Staying Ahead of Payments Fraud and Cybersecurity Threats: Trends to Watch

Digital payments, social engineering and business email compromise (BEC) are all payments fraud trends on the rise. Read on to explore the latest insights from the Association for Financial Professionals (AFP) 18th Annual Payments Fraud Survey that details these trends with tips to keep your organization safe.

Fraud is a significant threat, and new trends are emerging. Fraud remains a major problem:

71%

of organizations report having been victims of payments fraud attacks[1]

30%

Roughly 30% of companies saw an uptick in payments fraud in 2021[1]

These types of fraud are increasing and intensifying:

- Identity theft, stolen credentials, spoofing and other digital payment fraud schemes
- Business email compromise
- Social engineering

Actions to mitigate fraud:

- Strengthen your analytics and controls
  - Data lake
  - Proactive and reactive measures
  - Regularly look at anomalies – uncover undetected patterns
- Expose and block vulnerabilities
- Execute best practices Implement due diligence
- Educate staff regularly
- Stay current with fraud trends

Fraudsters are innovating around digital payments

As settlement speeds accelerate, new fraud types will emerge, creating a need for corresponding fraud prevention tooling for Real Time Payments (RTP)

ACH debit and credit fraud attacks are rising

37%

of financial professionals reported fraud attacks via ACH debit[1]

41%

of organizations report ACH credits were impacted by business email compromise[1]

Tips to block same-day ACH debit and credit fraud:

- Maintain and promptly enforce ACH debit policies and procedures
- Conduct daily reconciliations vs. monthly
- Use ACH debit filters/debit blocks
- Update company IDs for filters on a timely basis
- Hold an independent review of the processes done by internal audit

Social engineering is a growing challenge

A trend on the rise

- 35% reported increased concern around identity theft and social engineering[1]
  - A 14% increase over the 2021 report[1]
- COVID-19 created widespread panic and fear that helped bolster this type of fraud

Avoid social engineering:

- Don't click links from unsolicited text messages or emails
- Only use a company phone number that is verified using a company directory or by calling the requestor directly
- Educate staff on how to identify a social engineering scam

Business Email Compromise remains a substantial threat

In 2021, BEC was the source of the majority of payments fraud attempts and attacks

55%

of companies experienced actual or attempted payments fraud because of BEC[1]

58%

of respondents indicated their AP departments were compromised through email scams[1]

Top ways you can combat BEC:

1. Implement company policies for providing appropriate verification (e.g., contact information from a system of record) before making any changes to existing information
   - Invoices
   - Bank deposits
   - Contact details
   - Authentication of the party (both consumer or commercial) prior to execution of a "net-new" or "net-change" of data
2. Confirm requests for any transfer of funds by executing a callback to an authorized contact at the payee organization using a phone number from a system of record
3. Use real-time tools in order to detect both mismatches from expected counterparty information while simultaneously authenticating the counterparty wherever possible
4. Educate employees on BEC threats and how to identify email scams

Fraud mitigation components must work together to battle these ongoing and emerging threats.

- Build and maintain awareness
- Utilize monitoring and reporting tools
- Practice constant vigilance
- Identify vulnerabilities and close gaps
- Ensure policies and procedures are agile and responsive

[1] Installed Trends in Healthcare Payments Annual Report

For more fraud insights visit: **jpmorgan.com.**
View the full Association for Financial Professionals 18th Annual Payments Fraud Survey results **here.**

Contact your local J.P. Morgan representative to learn more about trends in payments fraud and cybersecurity threats.

Resources:

How Criminals Use Social Engineering to Target Your Company
Recognizing email threats and social engineering
Protecting Against Business Email Compromise

J.P.Morgan