ASSOCIATION FOR FINANCIAL PROFESSIONALS

2020 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Key Highlights

Underwritten by J.P.Morgan

2020 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Key Highlights

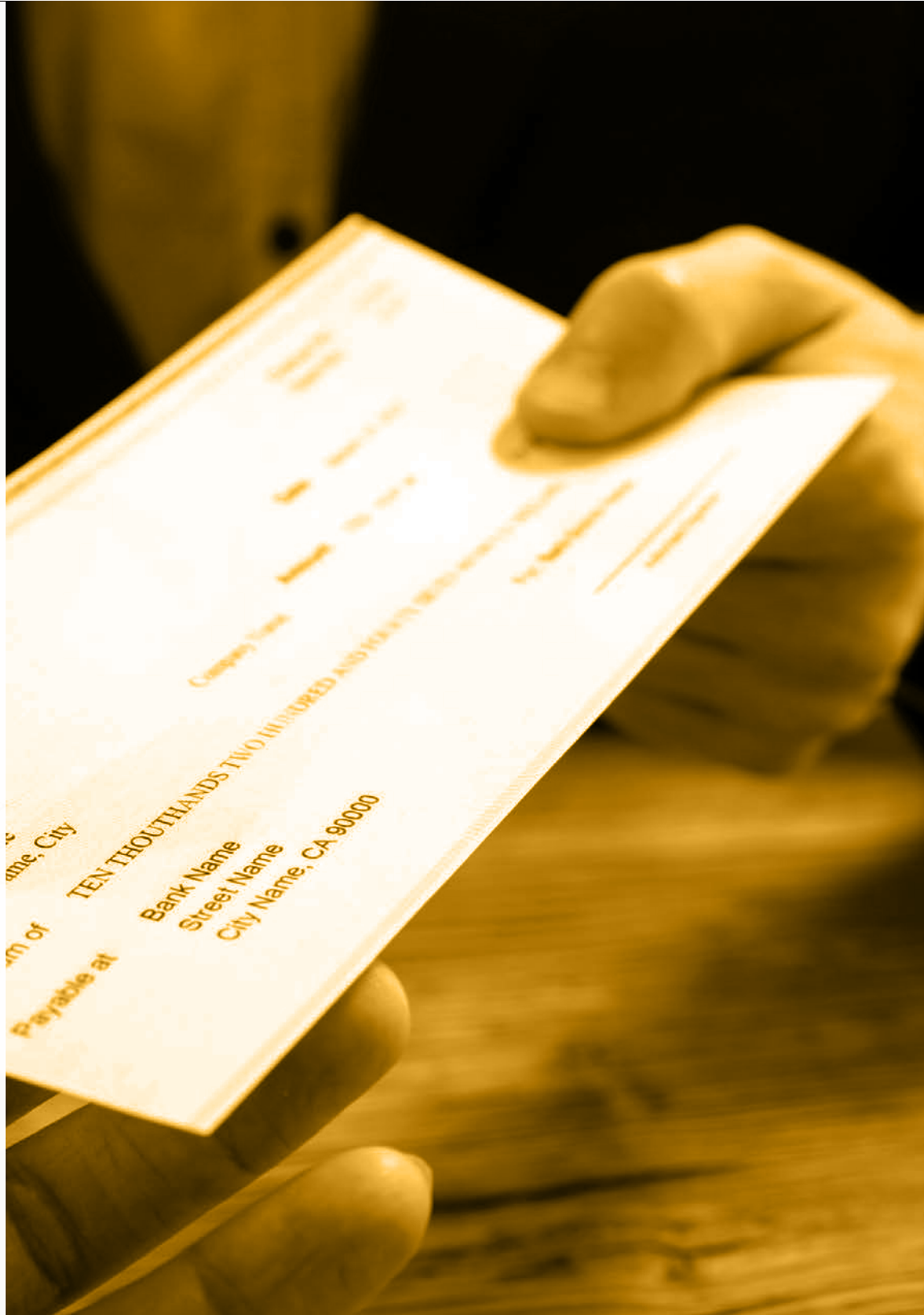
April 2020

2020 AFP® PAYMENTS FRAUD AND CONTROL SURVEY REPORT this summary report includes highlights from the comprehensive 2020 AFP Payments Fraud and Control Survey Report. The complete report comprising all findings and detailed analysis is exclusively available to AFP members. **Learn more about AFP membership.**

Underwritten by J.P.Morgan

TOPICS COVERED IN THE **COMPREHENSIVE 2020 AFP PAYMENTS FRAUD AND CONTROL SURVEY REPORT**

- Payments Fraud Trends
- Payment Methods Impacted by Fraud
- Losses Incurred from Payments Fraud
- Sources of payments Fraud
- Trends in Business Email Compromise (BEC)
- Financial impact of Business Email Compromise
- Departments Most Vulnerable to Payments Fraud
- Payment Fraud Controls
- Fraud Policy
- Corporate/Commercial Credit Cards



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)
  - 54 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

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.

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.

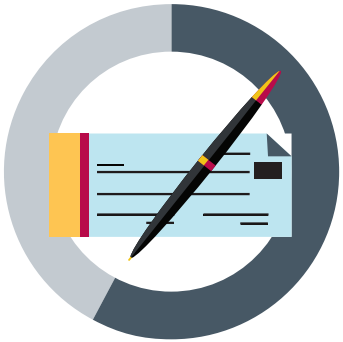
The second most-common source of payments fraud in 2019 was an external source or individual (e.g., forged check, stolen card); 58 percent of financial professionals report that payments fraud at their companies was the result of actions by an individual outside the organization.

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)

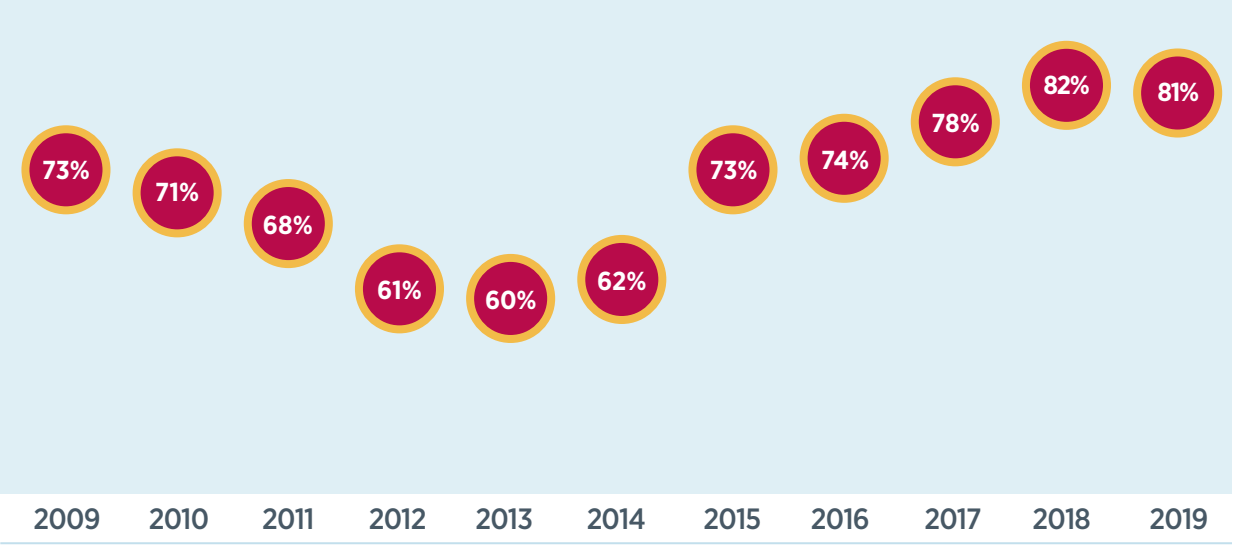
26%
Third-party or outsourcer
(e.g., vendor, professional services provider, business trading partner)

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.

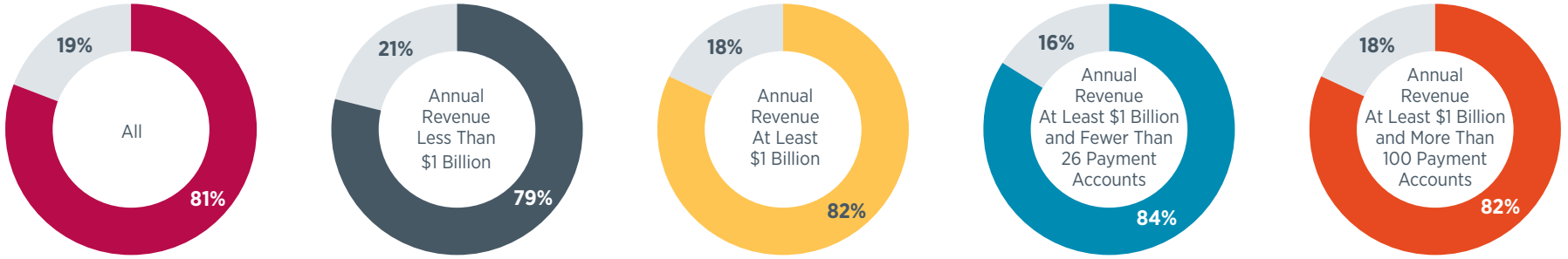
The fact that, overall, payments fraud is currently reported at over 80 percent of organizations is concerning. It suggests that fraudsters continue to succeed in their attempts to attack organizations' payment systems. It also signals that organizations cannot be complacent about the threats of payments 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

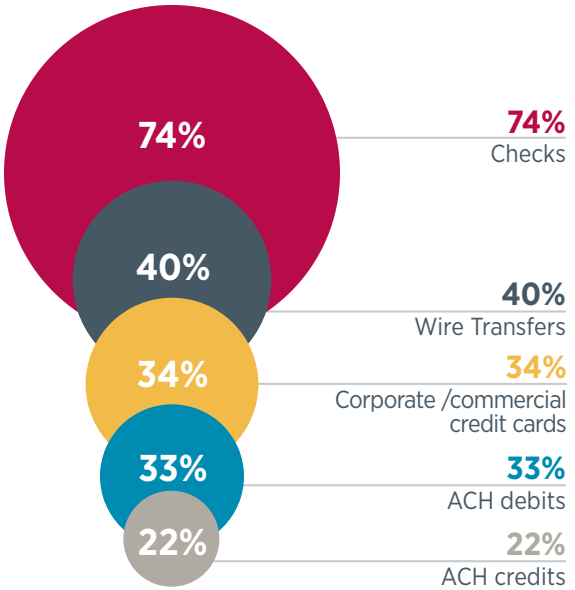
Checks and wire transfers continued to be the payment methods most impacted by fraud activity in 2019 (74 percent and 40 percent of organizations reporting such fraud, respectively). The percentage of financial professionals reporting check fraud activity increased four percentage points from 2018, while 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.

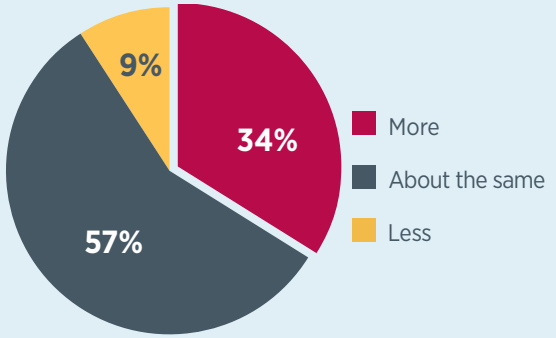
Payment Methods that Were Targets of Attempted and/or Actual Payments Fraud in 2019
(Percent of Organizations)



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)



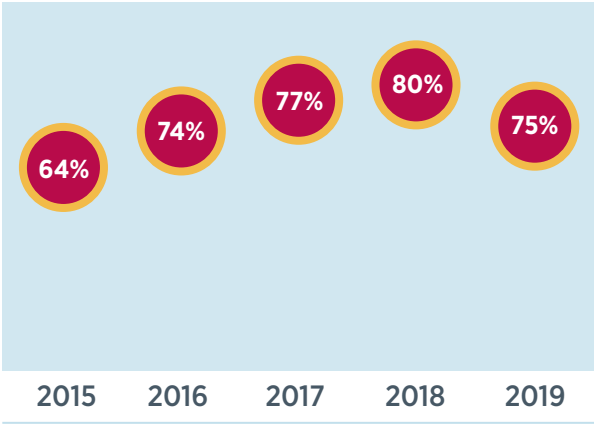
Business Email Compromise (BEC) At Its Lowest Since 2016

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. 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%	–	–

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)

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.

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%

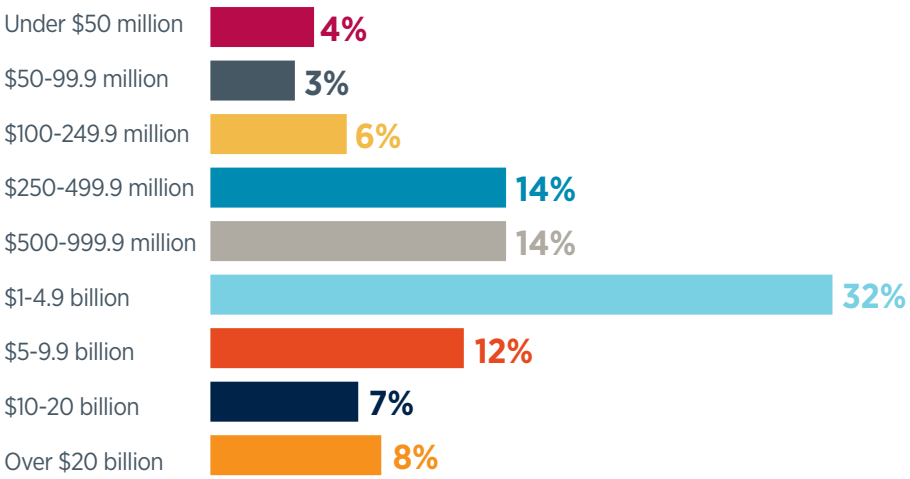
Controls Applied to All Accounts
(Percentage Distribution of Organizations)

	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%

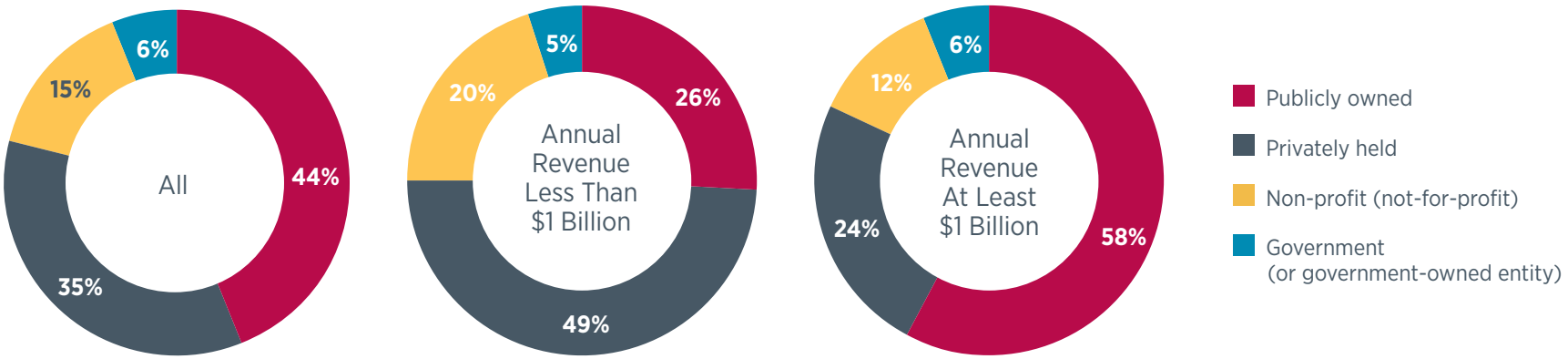
Annual Revenue (USD)
(Percentage Distribution of Organizations)



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

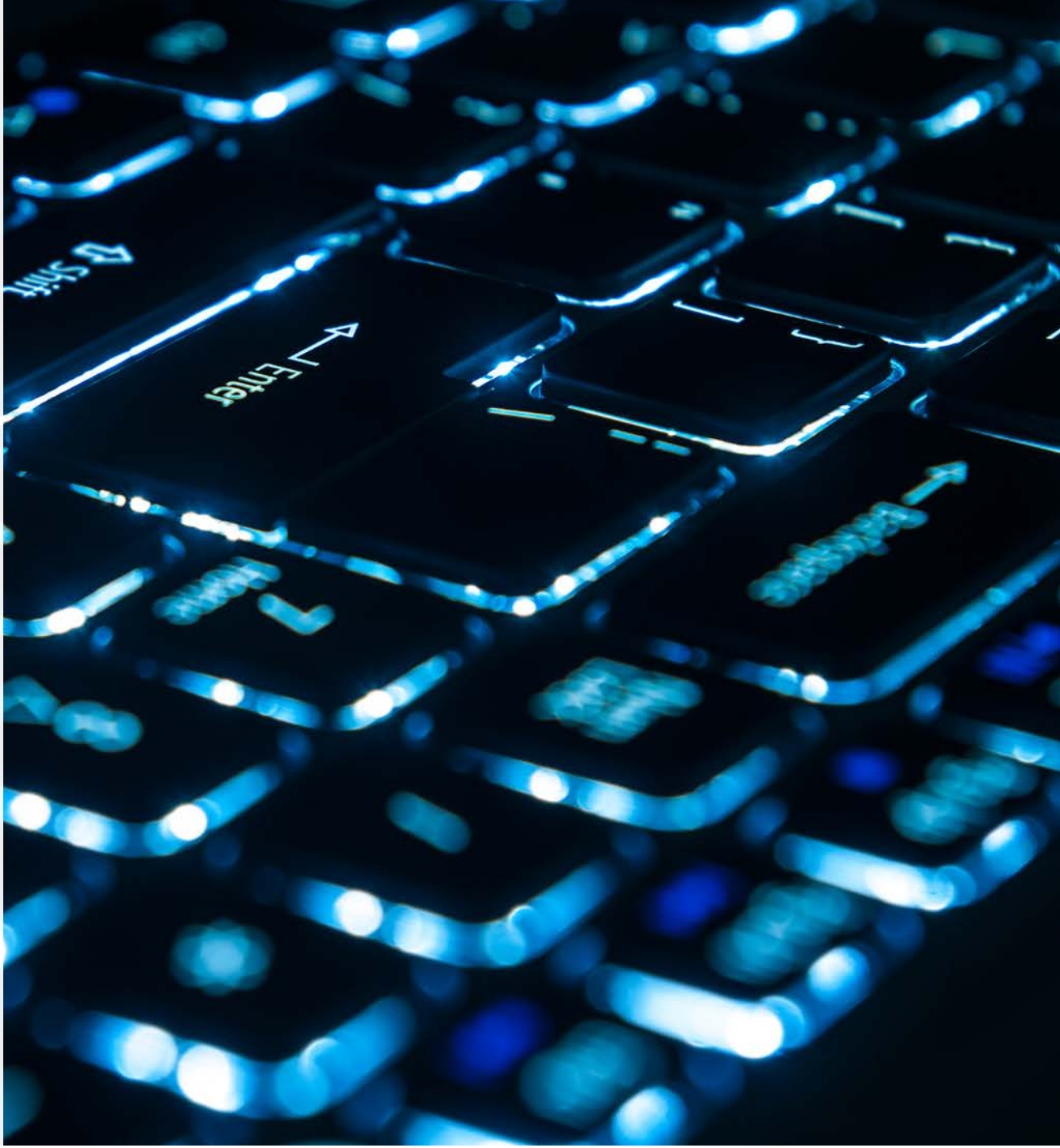
Don’t let your business be the next victim.

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