ASSOCIATION FOR FINANCIAL PROFESSIONALS

2020 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Comprehensive Report

Underwritten by J.P.Morgan

J.P.Morgan

We are proud to sponsor the AFP Payments Fraud and Control Survey for the 12th consecutive year and deliver the 2020 report.

According to the survey, 81 percent of companies were targets of payments fraud last year, once again proving that no industry is immune. Additionally, data for 2019 showed:

- 75 percent of organizations experienced Business Email Compromise (BEC)
  - 38 percent of organizations reported financial losses as a result of BEC
  - 42 percent of BEC scams targeted wires, followed by ACH credits at 37 percent
- 74 percent of organizations experienced check fraud in 2019—up from 70 percent in 2018
- Nearly one-third of organizations indicated that they have not received advice from their banking partners about mitigating potential risks associated with same-day ACH credit and debit transactions

While many of these statistics declined or stayed level since last year, it is important for businesses to stay vigilant by educating employees on the latest payments fraud practices and implementing tools and processes to safeguard their assets and data.

The non-financial implications of payments fraud are equally important to consider. For example, if a BEC attack exposes personal and confidential information, the reputational damage can be severe.

As a leader in treasury management services and electronic payments technology, J.P. Morgan is committed to mitigating fraud and protecting client information across our entire infrastructure. We will continue to invest in the technology, educational tools and risk management expertise to help protect your business.

We hope this survey informs you about potential cyber risks within your organization, so that you can better prepare for the future. And finally, we would like to thank the AFP for providing these valuable insights—they are an important reminder to remain committed to fraud detection and cybersecurity protocols.

With best regards,

Jennifer Barker
Managing Director
J.P. Morgan

Bob St Jean
Managing Director
J.P. Morgan

Jessica Lupovici
Managing Director
J.P. Morgan

Winston Fant
Managing Director
J.P. Morgan

Chad Prescott
Managing Director
J.P. Morgan

Alec Grant
Managing Director
J.P. Morgan

TABLE OF CONTENTS

INTRODUCTION

The payments fraud landscape in 2019 underwent few significant changes from the previous year. Payments fraud activity continued at near-record levels with 81 percent of financial professionals reporting that their organizations had been victims of an attempted or actual fraud attack. Despite the controls and processes organizations have put in place to safeguard their payment systems and minimize instances of fraud, it is evident that perpetrators of these crimes have not been discouraged and are still able to infiltrate payment systems. Although extensive use of sophisticated and advanced technology is assisting organizations in their battle to protect payment systems, that same technology is aiding criminals in their efforts.

Checks continue to be a popular payment method used for business-to-business (B2B) transactions (42 percent of B2B payments are made by check, as reported in the *2019 AFP Electronics Payments Report*). But while there has been a decline in check usage, the rate of fraud occurrences via checks continues to be elevated, and indeed topped the list of payment methods most frequently subjected to fraud attacks in 2019. It is encouraging that the share of organizations experiencing wire fraud activity is on the decline—down from 48 percent in 2017 to 40 percent in 2019. Financial professionals also need to be cognizant of ACH fraud; ACH debit fraud stayed constant—having occurred at 33 percent of organizations—while ACH credit fraud experienced a slight uptick. This may be a signal that fraud perpetrators are continuing to focus their efforts on check and ACH payment methods and a little less on wire transfers.

Financial professionals confirm that a significant share of their fraud attacks in 2019 was via Business Email Compromise (BEC). This is a method scammers resort to often as they are able to target payments via BEC with relative ease. They use email to phish unsuspecting employees at organizations. After a continued increase in BEC occurrences, such fraud declined in 2019 with 75 percent of organizations having been targets of BEC compared to 80 percent in 2018. Even though this is less than the last two years, it is still an elevated percentage. Organizations are concentrating on controlling BEC fraud by educating and training employees, as well as incorporating processes to validate payment requests internally. However, financial professionals do admit that incorporating BEC controls is challenging.

Each year since 2005, the Association for Financial Professionals® (AFP) has conducted its *Payments Fraud and Control Survey* to examine the trends in payments fraud in business-to-business (B2B) activities, the level of fraud activity, payment methods impacted by fraud and the extent of the impact from fraud. The survey also captures information on the strategies and controls being implemented by organizations and highlights the emergence of any new tactics which fraudsters are adopting.

Continuing these efforts, AFP conducted its 16th Annual *Payments Fraud and Control Survey* in January 2020. The survey generated 548 responses from corporate practitioners from organizations of varying sizes representing numerous industries. Their responses form the basis of this report and reflect data for 2019.

AFP thanks J.P. Morgan for its underwriting support of the *2020 AFP Payments Fraud and Control Survey*. Both the questionnaire design and the final report are the sole responsibility of AFP's Research Department. Information on the demographics of the respondents can be found at the end of the report.

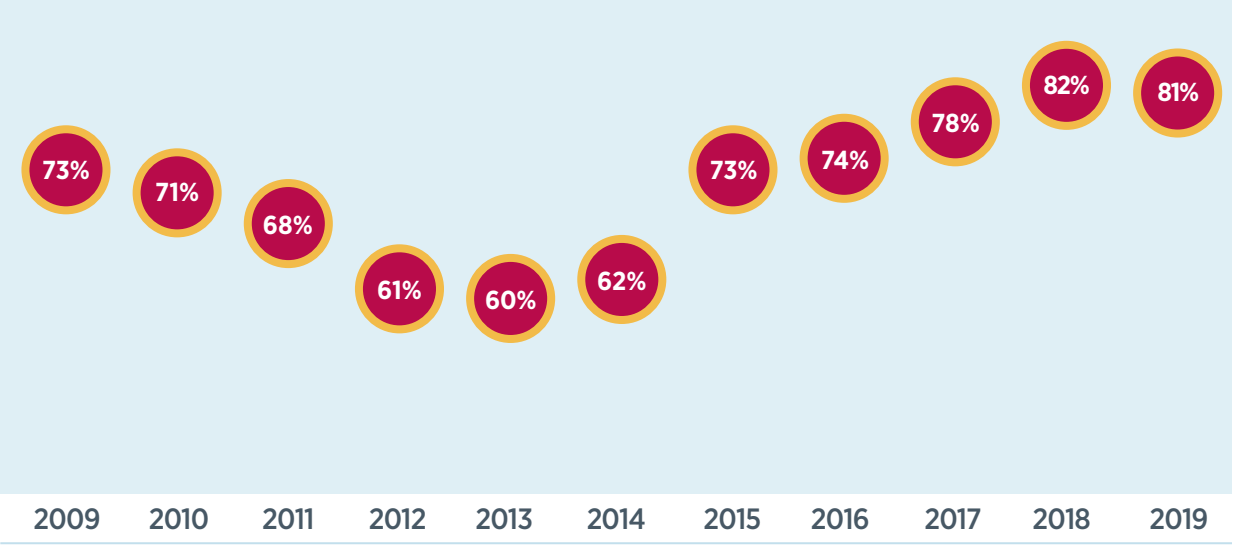
01 PAYMENTS FRAUD TRENDS

Over Eighty Percent of Organizations Report Being Targets of a Payments Fraud Attack

After a gradual decline in the percentage of organizations that experienced attempted or actual payments fraud from 2009 to 2013, there was an uptick in the share of companies that were victims of payments fraud attempts and attacks. In 2015, 73 percent of organizations were targets of payments fraud—a significant increase of 11 percentage points from 2014. That upward trend continued; 74 percent of financial professionals reported that their companies were victims of payments fraud in 2016, peaking in 2018 at 82 percent. In 2019, 81 percent of organizations were targets of attempted/actual payments fraud, still in the ballpark of the previous year's record-setting 82 percent.

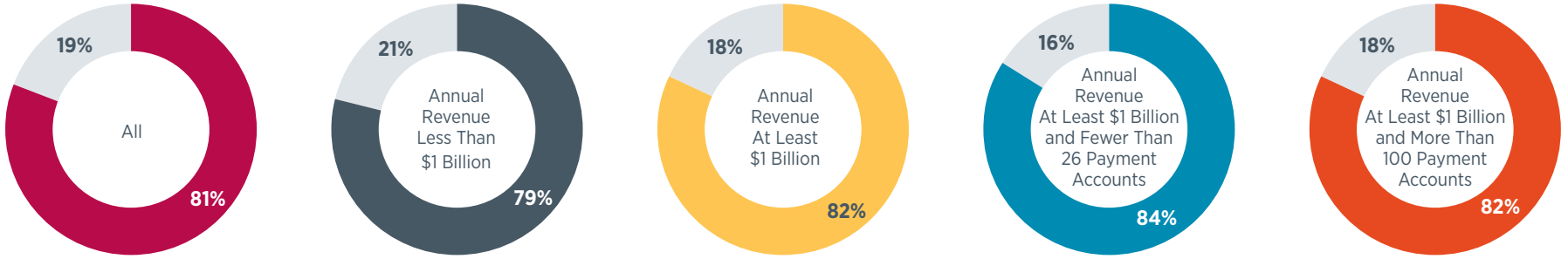
The fact that, overall, payments fraud is currently reported at over 80 percent of organizations is concerning. It suggests that fraudsters continue to succeed in their attempts to attack organizations' payment systems. It also signals that organizations cannot be complacent about the threats of payments fraud and is important that they take the necessary steps to make it as difficult as possible for criminals to succeed in their attacks.

Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud, 2009-2019



Larger organizations (with annual revenue of at least $1 billion) are slightly more susceptible to payments fraud attacks than are smaller ones (with annual revenue less than $1 billion): 82 percent compared to 79 percent. The three-percentage-point difference between the share of larger organizations and smaller ones that are victims of fraud is narrower than last year's figure of 18 percent.

Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud in 2019



Wire Fraud Activity Continues to Decline While ACH Fraud is on the Uptick

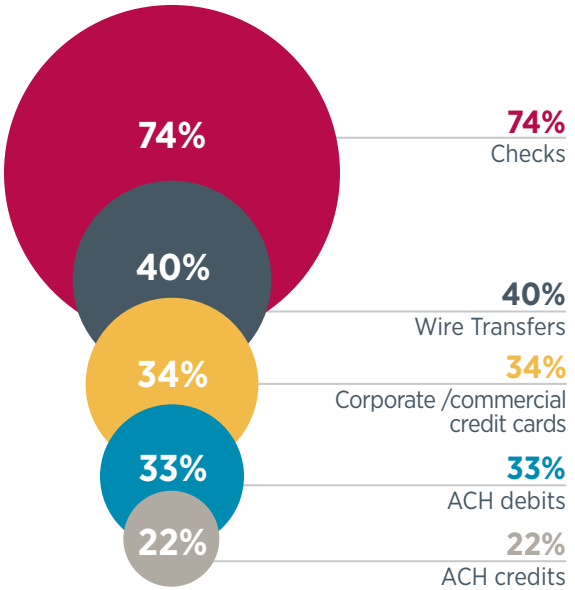
Checks and wire transfers continued to be the payment methods most impacted by fraud activity in 2019 (74 percent and 40 percent of organizations reporting such fraud, respectively). The percentage of financial professionals reporting check fraud activity increased four percentage points from 2018, while the share reporting fraud via wire transfers decreased five percentage points. Seventy percent of financial professionals reported that their organizations' check payments were subject to fraud attempts/attacks in 2018 while 74 percent report the same for 2019. Payments fraud via checks had been on the decline since 2010, but last year there was a slight uptick in check fraud activity. The fact that check fraud remains the most prevalent form of payments fraud is not surprising. Checks continue to be the payment method most often used by organizations. According to the *2019 AFP Electronic Payments Survey*, 42 percent of companies' B2B payments are made by check. Since checks are more prevalent as a payment method, they consequently are most often the targets of fraud.

The share of organizations that were victims of fraud attacks via wire transfers also decreased slightly—from 45 percent in 2018 to 40 percent in 2019. This is the third consecutive year in which wire fraud activity declined. Still, wire fraud activity continues to be high, especially considering the percentage of organizations experiencing such fraud was only in single digits until 2012.

This year's survey results reveal a slight increase in fraud activity via ACH credits while the incidence of ACH debit fraud was unchanged. Thirty-three percent of financial professionals report that their organizations' payments via ACH debits were subject to fraud attempts/attacks in 2019; that is identical to the survey results for 2018 and a five-percentage-point increase from 2017. Fraud activity via ACH credits increased two percentage points from 2018 to 22 percent in 2019.

These slightly elevated figures for ACH credits and ACH debits suggest that as fraudsters move away from targeting checks and wires, they are resorting to ACH transactions as vehicles for their scams. In efforts to avoid raising red flags and escape detection, perpetrators of such attacks are attempting to use payment methods previously not considered to be high risk.

Payment Methods that Were Targets of Attempted and/or Actual Payments Fraud in 2019
(Percent of Organizations)

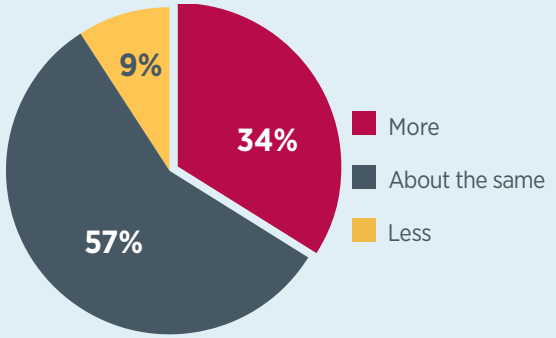


Faster payments **3%**
Virtual cards **3%**
eWallets **2%**

Instances of Payments Fraud is Unchanged for a Majority of Organizations

A majority of financial professionals (57 percent) reports that the incidence of payments fraud at their companies in 2019 was unchanged from that in 2018. Thirty-four percent of respondents whose organizations experienced payments fraud report that the number of incidents of fraud attempts increased in 2019 compared to 2018, whereas nine percent indicate it had decreased. These results are very similar to those in last year's survey. Organizations with annual revenue of at least $1 billion and with more than 100 payment accounts were more likely than companies with the same annual revenue but less than 26 payment accounts to have experienced an increase in fraud activity over the past year (38 percent compared to 32 percent).

Change in Incidence of Payments Fraud in 2019
(Percentage Distribution of Organizations that Experienced Attempted and/or Actual Payments Fraud)



Actual Financial Losses from Payments Fraud Not Extensive

Historically, actual financial losses from payments fraud attacks aren't extensive, and that continued to be the case in 2019. Fifty-four percent of respondents faced potential financial losses totaling less than $50,000 (or no loss) as a result of fraud activity in 2019. Twenty-three percent of financial professionals report there were no potential losses at their companies, while a full seven percent indicate that over $2 million may have been lost. However, loss of confidential and personnel information, while not a direct impact on the bottom-line, requires extensive efforts to resolve.

Actual direct financial losses were less than potential losses. Sixty-three percent of financial professionals report that their organizations did not incur a direct financial loss as a result of fraud activity, while 17 percent report a financial loss of less than $25,000.

Costs to manage, defend and/or clean up from fraud attacks were relatively low for most organizations that experienced such attacks. Forty-four percent of companies did not incur any expenses due to a fraud attempt and 38 percent spent less than $25,000 to defend against or clean up the fraud.

Potential Financial Loss from Attempted and/or Actual Payments Fraud in 2019

(Percentage Distribution of Organizations that Experienced Attempted and/or Actual Payments Fraud)

TOTAL DOLLAR AMOUNT	
Zero	23%
Up to $24,999	22%
$25,000-49,999	9%
$50,000-99,999	5%
$100,000-249,999	3%
$250,000-499,999	1%
$500,000-999,999	1%
$1,000,000-1,999,999	5%
$2,000,000 or more	7%

Actual Direct Financial Loss from Payments Fraud in 2019

TOTAL DOLLAR AMOUNT	
Zero	63%
Up to $24,999	17%
$25,000-49,999	6%
$50,000-99,999	4%
$100,000-249,999	5%
$250,000-499,999	3%
$500,000-999,999	1%
$1,000,000-1,999,999	1%
$2,000,000 or more	1%

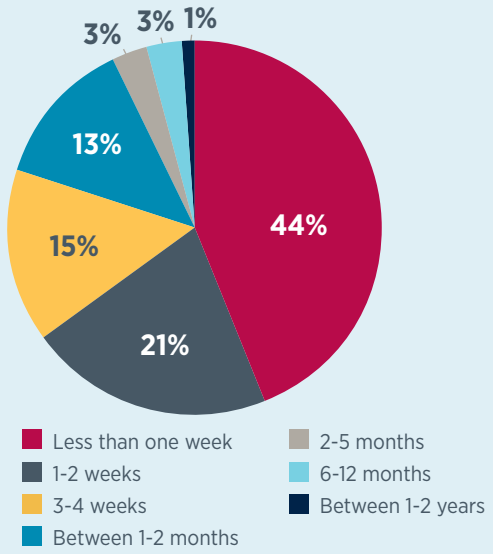
Costs to Manage/Defend/ Cleanup from Attempted and/or Actual Payments Fraud in 2019

TOTAL DOLLAR AMOUNT	
Zero	44%
Up to $24,999	38%
$25,000-49,999	6%
$50,000-99,999	3%
$100,000-249,999	3%
$250,000-499,999	2%
$500,000-999,999	2%
$1,000,000-1,999,999	1%
$2,000,000 or more	1%

Two-Thirds of Organizations Uncovered Fraud Attack within Two Weeks

Of those organizations that were victims of fraud attacks in 2019, 44 percent detected the fraudulent activity in less than one week. Thirty-six percent uncovered the fraud attack within one-to-four weeks; a mere one percent took one to two years before realizing they had been targeted. There is room for improvement in organizations' ability to detect occurrences of fraud promptly. If fraud is not detected within the first few days, the chances of a recovery from the fraud are slim.

Time Taken to Discover Fraud
(Percentage Distribution of Organizations)



Business Email Compromise (BEC) a Key Source Responsible for Attempted/Actual Payments Fraud Attempts

In 2019, the majority of payments fraud attempts/attacks originated from Business Email Compromise (BEC). Sixty-one percent of companies that experienced attempted or actual payments fraud in 2019 did so as a result of BEC. 2019 was the first year that BEC topped the list of "sources" of fraud attempts, and it is concerning how widespread this type of attack has become.

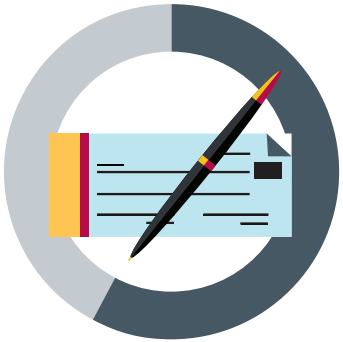
The second most-common source of payments fraud in 2019 was an external source or individual (e.g., forged check, stolen card); 58 percent of financial professionals report that payments fraud at their companies was the result of actions by an individual outside the organization.

Other sources of payments fraud include third parties or outsourcers such as vendors (experienced by 26 percent of organizations—a four percentage-point increase from 2018).

Fraudsters are aware of the red flags to which organizations are alerting their employees, as well as the training companies are providing to ensure that treasury and finance staff can detect phishing attempts. The continued occurrence of "sophisticated" fraud such as account takeovers suggests that fraud mitigation—in addition to robust internal controls—should also focus on network security and how to prevent external parties from gaining access to internal systems.

Sources of Attempted and/or Actual Payments Fraud in 2019
(Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud)

61%
Business Email Compromise
(BEC Fraud)



58%
Outside Individual
(e.g., forged checks, stolen card)

26%
Third-party or outsourcer
(e.g., vendor, professional services provider, business trading partner)

02 BUSINESS EMAIL COMPROMISE

What Is Business Email Compromise?

Business Email Compromise (BEC) is a sophisticated scam targeting businesses and referred to as Email Account Compromise (EAC) when targeting individuals that are otherwise responsible for payments. The scam is frequently carried out when a fraudster compromises legitimate business email accounts through social engineering or computer intrusion techniques (e.g., phishing) in order to conduct unauthorized transfers of funds.

Most victims of BEC/EAC note that wire transfers are a common method of transferring funds for business purposes; however, some also report that checks are a common payment method targeted by BEC. Fraudsters will use the method most commonly associated with their potential victim's normal business practices. This scam has evolved to include the compromising of legitimate business email accounts, requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees, and may not always be associated with a request for transfers of funds.

Statistical Data

The BEC/EAC scam continues to grow and evolve, targeting small, medium and large businesses as well as personal transactions. Between May 2018 and June 2019, there was a 100% increase in identified global exposed dollar losses (includes actual and attempted losses in US dollars). The scam has been reported in all 50 states and in 177 countries. According to the Internet Crime Complaint Center (IC3), the growing awareness of these ruses is part of the reason that BEC has increased.

The following BEC/EAC statistics were reported in victim complaints where a country was identified to the IC3 from June 2016 to July 2019:[1]

Domestic and International Incidents
166,349

Domestic and International exposed dollar loss
$26 billion

Total U.S. financial recipients
32,367

Total U.S. financial recipient exposed dollar loss
$3.5 billion

Total non-U.S. financial recipients
14,719

Total non-U.S. financial recipient exposed dollar loss
$4.8 billion

Note: Definition and Statistical data shared is from The Federal Bureau of Investigation (FBI)

[1]The Federal Bureau of Investigation (FBI)

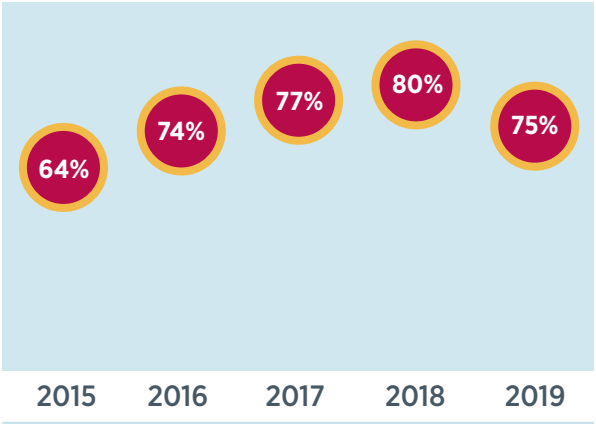
Business Email Compromise (BEC) At Its Lowest Since 2016

Fraud originating from BEC has decreased since 2018, and its incidence in 2019 was at its lowest level since 2016. The share of companies impacted by BEC in 2019 was 75 percent, a decline from 80 percent in 2018—which was a record high since AFP began tracking instances of BEC in 2016 (covering activity for 2015). The decline may signal that companies' efforts to prevent BEC are finally starting to pay off.

Eighty percent of companies have been actively training employees on how to detect fraudulent emails and thus better control instances of BEC (please see page 17). Despite the awareness and training companies are providing employees on BEC, the percentage of those organizations experiencing BEC attacks remains elevated at 75 percent. Perpetrators of BEC attacks have become more sophisticated in their techniques, and the emails appear to be authentic resulting in organizations falling victim to these attacks.

A large majority of organizations reports 25 or fewer instances of BEC fraud activity occur annually, and approximately 10 to 20 percent report 26-100 instances of BEC fraud. Respondents indicate that their organizations are often victims of emails from fraudsters pretending to be senior executives directing employees to transfer funds into fraudsters' accounts (17 percent report that this occurred between 26 and 100 times annually). Other types of spoofed emails include vendors receiving fraudulent emails from company's employees and emails from company's employees requesting a change in payroll bank account information.

Percent of Organizations that Experienced Business Email Compromise (BEC), 2015-2019



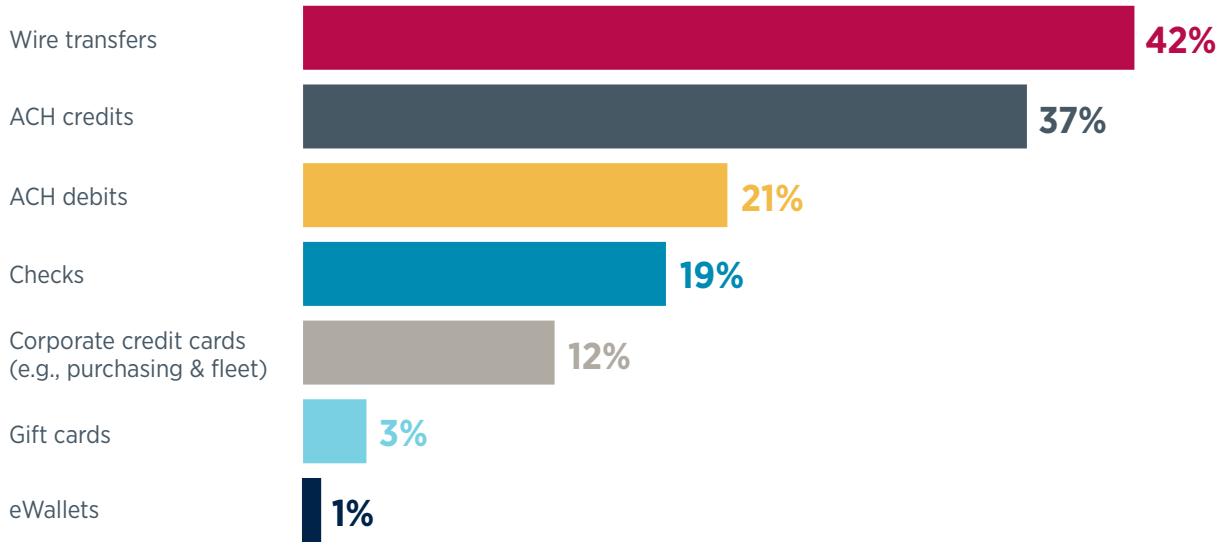
Most Prevalent Types of Business Email Compromise
(Percentage Distribution of Organizations Reporting Payments Fraud via BEC)

	25 OR FEWER INSTANCES ANNUALLY	26-100 INSTANCES ANNUALLY	101-200 INSTANCES ANNUALLY	200+ INSTANCES ANNUALLY
Emails from fraudsters impersonating as vendors (using vendors' actual but hacked email addresses) directing transfers based on real invoices to the fraudster's accounts	85%	12%	2%	1%
Emails from other third parties requesting changes of bank accounts, payments instructions, etc.	85%	11%	2%	2%
Emails from fraudsters pretending to be senior executives using spoofed email domains directing finance personnel to transfer funds to the fraudsters' accounts	80%	17%	1%	1%
Other: -Soliciting emails -Vendors receiving fake emails from company's employees -Fraudulent emails from employees requesting to change payroll bank account information	80%	20%	–	–

The Gap Between Wire Transfers and ACH Credits as the Prime Targets for Business Email Compromise Scams Continues to Narrow

The percentage of organizations that experienced payments fraud in 2019 via BEC impacting wire transfers decreased slightly—from 43 percent in 2018 to 42 percent. The 2019 figure is also a substantial decrease from the 54 percent in 2017 and the 60 percent in 2016. Although wire transfers remained the most favored payment method targeted for fraud via BEC, they were closely followed by incidence of ACH credit fraud: 37 percent of respondents report fraudsters accessed ACH credits using BEC in 2019—an increase from the 33 percent in last year's survey. ACH credits are only five percentage points behind wire transfers as the prime targets for BEC fraud. The percentage of financial professionals reporting that BEC compromised their organizations' check payments declined slightly—from 20 percent in 2018 to 19 percent in 2019. The shift to targeting ACH transactions through BEC further is likely because ACH is an easier touchpoint for those committing fraud, while there is greater sensitivity with wire transfers as they are frequently scrutinized.

Payments Methods Impacted by Business Email Compromise in 2019
(Percent of Organizations)



Financial Impact of Business Email Compromise Drops Significantly from Past Years

Organizations have been actively trying to mitigate BEC in several ways including end-user education and training, new company policies on any changes to existing bank accounts, and using call-back features or some other out-of-band verification method to confirm ACH and/or wire transfer requests. The percentage of financial professionals reporting that their companies were victims of BEC is currently the lowest it has been since 2016, and organizations are highly focused on mitigating such attacks.

The actual financial loss incurred at companies as a result of these scams is also on the decline. In 2018, 54 percent of organizations were impacted by a financial loss as a result of BEC, higher than the 46 percent of organizations that were impacted in 2017. However, in 2019, only 38 percent of organizations suffered a financial loss due to BEC. This 16-percentage-point decline is significant and is the lowest figure since AFP started tracking BEC fraud in 2015.

Thirty-one percent of smaller organizations (annual revenue less than $1 billion) incurred losses from BEC—a share also down from that reported in 2018—and 41 percent of larger organizations (annual revenue of at least $1 billion) had losses as a result of BEC, also a 16-percentage-point decrease from last year. These numbers are consistent with the *2019 Payments Fraud Survey* (data for 2018) in which larger organizations were also more likely to have suffered losses.

Estimated Total Dollar Loss to Organizations from BEC in 2019
(Percentage Distribution of Organizations that Experienced Payments Fraud via BEC)

	ALL	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS
No Loss	62%	69%	59%	66%	43%
Up to $24,999	17%	16%	17%	16%	17%
$25,000-49,999	4%	1%	7%	9%	6%
$50,000-99,999	6%	9%	5%	3%	6%
$100,000-249,999	4%	4%	3%	1%	9%
$250,000 - $499,999	3%	1%	4%	1%	9%
$500,000 - $999,999	1%	–	1%	1%	3%
$1,000,000 - $1,999,999	2%	1%	3%	1%	9%

Fifty-seven percent of organizations (annual revenue of at least $1 billion) and with more than 100 payment accounts were financially impacted by BEC in 2019 while about a third (34 percent) of companies with comparable annual revenue but fewer payment accounts were less affected. The majority of respondents who did report that their companies incurred a loss reported a loss of less than $50,000. A larger share of organizations with annual revenue of at least $1 billion and more than 100 payment accounts experienced a loss of more than $1,000,000. This indicates that fraudsters target larger organizations in order to steal larger amounts of money.

There are, of course, other "losses" that can result from BEC. If a fraud attack via BEC exposes personal and confidential information, the nonfinancial damages—while difficult to quantify—can be severe.

Organizations' Accounts Payable Departments Most Vulnerable to Being Targeted by BEC Fraud

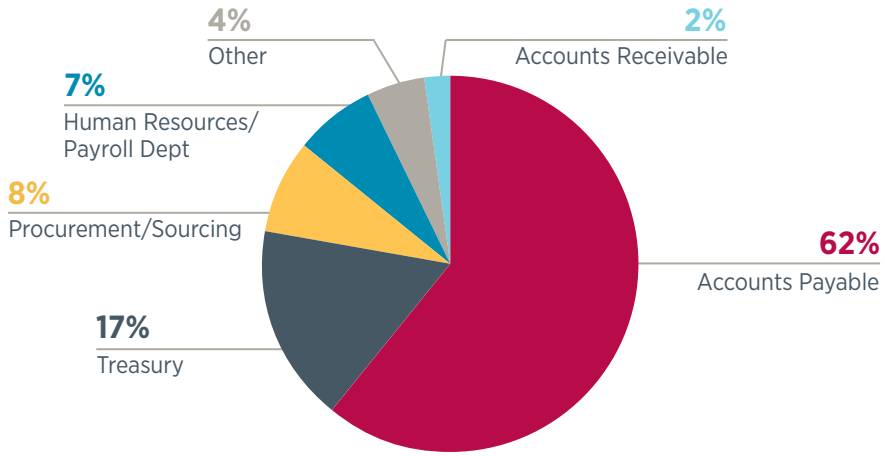
Business Email Compromise scams continue to morph into new shapes and forms, and fraudsters are using BEC to target various departments within organizations. Sixty-two percent of respondents report that their accounts payable department was the most vulnerable business unit targeted. The second-most vulnerable department being targeted by BEC fraud was the treasury department (17 percent).

Twenty percent of respondents from larger organizations—with annual revenue of at least $1 billion and more than 100 payment accounts—indicate that their procurement/sourcing department was most vulnerable to fraud; only six percent report that the treasury department was the most targeted function. But the numbers shift when it comes to organizations with annual revenue of less than $1 billion; nearly a fourth of respondents from those companies note that their organization's treasury department was the most vulnerable (23 percent), while four percent report that the department most impacted by fraud was procurement/sourcing.

Other departments within organizations reported to be the most vulnerable include:

- Human Resources
- Operations
- Sales
- Marketing
- Accounting
- Executive
- Management

Departments Most Vulnerable to Being Targeted by BEC Fraud
(Percentage Distribution of Organizations)



03 PAYMENTS FRAUD CONTROLS

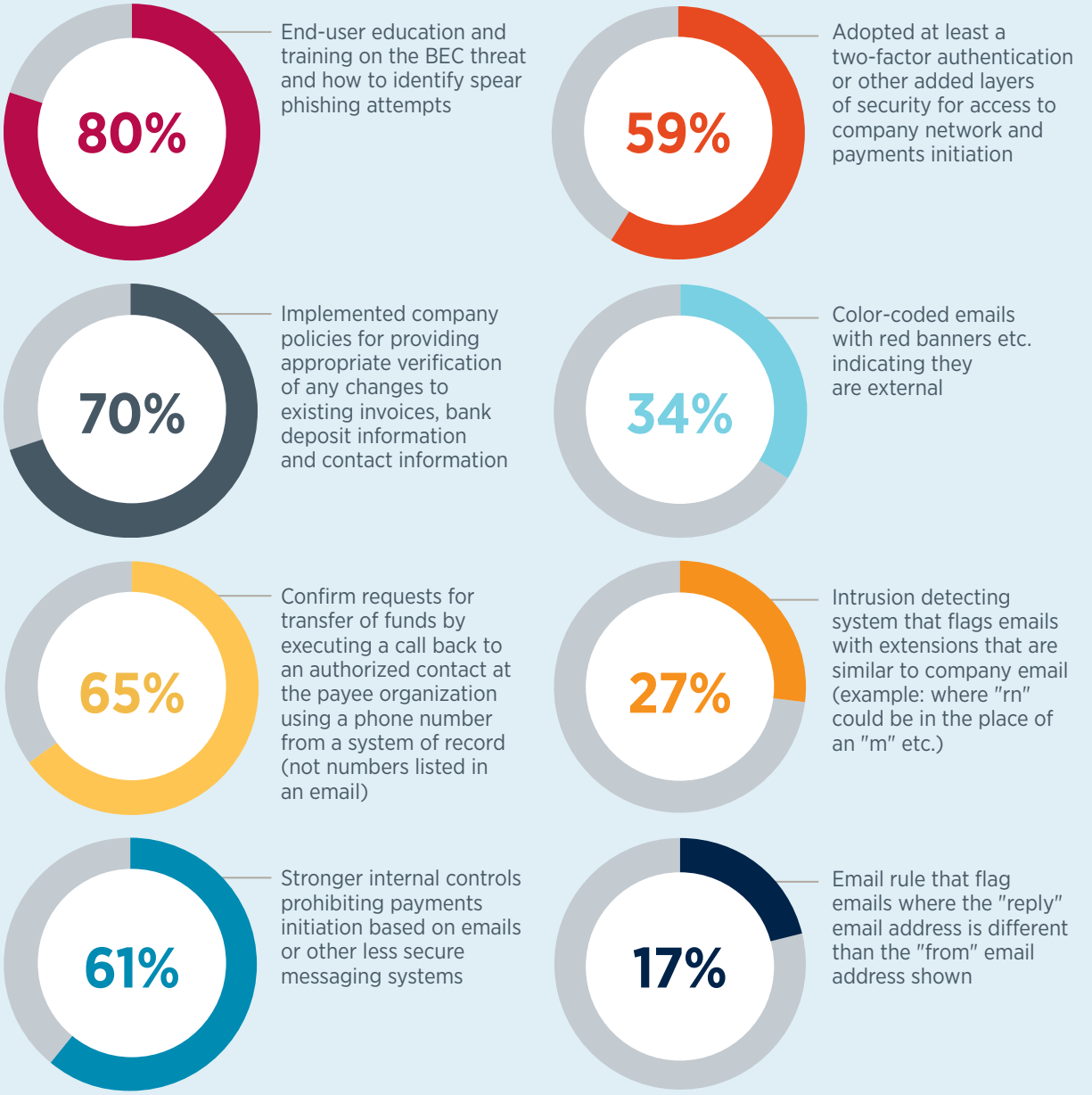
Education and Training Key in Controlling BEC

As mentioned earlier, Business Email Compromise is a popular method used by fraudsters to infiltrate an organization's financial systems. Successful attacks can result in organizations being adversely impacted financially; organizations' confidential information may also be comprised. **Eighty percent of financial professionals believe that educating employees on the threat of BEC and how to identify spear phishing attempts is an important element in efforts to control BEC.**

Other controls being implemented to prevent and contain BEC include:

- **Implementing company policies for providing appropriate verification of any changes to existing invoices, bank deposit information and contact information** (cited by 70 percent of respondents)
- **Confirming requests for transfer of funds by executing a call back to an authorized contact at the payee organization using a phone number from a system of record** (not numbers listed in an email) (65 percent)
- **Instituting strong internal controls that prohibit payments initiation based on emails or other less secure messaging systems** (61 percent)
- **Adopting at least a two-factor authentication or other added layers of security for access to company network and payments initiation** (59 percent)

Internal Controls Methods Implemented to Prevent BEC Fraud
(Percent of Organizations)

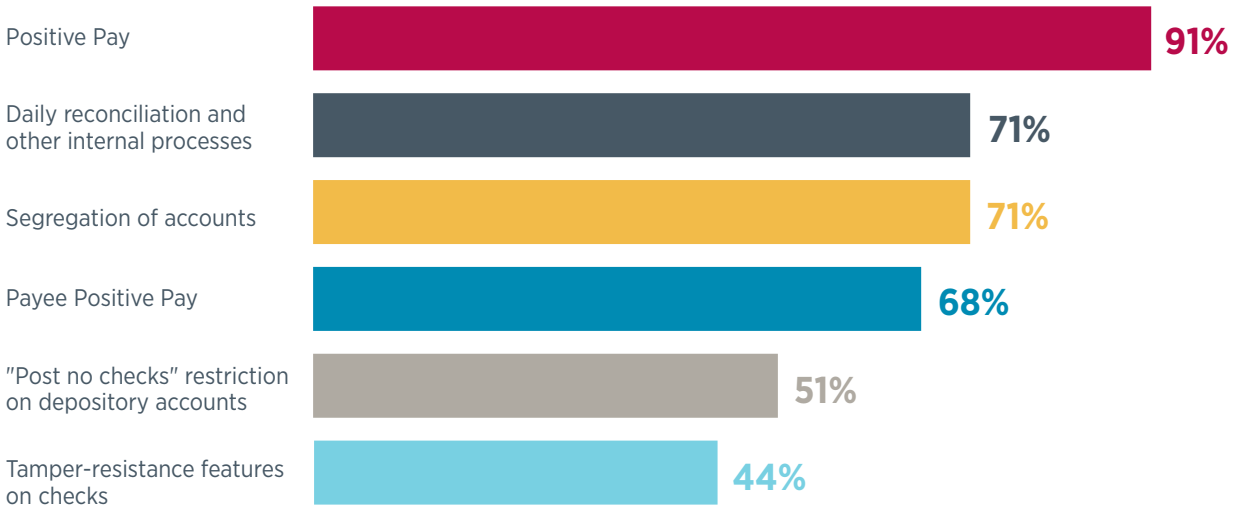


Positive Pay Most Frequently Used Procedure to Protect Against Check Fraud

Positive Pay continues to be the method most often used by organizations to guard against check fraud. This approach is used by 91 percent of organizations—slightly higher than the 88 percent reported for 2018. Protective measures such as Positive Pay are not generally included in the payment offering options from organizations' financial institution partners; Positive Pay is, rather an added service for which the bank charges an extra fee. This may explain the fluctuating use of Positive Pay in previous years. Seventy-one percent of organizations resort to segregation of accounts, and equal shares use daily reconciliations and other internal processes to combat and mitigate check fraud.

- **Payee Positive Pay** (cited by 68 percent of respondents)
- **"Post no checks" restriction on depository accounts** (51 percent)

Fraud Control Procedures and Services Used to Protect Against Check Fraud
(Percent of Organizations that Experienced At Least One Attempt of Check Fraud)



Effective Security Features on Checks

Seventy-three percent of organizations that use tamper-resistant features believe the VOID pantograph feature—i.e., the word VOID appears if check is scanned or copied—is effective in preventing check fraud. Security/safety paper (stains appear if checks are tampered with) is considered effective by 57 percent of financial professionals.

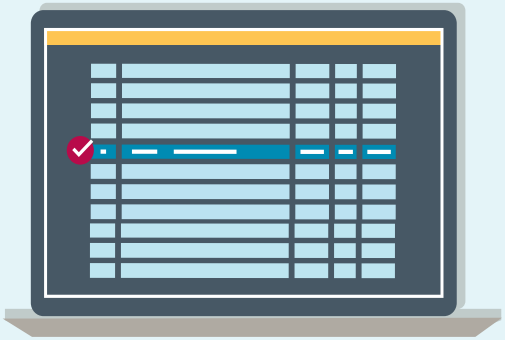
Defending Against Attacks on Security Credentials

In trying to protect their payment methods from attacks on security credentials, a large majority of organizations (72 percent) performs daily reconciliations. Over half—55 percent—keep internal processes the same for all types of payments (paper-based, electronic and virtual) and 48 percent are proactive and planning for disaster recovery, including the ability to continue with strong controls.

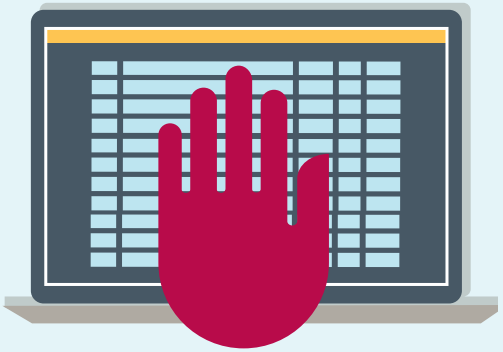
Controls Being Used to Prevent or Mitigate ACH Fraud

In 2019, 33 percent of organizations were victims of ACH debit fraud and 22 percent experienced ACH credit fraud. These figures are very similar to those reported for 2018. To minimize the occurrence of ACH fraud, organizations are implementing the following measures:

Reconcile accounts daily to identify and return unauthorized ACH debits, cited by **77 percent of respondents for 2019**—an increase from 65 percent in 2018



Block all ACH debits except on a single account set up with ACH debit filter/ACH Positive Pay (**69 percent**)—an increase from 63 percent in 2018



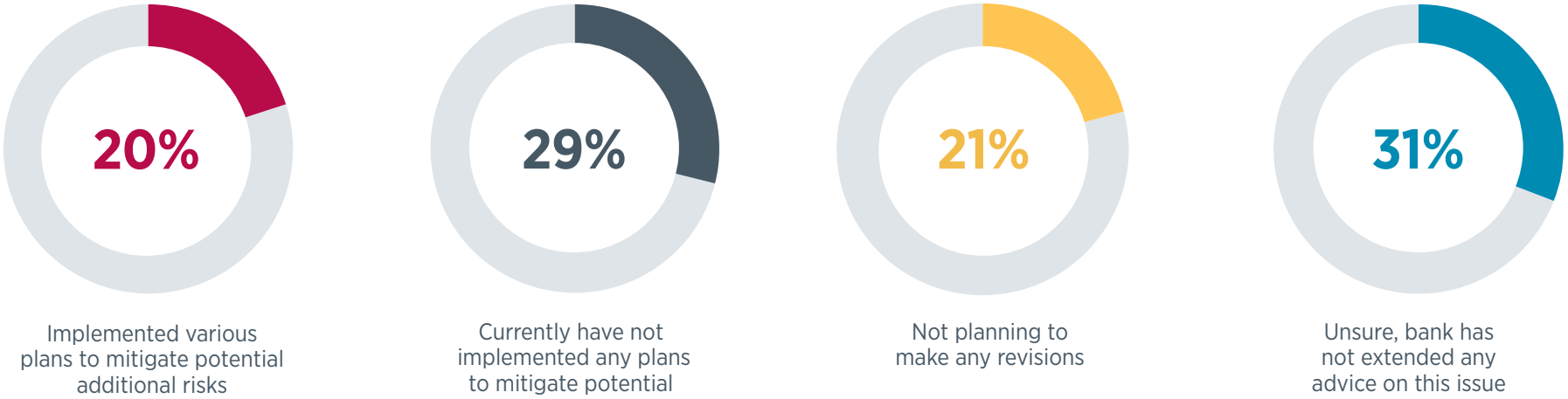
Block ACH debits on all accounts (**44 percent**)—an increase from 37 percent in 2018

Same Day ACH Presents Additional Risks for Both Credit and Debit Transactions

While Same-Day ACH is operational for both credit and debit transactions, only 20 percent of organizations have implemented plans to mitigate potential additional risks. Twenty-one percent of organizations are not taking any steps to prepare for and mitigate potential additional risks that might occur (a decrease from the 30 percent that reported the same in last year's survey) and 31 percent are unsure as their banking partners have not extended any advice.

There are companies that, while they have not yet implemented any plans to safeguard against and mitigate potential risks, are in the process of doing so (29 percent). As ACH usage becomes more widespread, the lack of planning for additional risks is an area of concern.

Organizations' Preparedness to Mitigate Potential Additional Risks with Same-Day ACH for Both Credit and Debit Transactions
(Percentage Distribution of Organizations that Experienced At Least One Attempt of ACH Fraud)



A Majority of Organizations Have a Fraud Policy

A fraud policy defines the responsibilities of an organization's management and staff in establishing and maintaining internal processes and fraud controls. Additionally, it defines responsibilities and processes when fraud is suspected or detected. A fraud policy communicates a company's position and the processes it has established to deal with fraud. Such a policy is part of an overall plan of fraud detection and prevention. A fraud policy can raise awareness, but awareness but can also set a company management's tone toward both internal and external fraud.

The time immediately following the discovery or allegation of fraud can be challenging. Having a document in place which identifies the parties, responsibilities and procedures to be followed can guide all those parties, departments and individuals involved in making the right decisions. This is important in ensuring the proper steps will be taken to deal with the individuals involved, as well as the preservation of evidence.

An organization's fraud policy should include:

- Definition of actions determined to be considered fraudulent
- Identification of parties and responsibilities for overall fraud incident management
- Formal procedures to be followed
- Notification that suspected fraud will be investigated and potentially prosecuted

The potential cons of a fraud policy are:

- Management's position on fraud is not stated
- Fraudulent circumstances will be unidentified
- Personnel do not know how to respond to any incidents of payments fraud

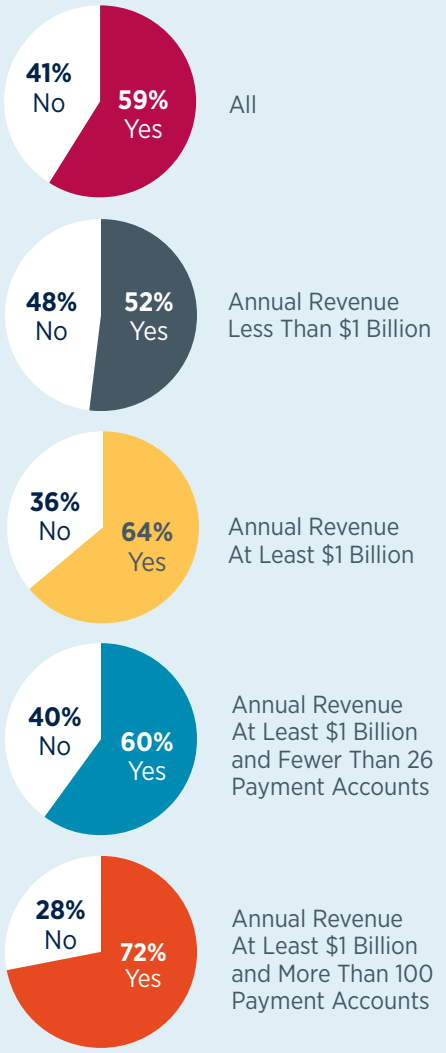
Fifty-nine percent of respondents confirm that their organization has a fraud policy. Large organizations—those with annual revenue of at least $1 billion—are more likely to have fraud policies than are smaller organizations with revenue less than $1 billion (64 percent compared to 52 percent).

Treasury functions at 47 percent of organizations are responsible for the fraud policy, while risk departments at 36 percent of companies own it. Other departments that are responsible for the fraud policy are:

- **Accounts Payable or Accounts Receivables** (cited by 21 percent of respondents)
- **Procurement** (10 percent)
- **Human Resources** (7 percent)
- **Other includes: Internal Audit, Legal, IT, Compliance, Cybersecurity, Controllers** (26 percent)

Even among those organizations that do have a fraud policy, 25 percent do not test the policy to ensure it is detecting fraud as it should. Of those that do test their policies, 55 percent do so annually. One-third does so more frequently, with 10 percent of companies testing bi-annually and 22 percent doing so every quarter. The remaining 13 percent include many that are unsure about the frequency of testing of their fraud policy. A few respondents indicate that testing is carried out sporadically and when needed.

Percentage of Organizations That Have a Fraud Policy
(Percentage Distribution of Organizations



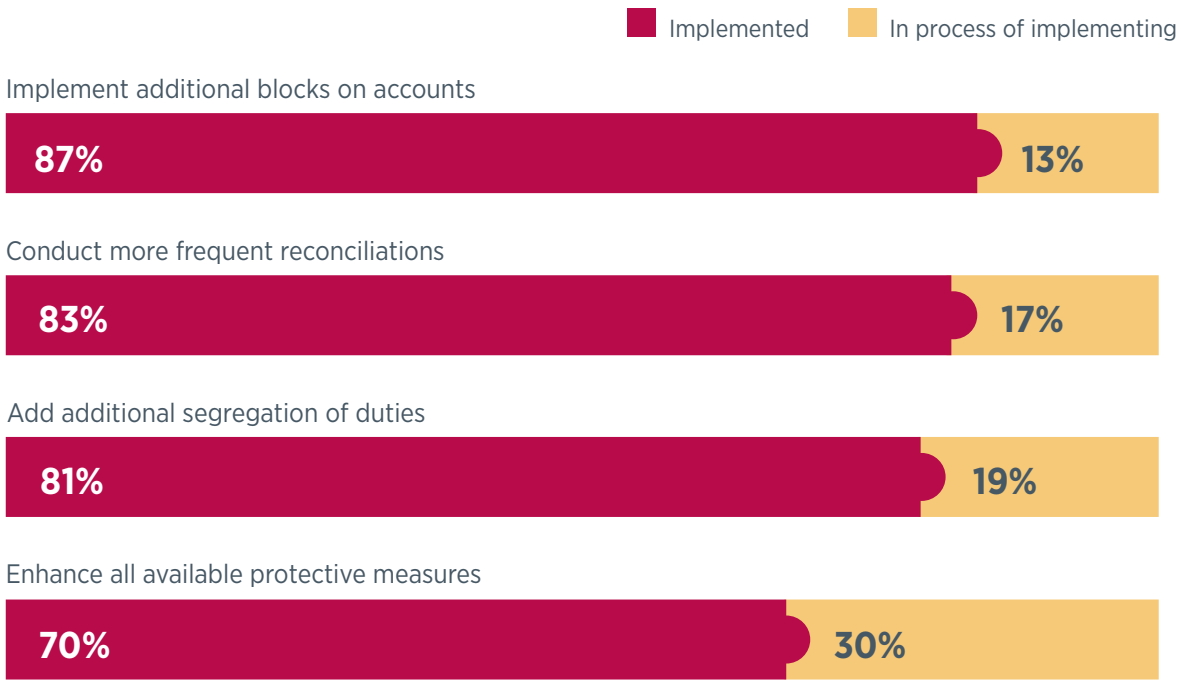
Additional Blocks on Accounts is the Most Implemented Safeguard Against Fraud

Eighty-seven percent of respondents report that their organizations have implemented additional blocks on accounts to safeguard against fraud; 13 percent of companies are in the process of implementing the blocks. The second-most frequent action that has been implemented to protect organizations against fraud is to conduct more frequent reconciliations (cited by 83 percent of respondents). Interestingly, 90 percent of larger organizations with annual revenue of at least $1 billion and more than 100 payment accounts have already implemented additional segregation of duties, but only 67 percent of them have implemented conducting more frequent reconciliations.

Additional blocks allow an organization to:

- Specify which companies are authorized to post ACH debits, rejecting those not authorized
- Set dollar limit ceilings
- Transactions rejected that do not meet the specified blocking parameters

Revisions Implemented/Are Being Implemented to Safeguard Against Fraud
(Percentage Distribution of Organizations)



Organizations are Quick to Act on Potential Fraud When Alerted

Nearly one-half of organizations (48 percent) has received a call from their payment partners/vendors alerting them to a potential fraud occurrence. This share increases to 63 percent for organizations with annual revenue of at least $1 billion and more than 100 payment accounts. The higher a company's revenue and the more payment accounts it has, the more attractive the target.

Of those organizations that have received a call alerting them to a potential fraud occurrence, a large majority (86 percent) has acted on the advice provided by their payment partners/vendors which prevented the fraud. Ninety-two percent of organizations with annual revenue of at least $1 billion and more than 100 payment accounts acted on the advice provided and prevented the fraud from occurring. Since more fraud attempts are targeted to larger organizations, it is not surprising that such companies would have more defined processes and therefore be more prepared to act on fraud and thus take it more seriously than other organizations.

Actions Taken Once Receiving a Call Alerting Us to Potential Fraud Occurrence
(Percentage Distribution of Organizations)

86%
Acted on the advice provided by payment partner/vendor and **prevented the fraud**

1% **Did not act** on the advice and the payment **did result in a fraud occurrence**

10% **Did not act** on the advice and the payment **did not result in fraud**

3% Other

Note: In some "other" cases, companies acted on advice of their payment partner, but it was not fraud.

Challenge to Implement Fraud Controls

It is imperative that organizations have controls in place that can adequately safeguard various payment methods from fraud attacks. Implementing fraud controls requires substantial investment of financial resources as well as people resources. Controls need to be able to efficiently prevent occurrences of fraud.

Fifty-two percent of respondents believe that the implementation of fraud controls to contain BEC is challenging, with 12 percent indicating it is very challenging to implement. Nearly a third of respondents (31 percent) reports that implementing controls to prevent card fraud is challenging. Other controls to prevent wire fraud, check fraud and ACH fraud are significantly easier to implement.

Challenge to Implement Fraud Controls
(Percentage Distribution of Respondents)

	VERY CHALLENGING TO IMPLEMENT 5	4	LESS CHALLENGING TO IMPLEMENT 3	2	NOT AT ALL CHALLENGING TO IMPLEMENT 1
Business Email Compromise controls	12%	40%	26%	16%	6%
Card fraud controls	7%	24%	39%	20%	10%
Wire fraud controls	3%	13%	27%	29%	28%
Check fraud controls	3%	12%	22%	23%	40%
ACH fraud controls	2%	9%	27%	26%	36%

Validating Fraud Controls

Validating fraud controls include the following:

- Annual review, and management approval, of organization's fraud policy
- Verification of processes and/or procedures in an organization's fraud policy
- Testing, to the extent appropriate, the fraud policy procedures through a practical exercise

It would be a good practice if organizations validated their fraud controls regularly: by validating fraud controls, companies are making a commitment to manage their exposure to payments fraud. It also assists in verifying the effectiveness of processes and procedures. Additionally, it also increases employee and vendor awareness of the company's position on fraud and fraudulent activities.

Costs involved in validating fraud controls often prevent organizations from doing so. Senior management at some organizations do not believe the process of validating fraud controls is necessary and so do not make such validation a high priority.

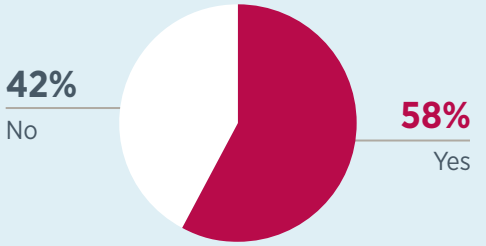
A majority of organizations currently validate their fraud controls. Larger organizations with annual revenue at least $1 billion are more likely to validate fraud controls than are their smaller counterparts.

Payment Partners/Vendors Evidencing Security Policies and Controls as Part of Regular Diligence

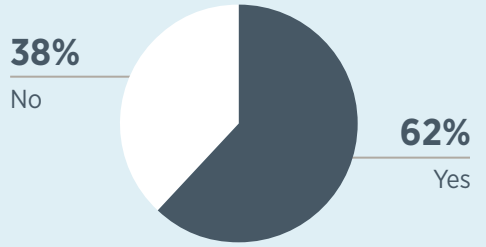
Evidencing security policies includes providing a compliance certificate or some other written evidence. It is a good practice as it confirms employees, vendors and suppliers are aware of a company's fraud policy. Additionally, it acknowledges the policy is undergoing some type of regular validation and highlights a company's low tolerance for fraud.

Financial professionals are extremely aware of the frequency of payments fraud and are proactively implementing policies and controls to minimize the instances of fraud attacks in order to be able to detect early warning signs. At the same time, less than half are evidencing security policies and controls as part of due diligence (46 percent).

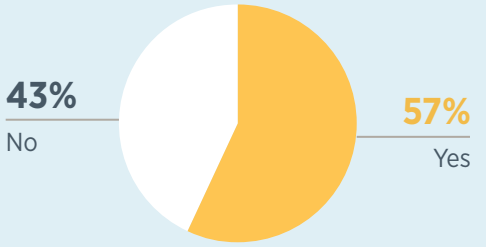
Validated Fraud Controls Implemented to Mitigate BEC Fraud
(Percentage Distribution of Organizations)



Validated Fraud Controls Implemented to Mitigate Check Fraud
(Percentage Distribution of Organizations)



Validated Fraud Controls Implemented to Mitigate ACH Fraud
(Percentage Distribution of Organizations)



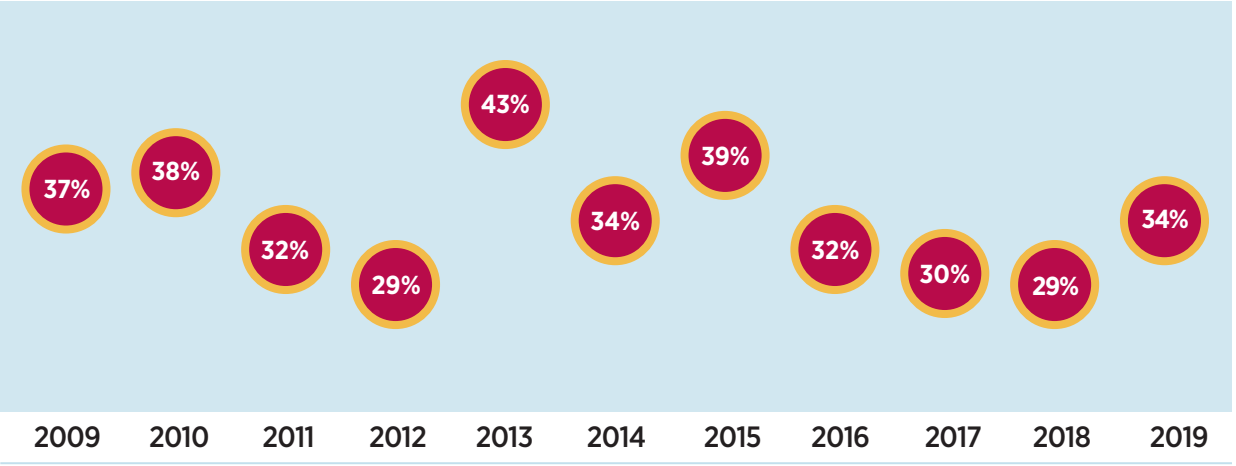
04 CORPORATE/COMMERCIAL CREDIT CARDS

Corporate/Commercial Credit Cards Are More Prone to Payments Fraud Attacks

Thirty-four percent of financial professionals report that their organizations were subject to corporate/commercial credit card fraud in 2019, a five-percentage-point increase from 2018.

The types of corporate/commercial cards most prone to fraud are Travel & Entertainment (T&E) cards (54 percent) and purchasing cards (51 percent). These figures are only slightly lower than those for 2018 (57 percent and 54 percent, respectively). Only 11 percent of respondents indicate that their organizations actually suffered a financial loss due to corporate/commercial card fraud. The main reason for the loss suffered by these companies was fraudulent credit card charges made by a third party (60 percent).

Percent of Organizations that Experienced Payments Fraud through Corporate/Commercial Credit/Debit Cards, 2009-2019



Major Concerns Regarding Fraud

Card-not-present—or online—fraud is reported to be a major concern by nearly three-fourths of respondents (72 percent). Stolen Credit/Debit cards is the second-most cited concern at 59 percent. Organizations with annual revenue of at least $1 billion and more than 100 payment accounts are more concerned than others about Stolen Credit/Debit cards, with 70 percent of respondents citing it as a major concern.

Other concerns regarding fraud reported include:

- Employee abuse
- Cash advances on Purchasing cards
- Cards used for personal use

Corporate credit card fraud saw a steady decline from 2009-2012, and then there was a substantial uptick in card fraud in 2013. Since then the percentage of organizations experiencing this type of fraud has fluctuated, with an increase in some years and in others a decrease. The concerns and issues surrounding credit card fraud have been fairly consistent over the years. Travel & Entertainment cards and purchasing cards are still the most vulnerable to fraud. At a majority of companies, the primary cause of card fraud is fraudulent charges made by a third party, again similar to past years. Financial professionals are continuing to grapple with card fraud and have not, as yet, had much success in preventing instances of such fraud.

CONCLUSION

Results from the *2020 AFP Payments Fraud and Control Survey* reveal that payments fraud activity is unlikely to abate any time soon. Scammers are becoming increasingly innovative with their repeated success in circumventing controls and their ability to infiltrate organizations' payments systems. They are relentless in their efforts. In 2018, the share of companies experiencing payments fraud was at a record level of 82 percent; in 2019 the share experiencing payments fraud declined by only one percentage point. That slight decline was despite companies having implemented greater controls to protect their payment methods, as well as their senior management being very cognizant of the possibility that their organization could become a victim of malicious attacks.

While any financial loss experienced as a consequence of a payments fraud attack may be insignificant and have little impact on an organization's bottom-line, the sheer inconvenience of an attack can be extensive. Any loss of confidential information—bank account information, vendor data, customer information, etc.—from payments fraud requires that companies manage and clean up from the fraud. In addition, any loss of confidential information can impact an organization's reputation and, depending on the industry, there is the added concern of regulatory risk.

Unfortunately, payments fraud attacks are the "new normal," and advancements in technology have opened the doors for fraudsters. Larger organizations with a large number of payments transacted are able to invest extensively in methods to safeguard their organization. Still, if criminals are able to successfully hack even a small share of payments, these fraudsters will benefit greatly: the risk may be worth the reward. Therefore, they persist regardless of the controls and barriers they face.

Results from the *2020 AFP Payments Fraud and Control Survey* reveal:

- Business Email Compromise was the most-often reported source of payments fraud attacks, with 61 percent of organizations reporting BEC as the source of attacks.
- Over 80 percent of organizations were targets of a payments fraud attack in 2019, the second-highest percentage since 2009.
- Although checks and wires are frequent targets of payments fraud, the incidence of attacks on these payment methods is declining. ACH payment methods appear to be of the most interest to fraudsters.
- Financial leaders at 80 percent of organizations are educating and training employees on BEC so the fraud is detected more efficiently.
- Over 60 percent of respondents report that BEC controls are challenging to implement.
- About one-third of companies reports experiencing more instances of payments fraud in 2019 than in 2018.
- Three-fourths of companies report being victims of BEC; while this is a smaller share than that reported in 2018 and 2017, occurrences of this type of payments fraud is still significant.
- Nearly 60 percent of organizations have a fraud policy in place.
- Corporate/commercial credit card fraud increased five percentage points from 2018 to 2019.

05 DEMOGRAPHICS OF SURVEY RESPONDENTS

About Respondents

In January 2020, the Research Department of the Association for Financial Professionals® (AFP) surveyed nearly 8,000 of its corporate practitioner members and prospects. The survey was sent to corporate practitioners with the following job titles: Treasurer, Assistant Treasurer, Director of Treasury, Treasury Manager, Director of Treasury and Finance, Senior Treasury Analyst, Cash Manager and Vice President of Treasury. A total of 425 responses were received and are the basis of the survey results.

AFP thanks J.P. Morgan for underwriting the *2020 AFP Payments Fraud and Control Survey*. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibilities of the AFP Research Department. The following tables provide a profile of the survey respondents, including payment types used and accepted.

Methods Used to Maintain Payment Accounts
(Percentage Distribution of Organizations)

	ALL	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS
Centralized	78%	75%	79%	92%	56%
Decentralized	17%	19%	16%	6%	33%
Other	5%	6%	5%	2%	11%

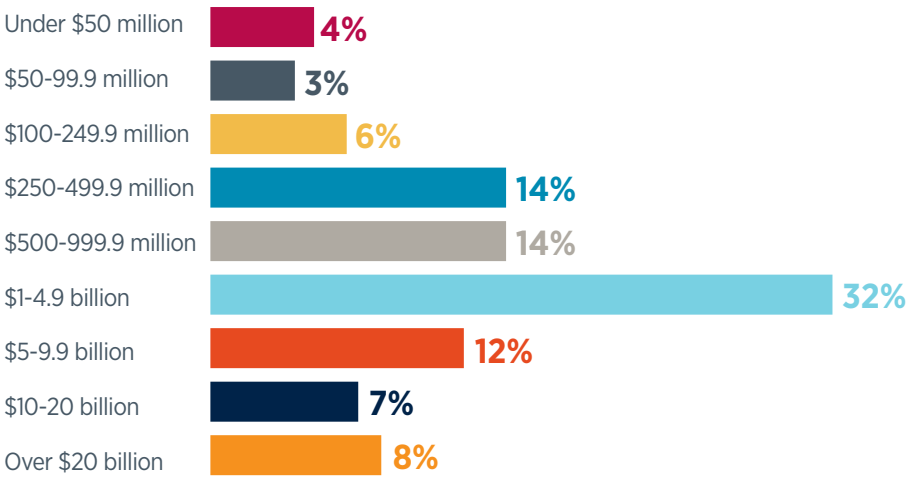
Controls Applied to All Accounts
(Percentage Distribution of Organizations)

	ALL	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS
Yes, applied to all accounts in all areas	85%	80%	88%	89%	83%
Yes, applied to all accounts but in select areas	10%	12%	8%	8%	11%
Not applied to all accounts	5%	7%	4%	3%	6%
Other	–	1%	–	–	–

Number of Payment Accounts Maintained
(Percentage Distribution of Organizations)

	ALL	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS
Fewer than 5	21%	27%	17%	32%	–
5-9	19%	19%	18%	35%	–
10-25	17%	16%	18%	33%	–
26-50	13%	13%	13%	–	–
51-100	10%	10%	10%	–	–
More than 100	20%	15%	24%	–	100%

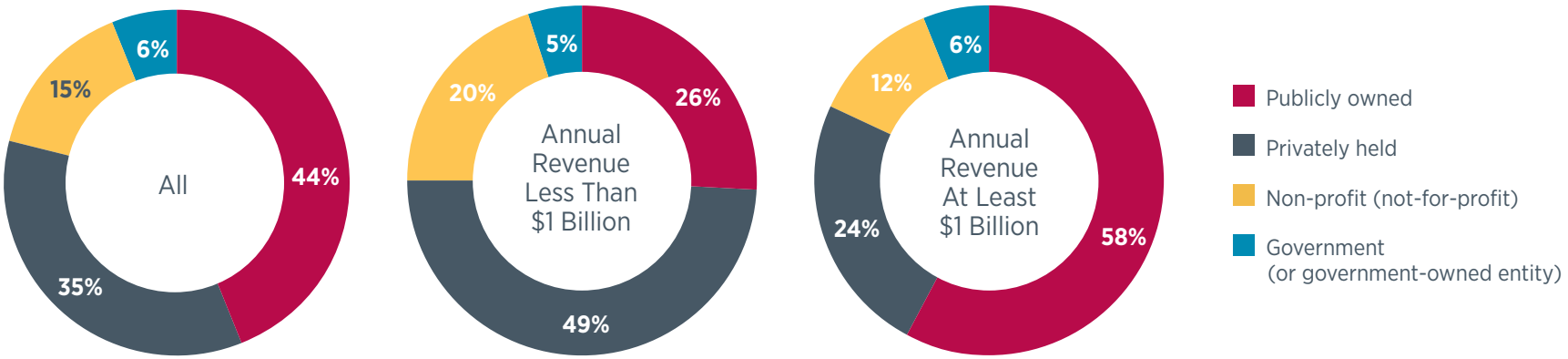
Annual Revenue (USD)
(Percentage Distribution of Organizations)



Industry
(Percentage Distribution of Organizations)

	ALL
Administrative Support/Business services/Consulting	3%
Banking/Financial services	7%
Construction	2%
Energy	4%
Government	6%
Health Care and Social Assistance	10%
Insurance	9%
Manufacturing	18%
Non-profit	8%
Petroleum	1%
Professional/Scientific/Technical services	2%
Real estate/Rental/Leasing	5%
Retail Trade	6%
Software/Technology	4%
Telecommunications/Media	2%
Transportation and Warehousing	5%
Utilities	4%
Wholesale Distribution	4%

Organization's Ownership Type
(Percentage Distribution of Organizations)



AFP Research

AFP Research provides financial professionals with proprietary and timely research that drives business performance. AFP Research draws on the knowledge of the Association's members and its subject matter experts in areas that include bank relationship management, risk management, payments, FP&A and financial accounting and reporting. Studies report on a variety of topics, including AFP's annual compensation survey, are available online at www.AFPonline.org/research.

About AFP®

Headquartered outside of Washington, D.C. and located regionally in Singapore, the Association for Financial Professionals (AFP) is the professional society committed to advancing the success of treasury and finance members and their organizations. AFP established and administers the Certified Treasury Professional® and Certified Corporate FP&A Professional® credentials, which set standards of excellence in treasury and finance. Each year, AFP hosts the largest networking conference worldwide for more than 7,000 corporate financial professionals.

4520 East-West Highway, Suite 800
Bethesda, MD 20814
T: +1 301.907.2862 | F: +1 301.907.2864

www.AFPonline.org

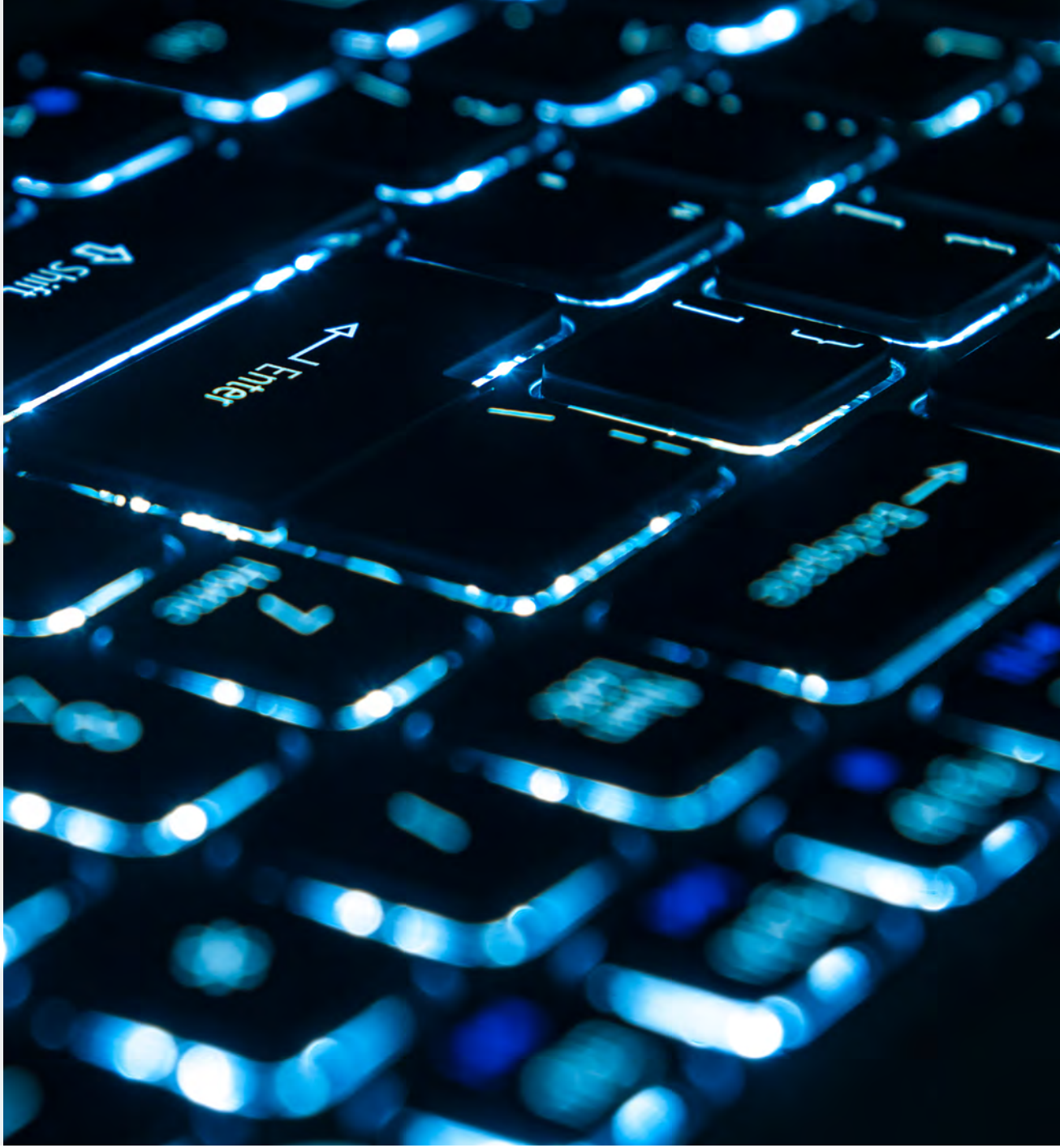
Don’t let your business be the next victim.

Prevent fraud and stay secure with the help of J.P. Morgan.

Last year, 81 percent of financial professionals reported that their organizations had been victims of attempted or actual fraud attacks.

Our sophisticated fraud products and controls can help protect your accounts, assets and data—but we also need you to take action.

Safeguard your business today by visiting **jpmorgan.com/fraudprotection**



J.P.Morgan