ASSOCIATION FOR FINANCIAL PROFESSIONALS

2021 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Key Highlights

Underwritten by: J.P.Morgan

J.P.Morgan

We are proud to sponsor the AFP Payments Fraud and Control Survey for the 13th consecutive year and share the 2021 report.

Results from this survey reflect data for 2020, a year marked by the COVID-19 pandemic and its ensuing global disruption. Many businesses like yours had to adapt quickly and transition employees to remote environments almost overnight. There was a high degree of uncertainty over whether these changes—while necessary to limit the spread of the virus—would leave organizations more vulnerable to payments fraud.

One silver lining is that AFP-reported incidents of attempted or actual payments fraud decreased overall last year. However, fraudsters are becoming savvier and more relentless with certain schemes. Business Email Compromise (BEC), for example, increased in 2020, with more than three fourths of companies saying they were targeted. We should not let up on addressing these key areas of fraud through employee education and product innovation.

J.P. Morgan continues to invest heavily in fraud prevention technology, solutions and expertise to help protect our clients. We hope this report informs you of the progress organizations have made in the fight against fraud—as well as the challenges that remain. Let's continue to face them together.

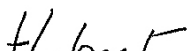
With best regards,

Sue Dean
Managing Director
J.P. Morgan

Bob St Jean
Managing Director
J.P. Morgan

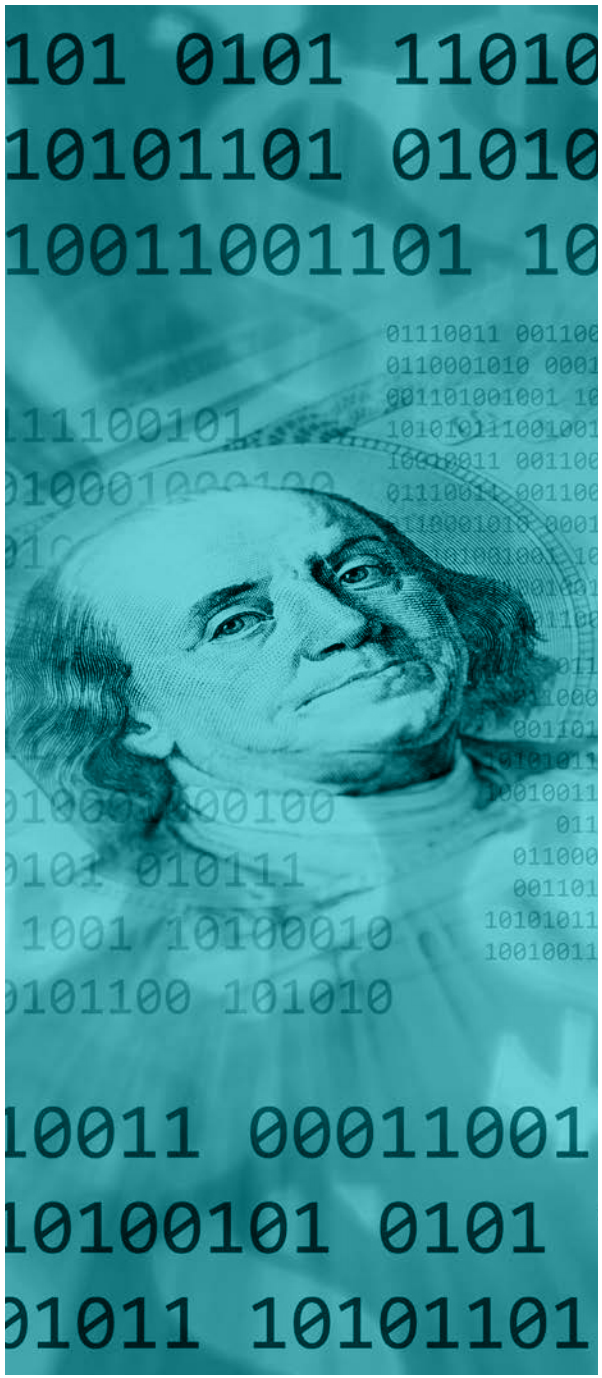
Jessica Lupovici
Managing Director
J.P. Morgan

Winston Fant
Managing Director
J.P. Morgan



Hubert JP Jolly
Managing Director
J.P. Morgan

Alec Grant
Managing Director
J.P. Morgan



2021 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Key Highlights

April 2020

This summary report includes highlights from the comprehensive *2021 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 2021 AFP® Payments Fraud and Control Survey Report

Overview of Payments Fraud Trends

- Payment Methods impacted by fraud
- Losses Incurred from payments fraud
- Sources of payments fraud
- Detecting fraud activity

Trends in Business Email Compromise (BEC)

- Targets for BEC Scams
- Financial Impact of BEC
- Departments Most Vulnerable to BEC

Payment Fraud Controls

- BEC Controls
- Security Credential Controls
- Check Fraud Controls
- ACH Fraud Controls
- Validating Fraud Controls
- Fraud Policy

INTRODUCTION

After reaching record high levels in 2018 and 2019, payments fraud activity declined slightly in 2020. Seventy-four percent of organizations were targets of an attempted or actual payments fraud attack last year, down from 81 percent in 2019. Only time will tell whether this decline is just temporary or the beginning of a sustained decrease in the percentage of companies falling victim to such attacks.

Alleviating payments fraud is top-of-mind for business leaders, and organizations are actively implementing controls and measures to restrict the occurrence of such activity. It is possible that the concerted focus by treasury and finance professionals on preventing their organizations from falling victim to perpetrators of the attacks is paying off. Additionally, while advances in and widespread use of technology have increased payments efficiency, they have also provided criminals with more sophisticated tools to facilitate payments fraud success.

The global COVID-19 pandemic altered the way organizations and their staff operated for a significant part of 2020. To stem the spread of the virus, organizations required employees to work remotely. Many organizations continue to have their staff work "from home." Pre-pandemic, working away from the office was not a normal practice for treasury departments, primarily due to security issues. For employees to socially distance, however, organizations had no choice but to allow their staff to work remotely. Even though there was a decline in overall payments fraud activity in 2020, practitioners do attribute some of the increase in fraud to the pandemic.

Business email compromise (BEC) continued to be the primary source of payments fraud activity at organizations. In these type of attacks, scam artists use emails to dupe accounting departments into transferring funds to illegitimate accounts. Fraudsters spoof URLs and send emails pretending to be vendors or company senior management requesting either a change in bank account information or a transfer of funds to a fraudulent account. With employees working from their homes, the ability to verify an email with a colleague was more challenging. This may be one reason behind the increase in payments fraud via BEC during 2020. The shift from a paper-based/in-person process to electronic methods for check printing and approvals could also explain some of the uptick observed in fraud during the last year. Increased fraud during the pandemic could also be due to Paycheck Protection Program (PPP) loans and other stimulus organizations received.

Treasury and finance professionals must be equipped with the appropriate tools, information and resources in order to outsmart fraudsters. With email increasingly becoming an avenue used by criminals to deceive the organizations they are targeting, extensive training and education need to be offered to company staff. This is not an issue solely for payments departments—every employee should be trained in how to identify a hoax email or request. Additionally, organizations need to have systems and processes in place that will allow for little or no fraud activity to occur such as implementing callbacks to validate payment related requests. While financial loss due to payments fraud may not be large, the risk of reputational damage could be far more significant.

The Association for Financial Professionals® (AFP) has conducted its Annual Payments Fraud Survey every year since 2005. The surveys examine the nature of fraud attacks on business-to-business transactions, payment methods impacted and the strategies organizations are adopting to protect themselves against fraudsters. Continuing this research, AFP conducted the 17th Annual Payments Fraud and Control Survey in January 2021. The survey generated 520 responses from corporate practitioners from organizations of varying sizes representing a broad range of industries. Results from this survey presented in this report reflect data for 2020.

AFP thanks J.P. Morgan for its long-time and continued underwriting support of AFP's Payments Fraud Survey series. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibilities of the AFP Research Department. Information on the survey methodology and respondents' demographics can be found at the end of this report.

Nearly 75 percent of Organizations Were Targets of a Payments Fraud Attack in 2020

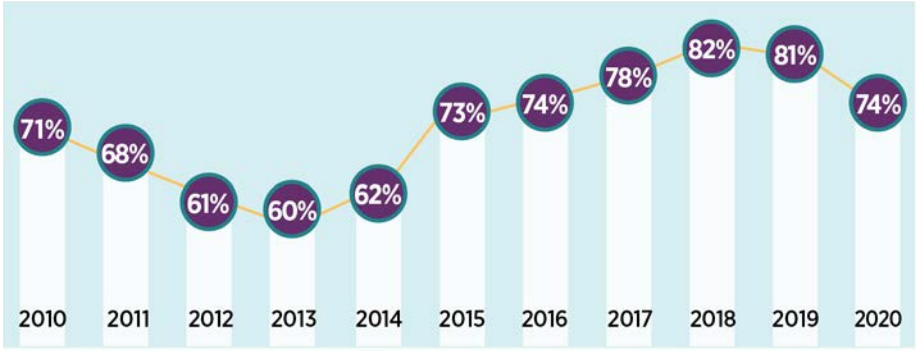
There had been a gradual increase in payments fraud activity at organizations from 2013 through 2018. While the increase was incremental but steady, we observed a significant uptick of 11 percentage points between 2014 and 2015. In the previous two years, record levels of payments fraud activity were reported, with over 80 percent of organizations having been victims of payments fraud attacks in 2018 and 2019.

In 2020, 74 percent of organizations were targets of payment scams. While that is a smaller share than the percentages reported in 2018 and 2019, it still signals that a significant share of companies continues to be impacted.

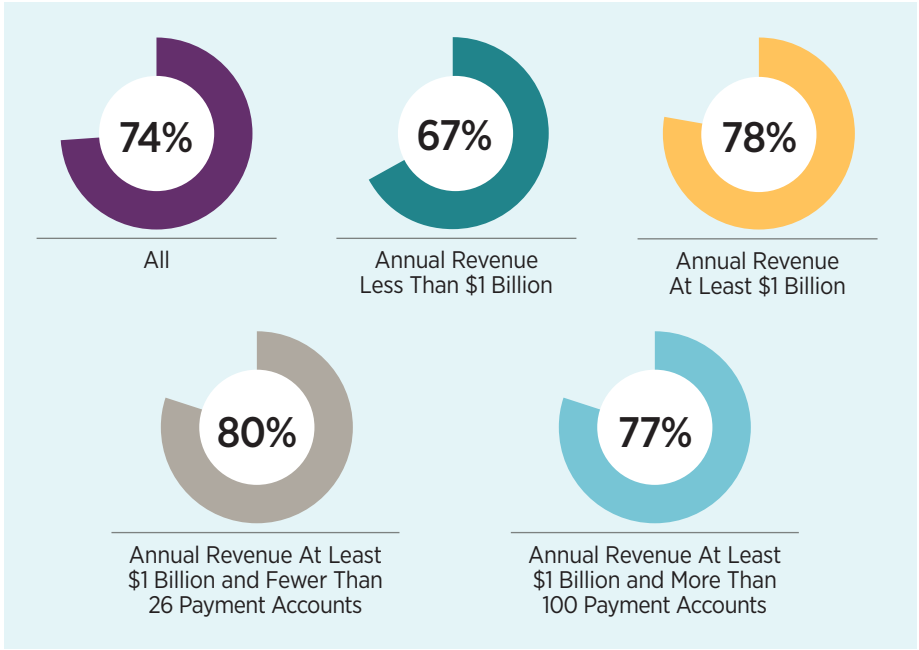
Last year was a year like no other. The COVID-19 pandemic spread across the globe requiring severe social distancing measures to be implemented. Many companies mandated that their employees work remotely. Tasks which were normally carried out only in offices in a secure setting with stringent processes were now being performed in employees' home offices. We can argue that this "working from home" environment should have resulted in even higher instances of payments fraud activity than in in the previous two years. But companies—realizing they were more vulnerable—likely heightened security controls and encouraged their staff to be even more vigilant about payment processes to avoid fraud occurrences. Additionally, in their attempts to bolster their liquidity resources and preserve their cash, organizations cut back on spending and reduced their workforce and/or furloughed staff. These actions more than likely translated into a reduction in payment transactions, fewer business-to-business (B2B) payments and fewer checks being written.

A greater share of survey respondents from larger organizations and those with fewer payment accounts—i.e., those with annual revenue of at least $1 billion and with less than 26 payment accounts—report they experienced payments fraud in 2020 compared with the share of respondents from other organizations. Eighty percent of these organizations were victims of payments fraud. Fewer smaller organizations—those with annual revenue less than $1 billion—were targets of payments fraud in 2020 than were larger organizations (with revenue of at least $1 billion): 67 percent compared to 78 percent. Fraudsters were more inclined to target larger organizations, exposing deficiencies around process controls using social engineering.

Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud, 2010-2020



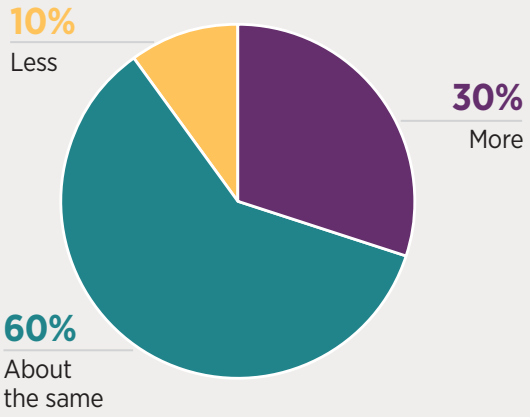
Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud in 2020



Increase in Instances of Fraud at 30 Percent of Companies

Sixty percent of financial professionals report no change in the incidence of payments fraud in 2020 compared to 2019, while 30 percent indicate there had been an increase and 10 percent report a decline. It is encouraging to see a decrease in the share of financial professionals reporting an increase in payments fraud activity—from 34 percent in 2019 to 30 percent in 2020. A larger percentage of respondents from organizations with annual revenue of at least $1 billion and more than 100 payment accounts report increase in payments fraud occurrences at their companies since last year compared to those organizations with annual revenue of at least $1 billion but fewer payment accounts.

Change in Incidence of Payments Fraud in 2020
(Percentage Distribution of Organizations)

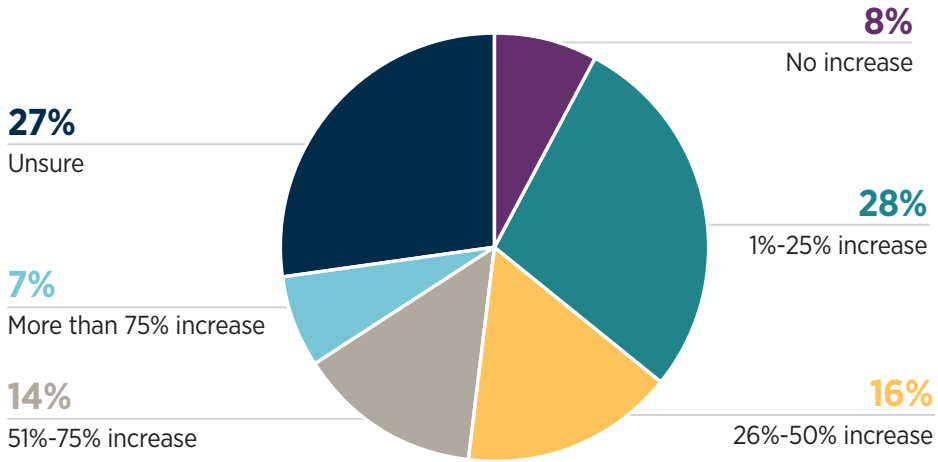


COVID-19 Pandemic to Blame for Some of this Increase

Sixty-five percent of respondents believe some of the increase in fraud at their companies was due to the pandemic, 27 percent are unsure of the pandemic's role on fraud activity and eight percent do not believe the pandemic is to blame for an increase in payments fraud at their organizations. Twenty-eight percent of financial professionals report that one to 25 percent of the increase in fraud activity was likely due to the pandemic while 30 percent attribute 26 to 75 percent of the increased fraud instances to the pandemic; seven percent indicate that over 75 percent of fraud activity observed in the past year was due to the pandemic.

With social distancing measures put in place because of COVID-19, companies repositioned staff to work remotely, requiring business leaders to dust off their Business Continuity Plans (BCPs). BCPs became a primary focus during the pandemic as they assisted in strengthening controls since face-to-face communication and signoff approvals were no longer the norm. Fraudsters attempted to expose the cracks in these well laid-out BCPs, exploiting deficiencies in communication to extract financial gains via BEC and attempt fraudulent bank account changes for vendors. Consequently, BCP plans were shored up, policies tightened further and processes reestablished to prudently manage fraud related to the pandemic.

Share of Increased Fraud due to Pandemic
(Percentage Distribution of Organizations)



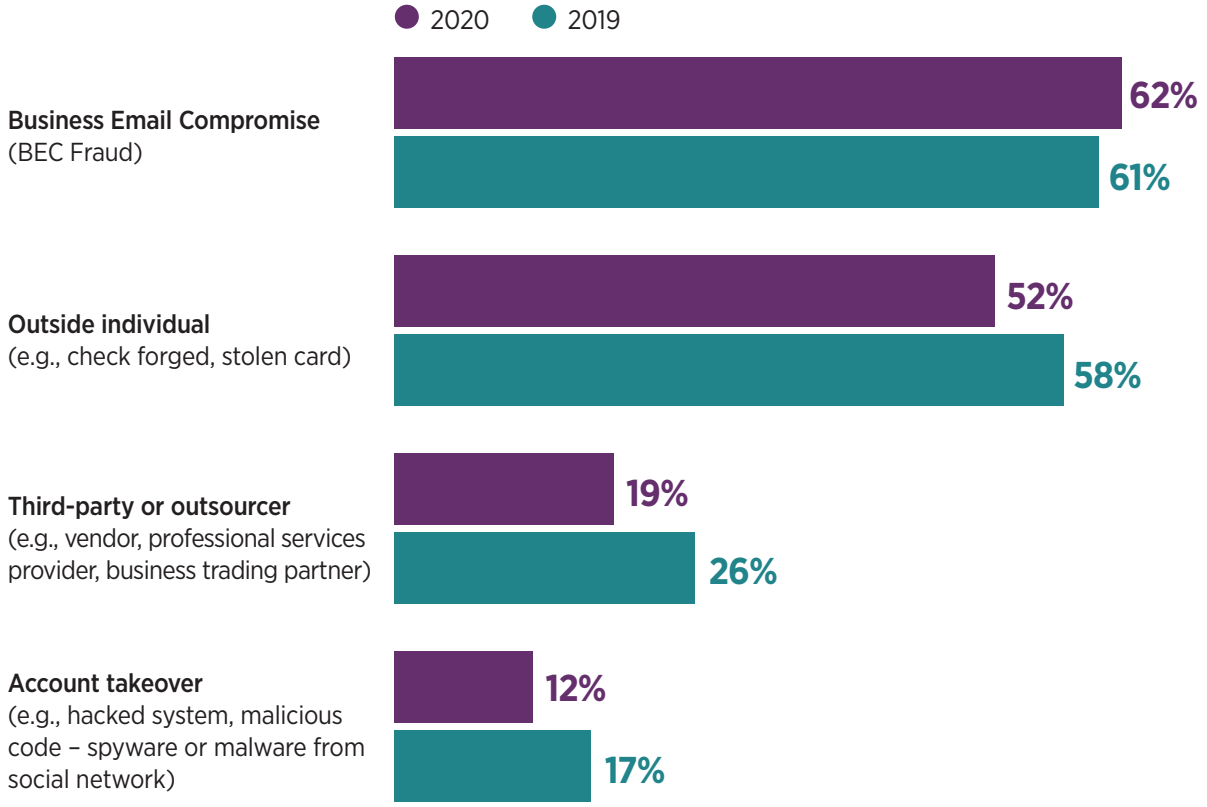
Business Email Compromise (BEC) Continues to be the Primary Reason for Attempted/Actual Payments Fraud Attempts

In 2019, BEC emerged as the key source of fraud attempts at organizations; 61 percent of companies that experienced attempted or actual payments fraud in 2019 did so as a result of BEC. In 2020 as well, BEC continued to be a primary reason for fraud, as 62 percent of practitioners indicate BEC as the primary source of fraud attacks at their organizations. While treasury and finance leaders are very aware of how widespread this type of fraud has become, they are not able to obstruct it sufficiently. Fraudsters are successfully infiltrating payment activity at organizations by using email to do so. Their success in deceiving organizations encourages them to continue to use BEC.

The second most-often mentioned source of payments fraud in 2020 was an external source or individual (e.g., forged check, stolen card); 52 percent of financial professionals report that payments fraud at their companies was the result of actions by an individual outside the organization. This result is six percentage points lower that the figure reported in 2019.

Other sources of payments fraud include third parties or outsourcers such as vendors (experienced by 19 percent of organizations—a seven-percentage-point decrease from 2019). Account takeovers (e.g., hacked system, phishing, spyware or malware) are reported by 12 percent of respondents from companies that experienced attempted/actual payments fraud. Organizations' payment systems continue to be challenged by perpetrators of these attacks and BEC and external individuals are the most successful sources.

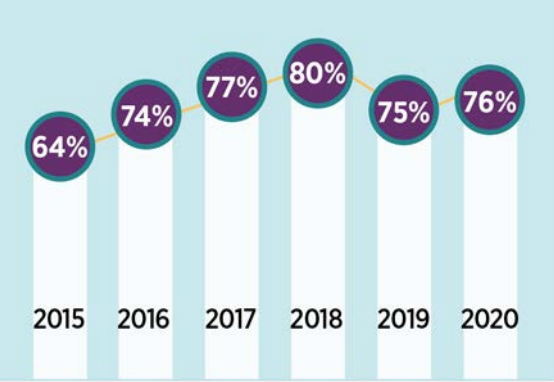
Sources of Attempted and/or Actual Payments Fraud in 2020
(Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud)



Business Email Compromise (BEC) Sees a Slight Increase

Seventy-six percent of organizations were targeted by BEC in 2020, only one percentage point higher than reported in 2019, and in the ballpark of figures reported since 2016. Even though there has been an overall decline in payments fraud activity, from 81 percent in 2019 to 74 percent in 2020, BEC continued to be on the uptick.

Percent of Organizations that Experienced Business Email Compromise (BEC), 2015-2020



Most Organizations Experienced Fewer than 25 Instances of BEC Fraud in 2020

A large majority of organizations experiences 25 or fewer instances of BEC fraud activity occur annually. Types of BEC attacks they are falling victim to include:

- Emails from third parties requesting bank changes, payments instruction, etc.
- Emails from fraudsters posing as senior executives requesting transfer of funds
- Emails from fraudsters impersonating as vendors.

Few companies are reporting seeing more than 25 instances of BEC fraud annually.

Most Prevalent Types of Business Email Compromise (BEC) Fraud
(Percent of Organizations)

	LESS THAN 25 INSTANCES ANNUALLY	26-100 INSTANCES ANNUALLY	101-200 INSTANCES ANNUALLY	200+ INSTANCES ANNUALLY
Emails from other third parties requesting changes of bank accounts, payments instructions, etc.	88%	9%	2%	1%
Emails from fraudsters pretending to be senior executives using spoofed email domains directing finance personnel to transfer funds to fraudsters' accounts	87%	9%	2%	2%
Emails from fraudsters impersonating as vendors (using vendors' actual but hacked emails addresses) directing transfers based on real invoices to the fraudsters accounts	87%	11%	1%	1%

A: Business Email Compromise Controls

Myriad of Controls Used to Curtail BEC

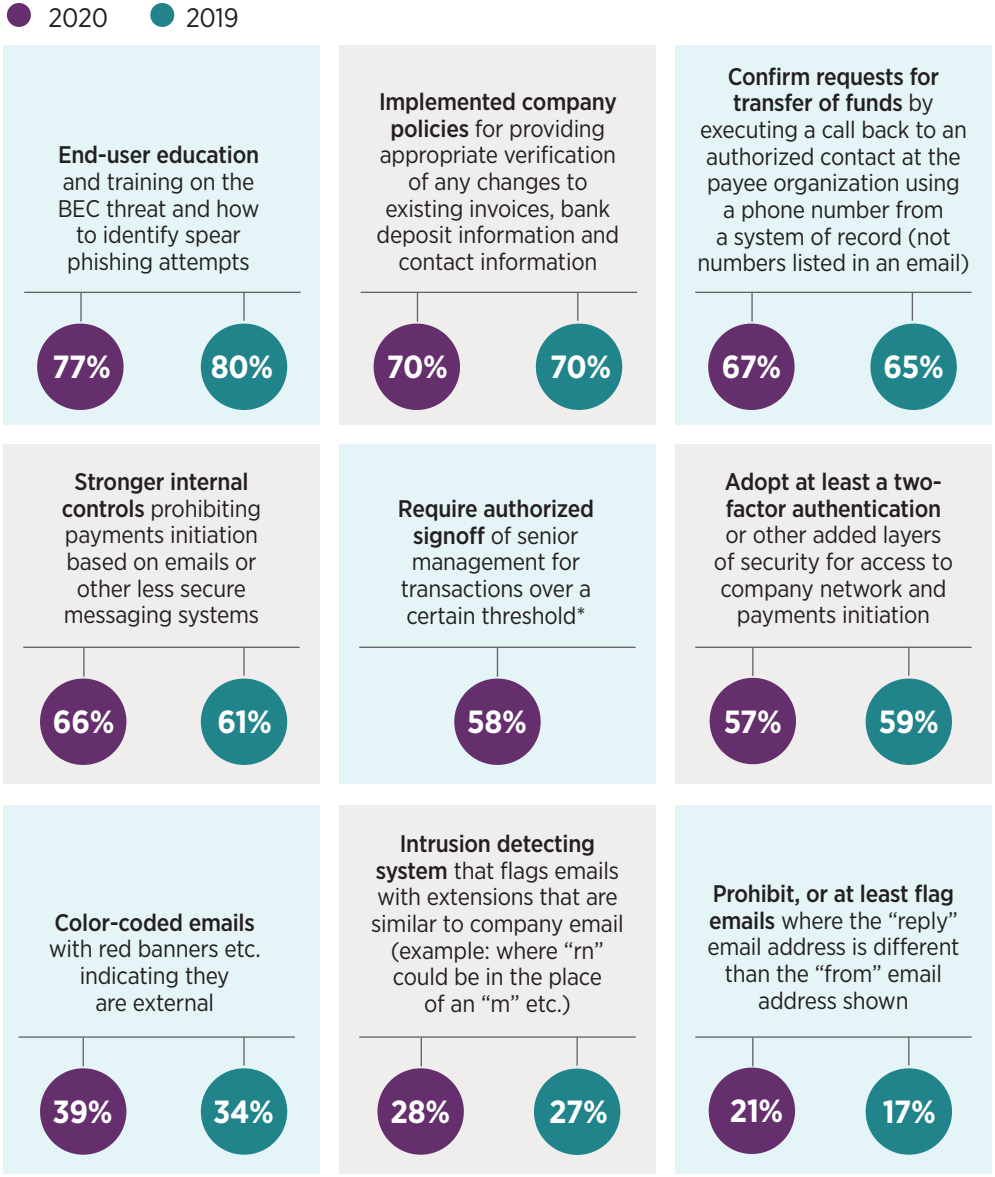
Fraudsters are increasingly using email to con organizations' employees into believing they are legitimate vendors, staff, senior management, et al., and compromising organizations' payment systems. Employees and payments staff at these companies may believe these fake emails are legitimate and transfer funds to these criminals. Not only can some of these attacks result in organizations being adversely impacted financially, but inadvertently organizations' confidential information may also be compromised. As companies implemented Business Continuity Plans in response to staff working remotely, ensuring existing processes were in place to mitigate fraud was increasingly important.

Seventy-seven percent of financial professionals believe that educating employees on the threat of BEC and training them to identify spear phishing attempts are important components in controlling BEC. This is critical if employees are working remotely and so have minimal in-person interaction.

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 any 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) (67 percent)
- **Instituting strong internal controls that prohibit payments initiation based on emails or other less secure messaging systems** (66 percent)
- **Requiring authorized signoff from senior management for transactions over a certain threshold** (58 percent)
- **Adopting at least a two-factor authentication or other added layers of security for access to company network and payments initiation** (57 percent)

Internal Control Methods Implemented by Respondents to Prevent BEC Fraud
(Percent of Organizations)



*was not included in last year's survey

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

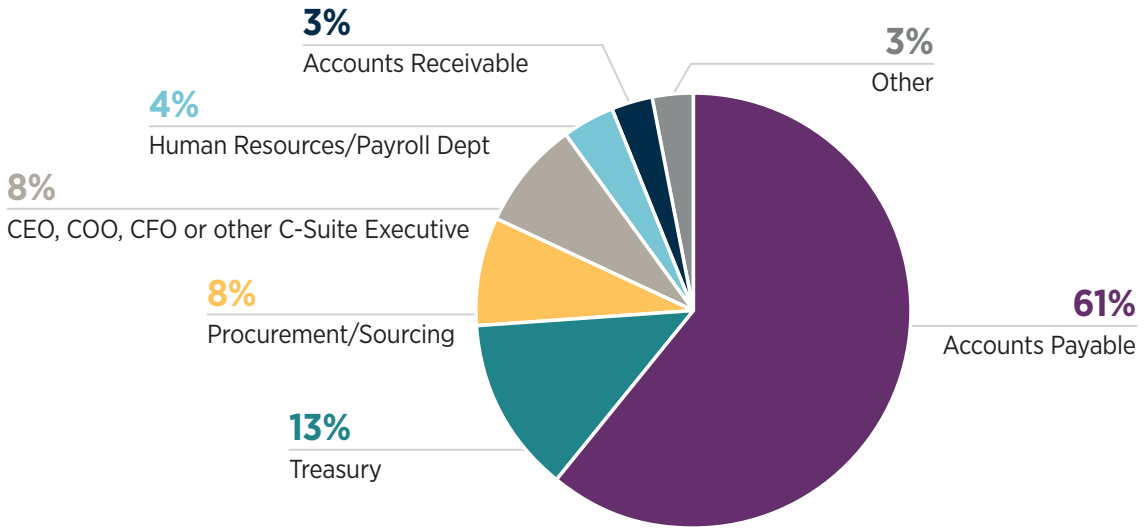
Business Email Compromise scams continue to take various forms and change as criminals get more creative. While these scam artists might target an entire organization, they generally are more focused on the Accounts Payable department as that is where payments originate. Sixty-one percent of respondents indicate that their Accounts Payable department was the most vulnerable business unit targeted. This is very similar to the 62 percent reported in the *2020 AFP® Payments Fraud and Control Report*. The other department most susceptible to BEC fraud was the Treasury department (13 percent).

Seventeen percent of respondents from larger organizations—those 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, and only two percent report that the CEO, COO, CFO or other C-Suite executives were the most targeted group. But the results shift for smaller organizations with annual revenue of less than $1 billion: 14 percent of respondents from those companies note that their organization's CEO, COO, CFO or other C-Suite executives were the most vulnerable, while five percent report that the department most impacted by fraud was procurement/sourcing.

Other departments within organizations reported to be vulnerable include:

- Operations
- Customer Support
- Accounting
- Vendor management

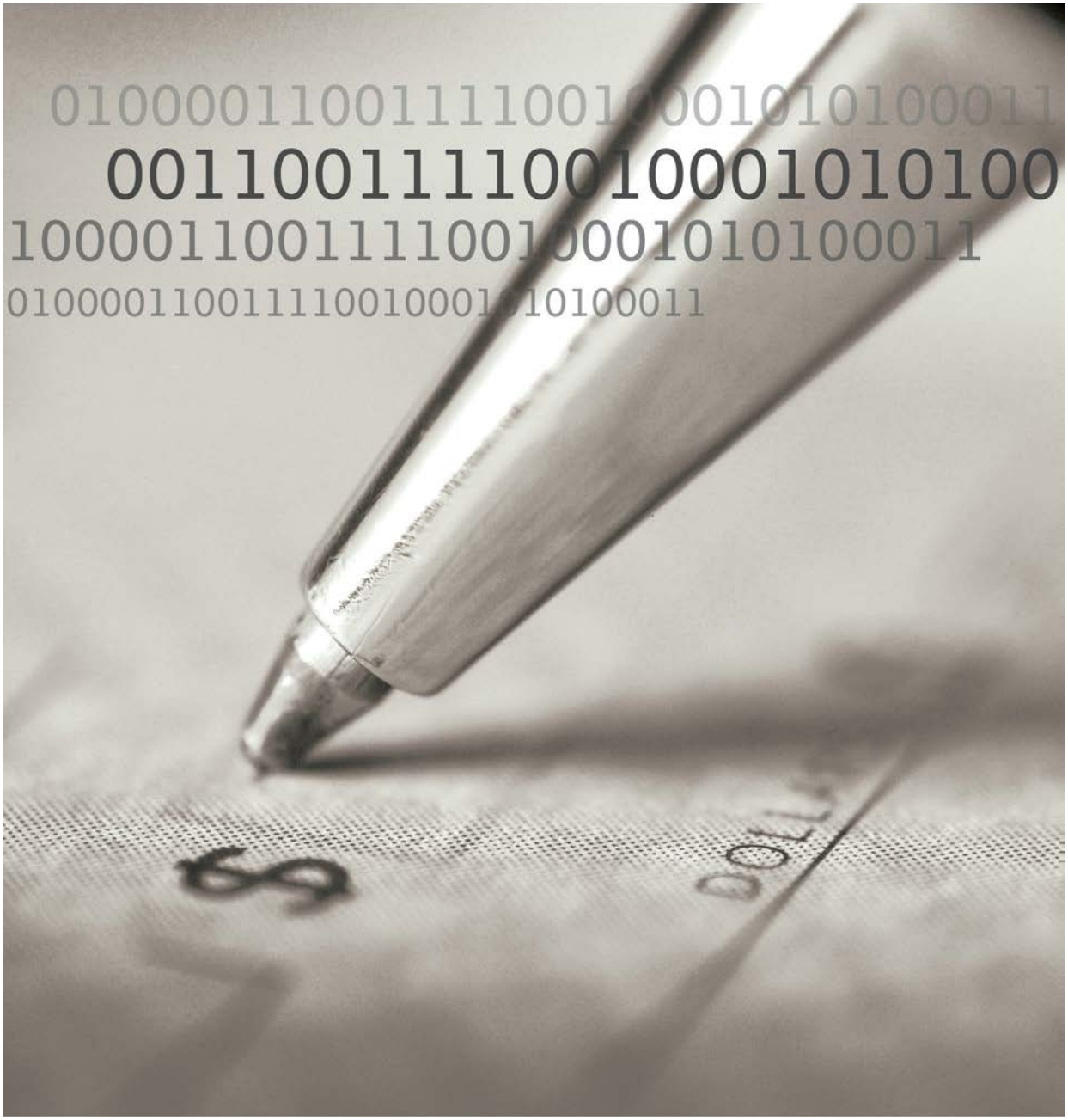
Departments Most Vulnerable to Being Targeted by BEC Fraud
(Percentage Distribution of Organizations)



Checks and Wires Continue to be Most Susceptible to Payments Fraud

In 2020, checks and wire transfers continued to be the payment methods most impacted by fraud activity (66 percent and 39 percent, respectively). The percentage of financial professionals reporting fraud activity via these two payment methods, however, has decreased in the past year, from 74 percent and 40 percent, respectively, in 2019. The 8-percentage-point decrease in check fraud activity is fairly substantial and its incidence is the lowest since 2008 when it was 94 percent. Contributing to the decline in check fraud is the fact that organizations are using fewer checks in their B2B transactions as well as increasing the use of electronic payments as a consequence of staff working remotely. According to the 2019 *AFP® Electronic Payments Report*, 42 percent of organizations reported using checks for B2B payments in 2019, while in 2004 over 80 percent of companies were using checks for similar transactions.

The share of organizations that were victims of fraud attacks via wire transfers has also decreased—from 48 percent in 2017 and 45 percent in 2018 to 40 percent in 2019 and 39 percent in 2020. Companies are more efficient at detecting potential fraud and mitigating it appropriately. Even though results suggest a clear downward trend, wire fraud activity continues to be high, especially considering the share of organizations experiencing such fraud was only in the single digits until 2012.



CONCLUSION

The incidence of payments fraud declined slightly in 2020. There had been a gradual increase in payments-fraud activity at organizations from 2013 to 2018, and in 2018 and 2019 record levels of payments fraud activity were reported, with over 80 percent of organizations having fallen victim to payments fraud attacks. In 2020, 74 percent of organizations were targets of payment scams. While that is smaller than the shares reported in 2018 and 2019, it is evident that a significant percentage of companies continue to be impacted.

The entire world began to grapple with the COVID-19 pandemic in 2020. The potential for increased occurrences of payments fraud were certainly on the radar for treasury and finance professionals as they organized how their staff could continue to function as seamlessly as possible as they worked "from home" without adversely impacting the organization's operations. Despite the increased cognizance, 65 percent of respondents believe some share of the increase in fraud at their companies was due to the pandemic.

Checks and wire transfers continued to be the payment methods most impacted by fraud activity in 2020. The percentage of financial professionals reporting fraud activity via these two payment methods, however, has decreased in the past year. The incidence of check fraud was at its lowest level since 2008. Contributing to the decline in check fraud is the fact that organizations are using fewer checks in their business-to-business transactions.

The share of organizations that were victims of fraud attacks via wire transfers has also been decreasing gradually. But this year's survey results also reveal a slight increase in fraud activity via ACH debits. This shift in fraud activity from checks and wires to ACH transactions signals that these perpetrators are targeting ACH payment methods more frequently than check and wire transfers. The share of organizations experiencing corporate/commercial credit card fraud also decreased substantially in 2020.

As was the case in 2019, business email compromise—or BEC—was the primary source of payments fraud attacks at organizations in 2020. While treasury and finance leaders are keenly aware of how widespread this type of fraud has become, they are not able to alleviate instances of this BEC. Fraudsters use email to successfully infiltrate payment activity at organizations. BEC scams continue to take various forms and change as these criminals become more creative. Even though these scam artists might target the entire organization, they are more focused on the Accounts Payable department as that is where payments originate.

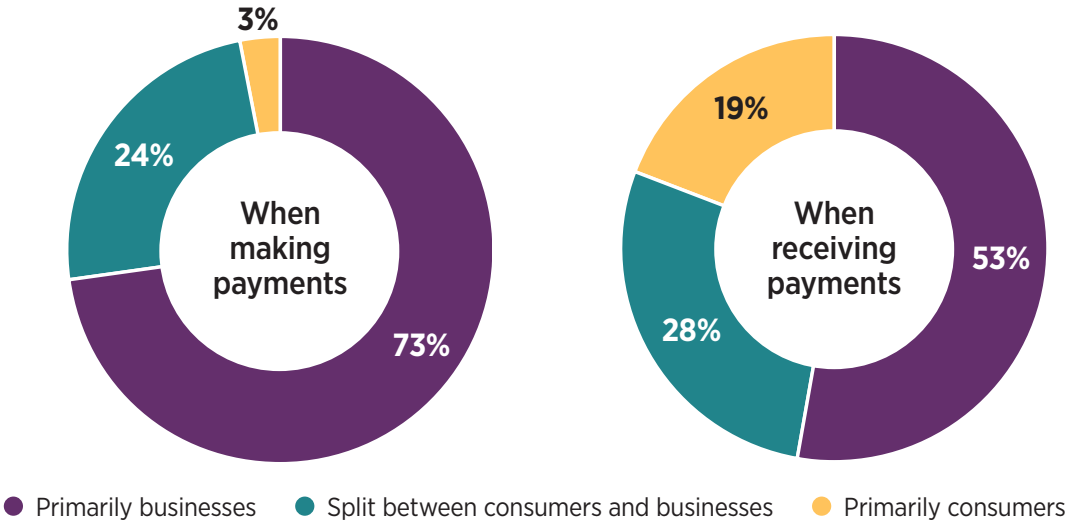
As business leaders focus on safeguarding against fraud, they understand those planning these attacks are devising new methods to deceive their unsuspecting victims. It is vital that treasury and finance professionals continue to be vigilant and protect their organizations against future attacks to the best of their abilities. It might involve validating fraud controls regularly to ensure they are doing what they are supposed to do—that is, preventing fraud as well as strategizing and implementing new controls that might be more effective in preventing criminals from being successful in their endeavors.

ABOUT RESPONDENTS

In January 2021, the Research Department of the Association for Financial Professionals® (AFP) surveyed over 9,000 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 534 responses were received and after removing duplicates, etc., we eventually had 520 responses from practitioners, and these form the basis of the report.

AFP thanks J.P. Morgan for underwriting the *2021 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.

Type of Organization's Payment Transactions
(Percentage Distribution of Organizations)



Methods to Maintain Payments 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	80%	86%	75%	90%	60%
Decentralized	16%	12%	18%	8%	28%
Other	5%	2%	7%	2%	13%

Accounts to which Controls are Applied

(Percentage Distribution of Organizations)

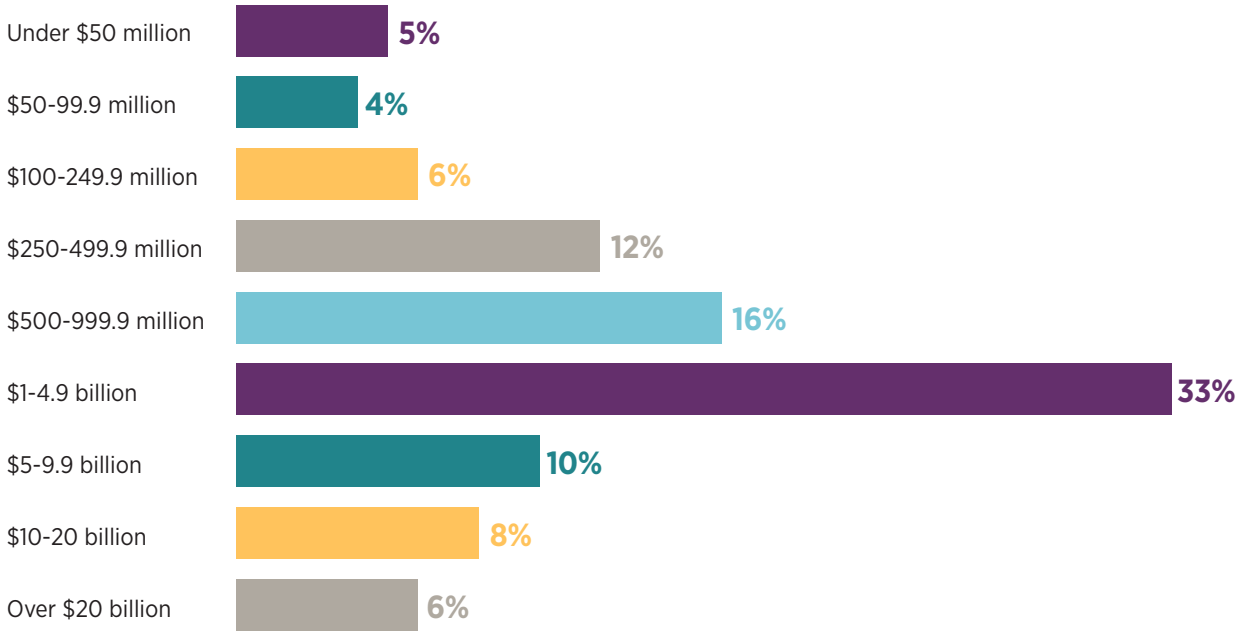
	ALL	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS
Applied to all accounts in all areas	87%	85%	87%	86%	87%
Applied to all accounts but in select areas	10%	12%	10%	12%	7%
Not applied to all accounts	3%	1%	4%	2%	5%
Other	1%	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	23%	36%	14%	28%	–
5-9	17%	19%	16%	33%	–
10-25	19%	20%	19%	39%	–
26-50	12%	7%	15%	–	30%
51-100	11%	8%	13%	–	25%
More than 100	18%	11%	22%	–	45%

Annual Revenue (USD)
(Percentage Distribution of Organizations)



Organization's Ownership Type
(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
Publicly owned	38%	21%	52%	46%	57%
Privately held	38%	49%	29%	28%	31%
Nonprofit (not-for-profit)	14%	21%	11%	14%	7%
Government (or government-owned entity)	9%	10%	8%	12%	5%

Industry Classification
(Percentage Distribution of Organizations)

	ALL
Agricultural, Forestry, Fishing & Hunting	1%
Administrative Support/Business services/ Consulting	3%
Banking/Financial services	5%
Construction	2%
Energy	4%
Government	7%
Health Care and Social Assistance	7%
Hospitality/Travel/Food Services	2%
Insurance	8%
Manufacturing	20%
Non-profit	8%
Petroleum	2%
Professional/Scientific/Technical Services	1%
Real estate/Rental/Leasing	5%
Retail Trade	7%
Wholesale Distribution	5%
Software/Technology	3%
Telecommunications/Media	3%
Transportation and Warehousing	4%
Utilities	4%

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

Be Informed and Stay Ahead of Fraud

Unprecedented disruption calls for established expertise.

Combine insights from AFP's survey with J.P. Morgan's advanced fraud prevention tools and applied best practices to protect your organization against future challenges.

Learn more by visiting **jpmorgan.com/fraudprotection**

J.P.Morgan