Fraud in Payment Flows

Points of Control & Vulnerability

STRATEGIC TREASURER

Bottomline

Access Full Report

2020 | Treasury Fraud & Controls Survey

UPSTREAM PREVENTION

DOWNSTREAM DETECTION

PAYER SETUP CONCERNS

- *Fraudulent Employee*
- *Fictitious Vendor*
- *Invalid Instructions*
- *Sanctioned Party*

DISBURSEMENT VULNERABILITIES

- *False Invoices*
- *Misdirected Payments*
- *Compromised Gateway*
- *Out-of-Band Validation*

Segregation of Duties

83% of organizations utilize dual controls

Employee Education

66% train at point of hire;
70% train annually

Internal System Monitoring

51% of firms have user monitoring software

ACH Fraud

27% experienced attempts;
2% resulted in staff termination

Incident Management

Less than half **(49%)** have a reaction plan

Reconciliation (Declining!)

28% (down from 45% in 2016) daily reconcile **>90%** of accounts

Visibility (Stable)

~2/3rd have daily visibility to **>90%** of accounts since 2016

RECONCILIATION CONCERNS

- *Speed to Detect*
- *Lack of Visibility*
- *Slow/No Reconciliation*
- *Appropriate Automation*

Ransomware

19% success rate;
9% firms paid;
9% had follow-on attack

Research Overview

The risk of fraud has risen despite elevated spending and confidence as criminals continue to operate in increasingly sophisticated and automated ways. Payment diversion and imposter fraud are generating the most realized losses.

Discover more from the experience and perspective of 350+ corporate and bank practitioners who participated in the 4th annual Treasury Fraud and Controls Survey by downloading the results report.

NOTABLE CORRELATIONS

There are significant links between fraud training and fraud interdiction services in relation to lower realized losses. Firms utilizing payment fraud solutions with interdiction capability experienced 75% fewer losses in BEC, imposter, and CEO fraud.

Organizations without fraud prevention training for employees experienced greater losses across various types. No training correlated with greater losses by these factors:

2x ACH Fraud, 4x BEC Fraud, and 5x Ransomware—among others.

Multi-factor Authentication (MFA)

66% utilize on wire payments;
44% on non-wire

Principle of Least Privilege

Less than **1 in 5** utilize this control principle

Imposter Fraud/Business Email Compromise (BEC)

67% hit by attempts;
18% resulted in financial loss

Fraud Detection & Interdiction

20% have system in place;
17% have alert-only