BUILT FOR
BETTER BUSINESS

Keeping your information safe

PROTECTING YOUR BUSINESS FROM FRAUD

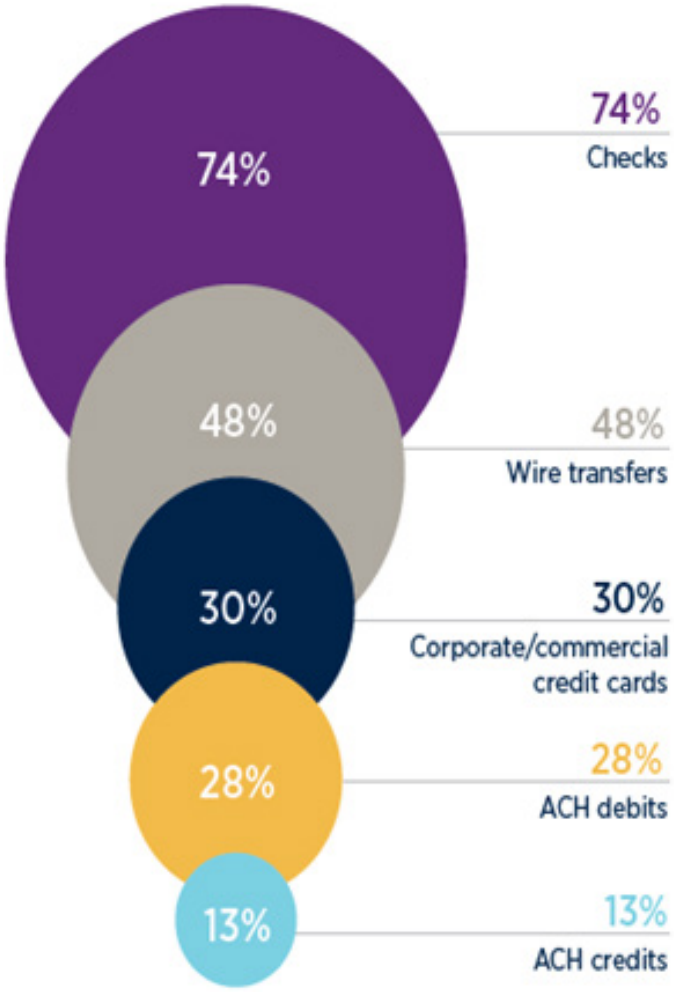
In an age where fraud attempts and attacks are at an all-time high, you owe it to yourself and your business to protect your cash.

While it is common for businesses to protect their physical assets with security systems and insurance, it is equally important to protect business data. Much of a company's secure data is maintained within the technology the company is using. Today, more and more businesses are using technology that helps streamline, enhance and improve efficiencies within an organization. Rather than restricting the use of these tools that improve your company's success, it is key to ensure the risk exposure these tools bring is effectively monitored to protect business data and systems. Protection of your valuable data, systems and networks requires ongoing risk review that is managed within a company cybersecurity strategy. An assessment of the risk exposure that exists and reviewing the best practices available to mitigate the potential of financial impact is key to managing your risk exposure.

The Many Forms of Fraud

Payment fraud reached a record breaking high with 78% of businesses reporting payment fraud attempts or attacks in 2017. The Association for Financial Professionals' 2018 Payments Fraud and Control Survey Report found that checks have been, and continue to be, the payment method most often exposed to fraudulent

Payment Methods that were Targets of Attempted/Actual Payments Fraud in 2017
(Percent of Organizations)

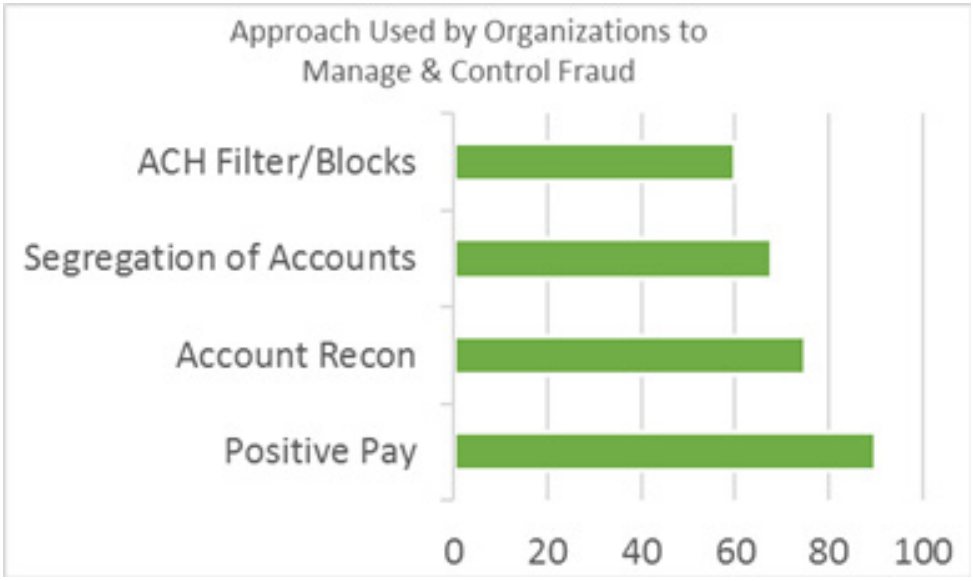


Source: 2018 AFP® Payments Fraud and Control Survey

activity, followed by wire transfers, corporate or commercial credit cards, ACH Debits and Credits. It's no longer a matter of "if," but more a matter of "when" payment fraud will impact your business. Unfortunately, many discover the hard way that paper checks are not secure and are easily compromised.

In addition to the rise in payment fraud, cyberattacks continue to evolve and change, making it essential for organizations to protect the systems that maintain their data. Business Email Compromise (BEC) is another form of fraud that is constantly evolving. BEC is an exploit in which the attacker gains access to a corporate email account and spoofs the owner's identity to defraud a company, or its employees and/or customers of money. BEC negatively impacts wire transfers the most (54%), with paper checks following as a close second (34%).

Discovering payment fraud activity is not as elusive as one might think. The Association for Financial Professionals recorded 65% of fraudulent payment activity comes from outside an organization. Therefore, it makes sense that treasury and accounts payable staff are the most likely to play an active role in helping identify instances of payment fraud. Treasury and accounts payable professionals are arming their organizations by implementing new best practices, along with leveraging technology in order to safeguard their funds and prevent a disruption to their business.



Source: 2018 AFP® Payments Fraud and Control Survey

Businesses have many easy-to-implement tools that are cost effective and streamline account reconciliation.

Best Practices

Mitigate Risk of Financial Loss

- Review Business Insurance Policies—Check your business insurance coverage for Cybersecurity Protection.
- Positive Pay—Compares the check number and dollar amount of each item presented against your account to your payment instructions. Allows you to view and decision checks before they post to your account.

- ACH Filters—ACH Alert/Filter allows you to create and manage an approved company list and maintain complete control of third parties debiting your account via the Automated Clearing House (ACH).
- Segregation of Accounts

Manage Risk

- Employee/Client Education—Best practices to combat BEC are based in security awareness and communication. To prevent BEC, companies should provide training for employees and address cyber security awareness to its customers.
- Dual Control—Segregation of duty, utilization of dual control for different functions and steps in the accounts payable (AP) Process.
- Payment Verification—Have procedures in place to confirm accuracy of payments before sending. If you get a request via email, call back a known phone number (not from email) to confirm.

Best Practices for your AP Process

- Master Vendor List—Create one list, registration process to add/make changes, continuous monitoring
- Review internal payment disbursement process.
- Payable Payment Type Strategy—Evaluate the shift from paper to electronic, analyze vendor payment teams, discount opportunities available.

Today, as payment fraud attempts are at a record high, companies need to protect themselves with a combination of AP best practice processes and savvy treasury management tools.