

Mitigating the 3 BIGGEST Accounts Payable FRAUD RISKS

Businesses now face increasing fraud risk, creating significant challenges for accounts payable teams. Last year, 78 percent of businesses were negatively impacted by payments fraud¹ and suffered from financial losses, reductions in efficiency and damage to the corporate brand image.

Here are a few leading forms of fraud taking place in B2B payments today, along with ways you can mitigate that risk:

CHECK PAYMENTS

75% of fraudulent payment activity is related to checks²,

Yet more than half of all businesses are still using checks as their primary method for business payments³, and 60% of businesses report only rare-to-occasional use of more-secure ACH transfers⁴

Mitigate risk by...

Transitioning to electronic payment methods

- Credit card
- Virtual card
- ACH payment options

BUSINESS EMAIL COMPROMISE (BEC)

According to the FBI, BEC attacks have grown to become a \$5.3 billion dollar industry⁵

It's as simple as this:

- 1 Fraudsters identify a time CEO is out of office
- 2 Pretend to be the CEO, reach out to AP employee requesting an immediate funds transfer
- 3 AP employee immediately transfers funds

Mitigate risk by...

Implementing segregation of duties and two-factor authentication to require additional approval while preventing accounts from getting hacked.

How it works:

- After AP Manager queues up a payment, Payment Authorizer is notified and prompted to enter password
- Payment Authorizer receives security code, usually via text message
- Payment Authorizer enters security code and releases the payment

ACH FRAUD

While ACH transfers were targeted much less frequently than checks, 28 percent of companies were subject to ACH debit fraud and 13 percent were subject to ACH credit fraud⁶

Typical ACH Fraud Scheme:

- Fraudsters contact a business or organization and make a request to update a vendor's payment information.
- When valid payments are made, the money goes to the updated account, creating a loss for both the actual vendor and paying business.
- Fraudsters then quickly move the funds to another international account or remove them from the specified account.

Mitigate risk by...

Authenticating every request, and verifying with previously saved vendor info independent of the current request.

Automating the accounts payable process offers businesses the opportunity to build best practices like these into their accounts payable process in a scalable and repeatable manner.

Curious to see how automating accounts payable can secure your vendor payment process?

Contact MineralTree for a personalized demo at mineraltree.com/demo

SOURCES FOR STATS:

(1) (2) (3) 2017 AFP | Payments Fraud and Control Survey
<https://commercial.jpmorganchase.com/jpmpdf/1520732417358.pdf>

(4) NACHA
<https://www.nacha.org/ach-network>

(5) Tracking Trends in Business Email Compromise (BEC) Schemes
<https://documents.trendmicro.com/assets/TrackingTrendsInBusinessEmailCompromise.pdf>

(6) 2018 AFP Payments Fraud and Control Survey Report
<https://commercial.jpmorganchase.com/pages/commercial-banking/services/2018-AFP-Survey>



mineraltree®
AP and Payment Automation

www.mineraltree.com