Payment fraud continues to impact most organizations

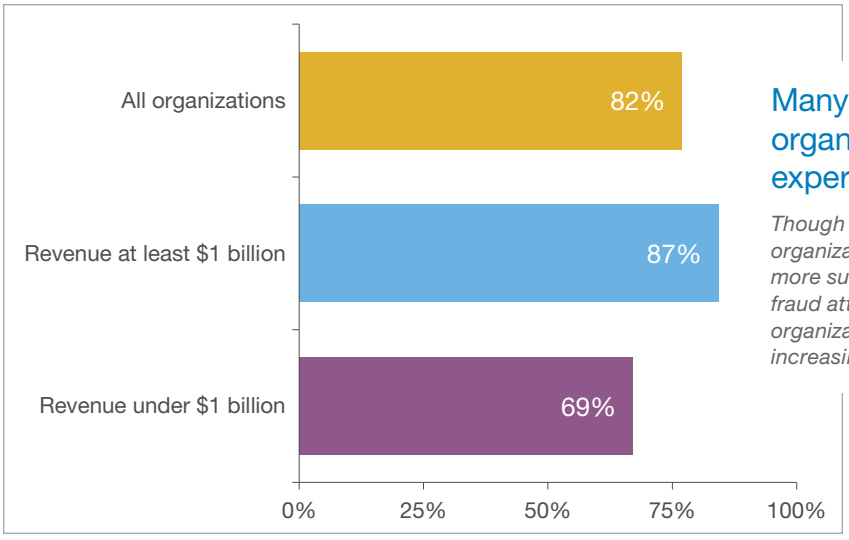
Since 2005, the Association for Financial Professionals (AFP) has conducted an annual survey on payment fraud to understand fraud trends and identify actions that could prevent fraud.

The survey offers insight into actions organizations can take to deter fraud and prevent financial loss. The results continue to make a strong case for integrating internal best practices with bank solutions to provide the most comprehensive fraud protection.

Fraud overview

Payments fraud activity has increased significantly over the past five years. According to the 2019 survey, over 80 percent of organizations surveyed were the target of attempted or actual payments fraud in 2018. This is the largest percentage since the AFP began its survey.

Organizations subject to attempted or actual fraud[1]



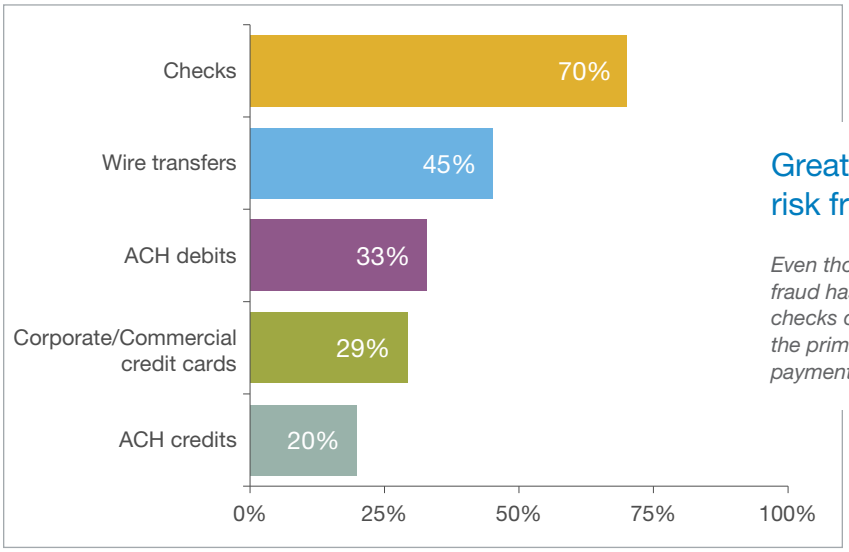
Many organizations experience fraud

Though larger organizations are more susceptible to fraud attacks, smaller organizations are increasingly a target.

Checks are the most widely used method of payment for business-to-business transactions and are a favorite target for fraudsters. Though most affected by fraudulent activity, check fraud has declined since 2010.

ACH credit and debit fraud, however, is on the rise. As fraudsters move away from check, and to a lesser extent wires, they're beginning to target ACH transactions. Since ACH payments are usually considered safer and harder to manipulate, the rise in ACH fraud indicates a more sophisticated type of fraud.

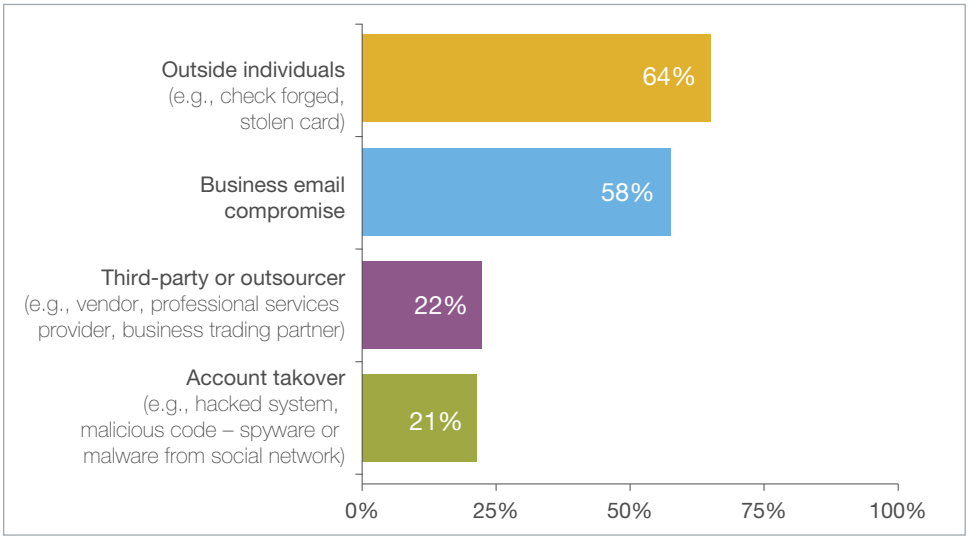
Prevalence of fraud by payment method[1]



Greatest fraud risk from checks

Even though check fraud has declined, checks continue to be the primary source of payment fraud

Sources of payment fraud[1]

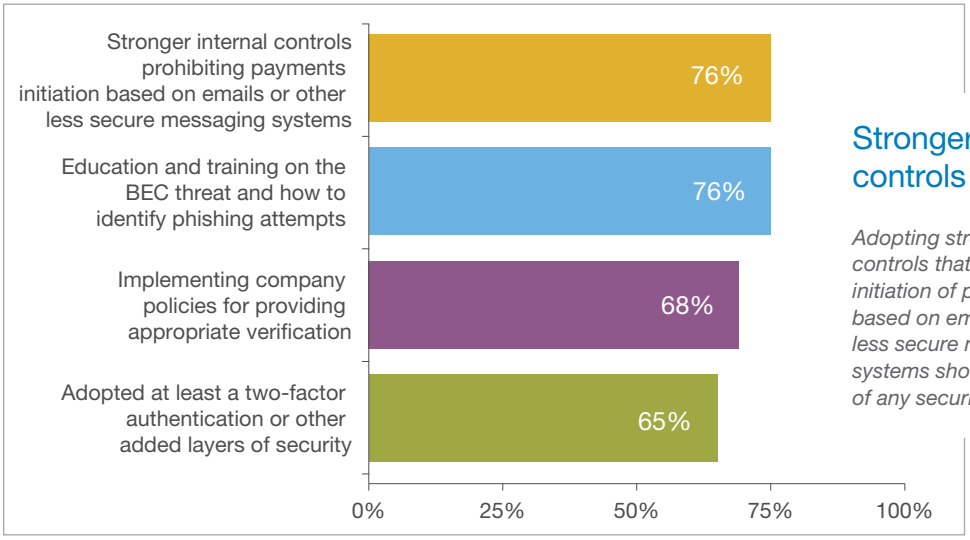


Business Email Compromise (BEC) fraud has been increasing since it was first discovered in 2013. In a BEC scam, fraudsters exploit online information to develop a profile on a target organization and its executives. Then, impersonating an executive, the fraudsters target employees with access to the organization's finances. Through email, fraudsters trick employees into making wire transfers to bank accounts thought to be those of trusted partners.

The number of organizations that fell victim to BEC rose from 64 percent in 2014 to 80 percent in 2018. According to the 2019 survey, the financial losses suffered by these organizations weren't significant. However, BEC fraudsters have become more creative and have found new ways to perpetuate their fraud attempts.

To protect against BEC, organizations have introduced many different procedures to help prevent fraudulent emails from "scamming" their employees.

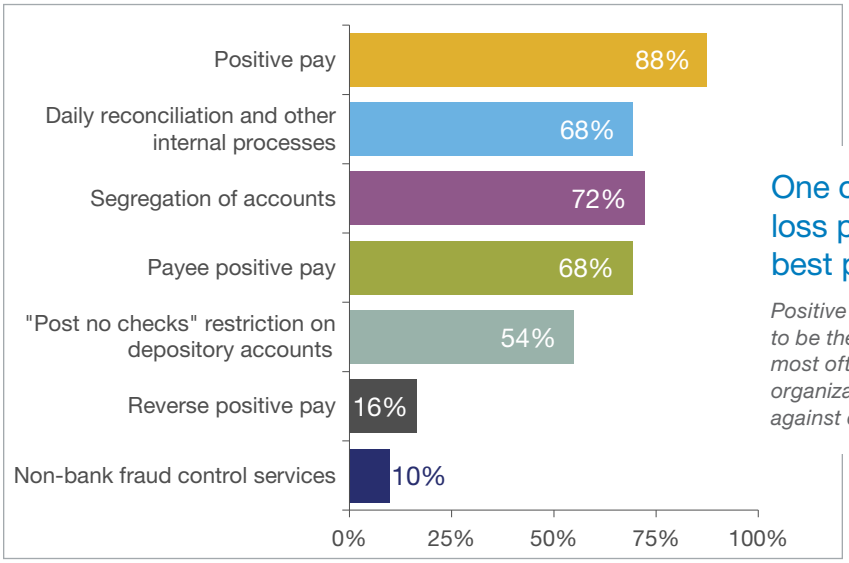
Guarding against email scams[1]



Stronger internal controls

Adopting strong internal controls that prohibit initiation of payments based on emails or other, less secure messaging systems should be part of any security strategy.

Fraud control procedures used to guard against check fraud[1]



One of many loss prevention best practices

Positive pay continues to be the method most often used by organizations to guard against check fraud.

Case file:

After experiencing check fraud, an organization adopted Positive Pay. After a time with no losses, the organization discontinued Positive Pay due to the belief that internal controls were sufficient to detect fraud. Soon, check fraud attempts were detected by bank tellers. Before Positive Pay was fully reinstated, the organization experienced $100,000 in check losses.

Solution: Consistently maintain Positive Pay on accounts issuing checks.

What is Positive Pay?

Positive Pay is a cash-management service employed to deter check fraud. Banks use Positive Pay to match the checks a company issues with those it presents for payment. Any check considered to be potentially fraudulent is sent back to the issuer for examination.

Don't wait until you become a victim of fraud to discover gaps in your fraud prevention program.

The Uniform Commercial Code (UCC) requires businesses to observe "reasonable commercial standards" to prevent fraud. Payment issuers may be precluded from receiving restitution from the paying bank if their own fraud prevention failures contribute to a forged or altered payment.

usbpayment.com/middle-market

[1]2019 AFP® Payments Fraud and Control Survey Report, data collected 2018

02-0061-01 (12/19) CAT-ID18225455