appzen

6 Most Common Types of Invoice Fraud

The average large company processes hundreds or even thousands of invoices every month. The sheer volume makes it impossible to closely examine each bill that comes through the door.

For those intent on deception, there are countless ways to exploit this vulnerability. Duplicate invoices, fake invoices, phishing schemes, vendor impersonation, unapplied discounts, cash skimming, cash lapping, shell companies... these are just a few of the methods used by motivated criminals to suck money out of large corporations, often without consequence. Both company outsiders and employees commit invoice fraud, and often the two groups work together.

How can your business prevent falling prey to invoice fraud schemes? Knowing exactly what to look out for is an important first step.

Common Risks

External Schemes

- Duplicate invoices
- Fake invoices
- Overbilling
- Not applying discount terms
- Changing payment terms
- Products not delivered
- Phishing scams

Internal Schemes

- Shell companies
- Duplicate invoices
- Fake invoices
- Cash skimming

1 False and Duplicate Invoices

Duplicate invoices are a huge source of leakages for big businesses. Two percent of a typical corporation's A/P invoices may be duplicates, reports AuditNet. For a company with $75 million worth of invoices each year, that's a whopping $1.5 million annually. Not all duplicate invoices are fraud, of course, but sneaking duplicate invoices under the radar is a popular tactic for criminals on the inside and outside of organizations.

In one case, accountant Stephen Jones sneakily defrauded his employer, CPCCommodities, of more than $765,000 over a five-year period. According to court records, "At times, Stephen Jones transferred money to his account in amounts similar to direct deposits of his salary, though he had already been paid... Stephen Jones also transferred money to his account in amounts of payments due on duplicate invoices received from vendors." Ultimately Jones was sentenced to serve two years in prison and pay full restitution.

Fraudsters may submit outright fake invoices as well. An inside connection to the business makes it easier to get away with this blatant deception, but external parties often try to get away with the crime by submitting invoices for amounts low enough that they'll fly under the radar. Subscriptions, directory listings, compliance services, and paper are just a few of the more common "services" criminals cook up fake invoices for, according to the Office of the Attorney General in Minnesota.

2% of a corporation's A/P invoices may be duplicate.

8 Signs of a Sketchy Invoice

Some criminals are extremely savvy; many are not. Watch out for these hallmarks of false invoices:

1. Rounded amounts (e.g., $1,500.00 vs. $1,487.23)
2. Invoices just below the sanctioned approval amount (e.g., supervisor can approve up to $2,000; invoice is for $1,990).
3. Abnormal invoice volume from one vendor
4. Vendors with mail drops (e.g., Mailboxes Etc.) as their mailing address
5. Invoices for vague, intangible services
6. Typos and grammatical errors
7. Arithmetic errors
8. Abnormal digit frequency in financial figures: Benford's Law specifies the probability of certain numerals' appearances in a data set—fake invoices will usually defy this scientific rule.

2 Shell Companies

As an accounts payable clerk for Tigrent Inc., a provider of financial literacy tools, 34-year old Florida resident Junipher Sayers managed to steal more than a million dollars from her employer by submitting false invoices and diverting them to shell companies she had created explicitly for the purpose.

Sixty-four year old New Jersey resident Philip Charles de Gruchy defrauded his former employers, Toys “R” Us and Tumi Luggage, out of a combined $3 million by creating shell companies with his deceased ex-wife Barbara Brown. Their fake companies (“CEM Direct Marketing” and “BI Insights”) billed for “marketing consulting work” that was either never delivered or was plagiarized from other firms’ work.

One employee and his wife stole $3 million dollars from Toys “R” Us and Tumi Luggage.

Both of these schemes used shell companies — companies which exist only on paper and provide no services — to carry out their fraud. This type of asset misappropriation presents a huge risk for companies. In a study of 2,504 occupational fraud schemes (fraud perpetrated by company insiders) across 125 countries, the Association of Certified Fraud Examiners (ACFE) found that such asset misappropriation made up 86% of fraud cases in 2020. Overall, occupational fraud resulted in more $3.6 billion in total losses.

3 Cash Skimming

Cash skimming refers to an employee stealing money from a business before that money has been recorded in the books. This type of fraud may seem minor — a few dollars pocketed here or there — but substantial, cumulative losses can occur.

In one example, the State of Washington Department of Transportation lost $118,000 as a result of a cash skimming scheme perpetrated by two ticket-takers in their ferry terminal. The ticket-takers collected cash fares but didn’t record the transactions or provide customers with a receipt. In another cash skimming scheme, a county landfill lost $165,000 in one year from cashiers stealing customer service fees paid in cash.

4 Non-Delivery of Product or Service

A company orders a product, the vendor submits an invoice, and... the product is never delivered. That's what happened in the case of Detroit multi-millionaire and businessman Gary Tenaglia, whose firm was contracted to remove ice and snow at the Detroit Metro Airport. Tenaglia billed the airport for $1.5 million worth of specialty de-icing product called NAAC, but he never actually ordered the product. Instead, he pocketed the cash.

Tenaglia appears to have conspired with accomplices as part of a wider corruption scandal but 3-way matching — in which the invoice is cross-verified with the purchase order and the receipt — is often the best way to begin to identify false invoices and/or undelivered products.

5 CEO Fraud

No, this isn't CEOs stealing money from their own business (though that happens too). In this scheme, criminals impersonating company execs send emails authorizing urgent payments. Think: "We need to close this deal immediately, here are the wiring instructions." A third party follows up to confirm, the accountant wires the money and breathes a sigh of relief — the deal will go through.

Except of course, it's all a scam. According to the 2020 FBI Internet Crime Report, CEO fraud is a sophisticated form of "business email compromise," generating 19,369 reports and adjusted losses of over $1.8 billion in 2020 alone. These types of identity theft scams are evolving to capture and compromise other kinds of personal information, which is used to transfer stolen funds and sometimes convert to cryptocurrency.

In one case, German company Leoni AG, a large, publicly-traded manufacturing company, lost 40 million Euros ($44.6 million) in the blink of an eye after their CFO received a fraudulent payment request. The request was carefully crafted with the company's internal protocol for transfers in mind. The company stock dropped by nearly 7 percent following the incident.

Many company executives think their recruiting processes will weed out fraudsters. But the ACFE found that only 4% of perpetrators had a prior fraud conviction.

Criminals may use malware to hack into executive email accounts, studying their patterns of speech, travel schedule, and business practices before sending out fraudulent requests. Or they'll use spoofed email addresses that look similar to a CEO's real address. The schemes can be quite sophisticated, and often specifically target companies that conduct extensive foreign transactions via wire transfer, since those payments are difficult to reverse.

6 Vendor Impersonation

Criminals may use spoofed emails to impersonate trusted vendors as well. Using a lookalike address (e.g., accounting@company.name.com instead of accounting@companyname.com), they might send an email saying they've changed ACH routing information or billing address, along with a fake invoice. Smart fraudsters will do their research: they'll use a company that you frequently do business with and figure out exactly which employee to target within your ranks.

Sometimes, the tone of the email might be a bit off, or a closer look at the email address might reveal the deception — but when your team is busy and unsuspecting, it's easy for something like this to slip under the radar.

In one example, an Arkansas woman impersonated Happy Egg Co., an organic egg supplier and emailed a customer of the company, Woodland Partners, stating that its bank account information had changed. The customer diverted payments to the new account and the fraud went undetected until Happy Egg Co. alerted Woodland Partners that it had fallen nearly a million dollars in debt.

Subtle Schemes

Some fraudsters prefer to perpetrate more subtle deceptions, trading lower rewards for less risk.

Examples include:

- Billing for more units than the quantity requested on the original purchase order (and the quantity ultimately received)
- Not applying discount terms from the contract
- Agreeing to net 60 terms on the contract but using net 30 on the invoice
- Not honoring "lowest pricing" guarantees on contract (e.g., advertising lower pricing available on the website but billing the original price)

Protecting Against Fraud

Invoice fraud is an insidious problem for large companies. Threats can come in all forms and from a wide variety of people — employees, vendors, hackers, and others. With millions of invoices coming in each year, audit teams are often too buried in their day-to-day responsibilities to proactively think about preventing fraud. Furthermore, auditors rarely have investigative mindsets, and a traditional financial statement audit is simply not designed to detect fraud.

But protecting against fraud is crucial for the bottom line. Below are some of the most common methods for protecting against occupational fraud, according to the Association of Certified Fraud Examiners:

- External audit of financial statements
- Code of conduct
- Internal audit department
- Management certification of financial statements
- External audit of internal controls over financial reporting
- Management review
- Hotline
- Independent audit committee
- Anti-fraud policy
- Employee support programs
- Fraud training for employees
- Fraud training for managers/executives
- Dedicated fraud department, function, or team
- Formal fraud risk assessments
- Surprise audits
- Proactive data monitoring/analysis
- Job rotation/mandatory vacation
- Rewards for whistleblowers

CEO fraud was responsible for over $1.8 billion in losses in 2020.

About AppZen

AppZen is the leader in Finance AI software, empowering autonomous finance operations for modern finance teams. Our patented artificial intelligence software accurately and efficiently processes information from thousands of data sources so that organizations can better understand internal spend and make smarter business decisions. It seamlessly integrates with existing expense and accounts payable workflows to read, understand, and make real-time decisions based on your unique spend policies, leading to faster processing times and fewer instances of fraud or duplicate spend. Global enterprises, including one-third of the Fortune 500, use AppZen's Expense Audit and Autonomous AP products to replace manual finance processes and accelerate the speed and agility of their businesses. To learn more, visit us at www.appzen.com.

APPZEN.COM