According to ACFE, 97% of cases include efforts to hide the fraud[3]. The top eight methods used are:



Pinpointing the root causes of fraud

In a P2P environment, both procurement and payment processes are susceptible to fraud. As the previous examples highlight, these include:

- **Phantom vendors**
  Often colluding with third parties, occupational fraudsters approve purchase orders, vendor master changes, and payments on behalf of non-existent or fake suppliers.
- **Impersonation**
  The fraudster sends official-looking correspondence—or makes a phone call in person—representing a genuine supplier and requesting a bank account or address change to redirect payments.

  While fraud of this nature may have a relatively short lifespan before payment demands arrive from the real supplier, large amounts may have already have been siphoned off from company funds.
- **Dormant POs**
  Inactive purchase orders with outstanding balances may be reopened by insiders, the bank account changed, and fraudulent invoices submitted against the PO. As long as amounts remain below the audit threshold, fraud of this type may remain undetected indefinitely.
- **Fake invoices**
  One-off invoices may be submitted to exploit the lack of controls required to manage the exception process. In many cases, the unsuspecting accounts payables clerk will create a new vendor record to make the payment without verifying the vendor or goods received.

All these forms of fraud can be traced to inadequate controls in the areas of indirect purchasing, account payables, vendor management, human data entry, and audits.

Addressing these areas reduces the risk of you being one of the over 50% of companies who experience losses due to fraud each year.

All these forms of fraud can be traced to inadequate controls in the areas of

- *indirect purchasing*
- *account payables*
- *vendor management*
- *human data entry*
- *audits*

6 Steps You Can Take to Prevent Fraud in 2020

According to ACFE's findings, "fraudsters tend to start small and increase their frauds rapidly over the first three years."

Frauds detected using proactive IT controls tend to last five months with average losses of only $39,000, while schemes that went undetected jumped to almost $1 million at the two-year mark.

> **"Organizations can reduce the impact of fraud by pursuing internal controls and policies that actively detect fraud."**

If you're responsible for P2P in your company, here are six controls you can put in place to reduce the chance of you becoming a victim of fraud:

1. Close the gap

Control spend with 100% purchase utilization, partnering with purchasing to enforce vendor vetting, the input of PO and contract numbers for traceability—including for one-off purchases.

2. Automate data capture

Implement enhanced requisitioning and purchase order matching with an automated data capture system that's accurate, inexpensive, and easy to deploy, reducing human touch points and increasing accuracy.

3. Implement workflows

Enforce controls through catalogs, punchouts, workflow, and permissions to prevent data from being entered, altered, or deleted without authorization, ensuring audit trails are in place to track all changes.

4. Enforce multi-level approvals

Impose a multi-person approvals matrix for all payments as part of the standard workflow, reducing dependence on a single individual for authorization.

5. Transform audit processes

Change audits from being based on line item amounts to random samplings independent of monetary value or time, increasing the chance of quickly identifying fraudulent activities. ACFE's research indicates that implementing surprise audits reduces losses in 51% of cases, and resulted in faster detection of attempted fraud 52% of the time.

6. Use intelligence

Leverage AI to detect patterns, irrespective of fraud schemes or time elapsed. According to ACFE, data monitoring and analytics accelerates detection by 58% and reduces losses by 52%.

Footnotes

1. Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse, ACFE, 2018
2. According to ACFE, when fraudsters collude, losses are more significant.
3. Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse, ACFE, 2018

About Michael Cichy

Michael joined Palette Software in 2010 and launched their US and Canadian operations. Prior to Palette he was a Co-founder of Attache' a consulting firm which assisted international software companies in building US operations and management teams.

With over 35 years of experience in process automation Michael has held management positions in Finance and Operations with Digital Equipment Corporation, The Army and Air Force Exchange Service, Kodak, and Oracle. He is a graduate of Northwestern University and holds CDIA and Six Sigma credentials.

About Palette Software

Palette Software is a market-leading vendor of financial process automation for domestic and global corporations, including AP Automation and Purchase to Pay Automation.

Palette solutions automate the connecting and matching of purchase orders, invoices and contracts, on-premise or in the cloud.

Customers experience significant and measurable cost savings, productivity gains and operational excellence. Palette solutions are GDPR compliant and optimize financial management for more than 4,000 customers in 50+ countries.

With 25 years of experience, Palette and its partners offer automation solutions for organizations of all sizes worldwide.

palettesoftware.com

Palette is now

rillion

rillion.com