



ASSOCIATION FOR
FINANCIAL
PROFESSIONALS

2022 AFP®

Payments Fraud and Control Report

Key Highlights

Underwritten by: **J.P.Morgan**

We are proud to support the *AFP® Payments Fraud and Control Survey* for the 14th consecutive year and share the 2022 report with you.

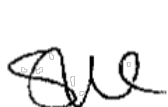
Results from the survey reflect data from 2021, as the world adjusted to new ways of working and living through the COVID-19 pandemic and other operational disruptions.

The evolving threat landscape demands that companies of all industries and sizes be agile and prepared against fraud risks. Fraudsters are constantly looking for new ways to commit payments fraud—whether by using social engineering to compromise confidential information or creating look-alike domains to impersonate vendors through business email compromise.

Because of these dangers, businesses must ensure they have the controls in place to combat rising fraud attempts. Strong callback processes and validation procedures are crucial when fulfilling new or altered payment requests to maintain resiliency and avoid fraud loss.

J.P. Morgan continues to prioritize our investment in fraud-prevention technology, solutions and expertise. We have the tools, insights and resources to help protect ourselves and the companies we work with. We hope this report provides you with valuable insights as we fight fraud together.

With best regards,



Sue Dean
Head of Solutions,
Commercial Banking
J.P. Morgan



Max Neukirchen
Global Head of
Payments & Commerce
Solutions
J.P. Morgan



Alec Grant
Head of Client Fraud
Prevention, Commercial
Banking
J.P. Morgan

J.P.Morgan

2022 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Key Highlights

April 2022

This summary report includes highlights from the comprehensive *2022 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](#)

Topics Covered in the Comprehensive 2022 AFP® Payments Fraud and Control Survey Report

Payments Fraud Activity

- Payments Fraud Trends
- Impact of Remote Work Environment on Payments Fraud
- Payment Methods Impacted by Payments Fraud
- Corporate/Commercial Card Fraud
- Losses Incurred Due to Payments Fraud Attempts/Attacks
- Detecting Payments Fraud Activity
- Primary Sources of Attempted/Actual Payments Fraud

Business Email Compromise (BEC)

- About Business Email Compromise
- Business Email Compromise Trends
- Financial Impact of Business Email Compromise
- Financial Losses Incurred Due to Business Email Compromise
- Targets of Business Email Compromise Scams
- Departments Most Susceptible to Business Email Compromise Fraud

Payment Fraud Controls

- Business Email Compromise Controls
- Check Fraud Controls
- ACH Fraud Controls
- Validating Payment Beneficiary Information and Sanction Screening
- Current Measures Implemented to Improve Controls and Measures Wished for in 2022

Underwritten by: **J.P.Morgan**

INTRODUCTION

In the past two years, the COVID-19 pandemic has altered the way many of us live, travel and—in many cases—the way we work. Globally, organizations mandated that employees work remotely. But that remote working required companies alter many of their processes and procedures. One of those processes impacted was payments. With less face-to-face interaction, employees were in a situation where verifying payments requests or transactions was more challenging, and financial professionals relied on emails and other forms of virtual communication for payments information. Not surprisingly, we should have expected fraudsters to make the most of this situation and target employees to fall victim to their ploys.

The 2022 AFP® *Payments Fraud Survey's* findings, however, suggest that remote working did *not* play a significant role in the incidence of payments fraud observed at organizations during 2021. Additionally, the share of organizations that were impacted by email fraud also declined, evidence of the extensive efforts made by business leaders to safeguard employees vulnerable in a remote working environment, and that the ramping up training and other validation and verification processes had some success.

Survey findings also reveal check fraud activity is unchanged from 2020's figures (66 percent), lower than recorded in past years.



INTRODUCTION (Continued)

The decline in check fraud can also be due to organizations using fewer checks for business to business (B2B) transactions as well as the increased use of digital payments due to staff working remotely. Indeed, any expectations that remote working environments would result in greater fraud activity was likely disproved due to cognizant financial practitioners who proactively implemented controls and processes to prevent fraud occurrences.

Payments fraud activity, however, continued to occur at many organizations. Even so, there are signs that suggest payments fraud activity is abating. Payments fraud activity had been increasing steadily since 2013 and in 2018 reached a new peak. More than 80 percent of financial professionals reported that their organizations were targeted by fraudsters in 2018—the largest percentage since the Association of Financial Professionals® (AFP) began tracking such activity. In the subsequent year, the percentage of organizations reporting incidents of payments fraud continued to be escalated at 81 percent; since then, fraud activity has declined. While that is an encouraging sign, recent survey results reveal that over 70 percent of companies continue to be targeted by fraudsters.

AFP first began tracking payments fraud via email—business email compromise (BEC)—in 2015. Fraudsters found email a relatively easy avenue through which to target organizations via their employees. Fraud via BEC continued to increase and peaked in 2018. Subsequently, email-based fraud became the primary source of fraud at a majority of companies. Financial

professionals reacted by implementing training for employees to help them identify emails that were phishing attempts. Additional controls were also introduced that required verification calls and other validation. Although BEC continues to be prevalent and the primary source of payments fraud at over half of organizations, efforts of those responsible for curbing fraud are resulting in some success.

Declining check usage is possibly also contributing to fewer instances of check fraud.

Checks continue to be the payment method most often targeted by fraudsters to infiltrate organizations. In 2021, two-thirds of organizations were prey to check fraud—a result unchanged from the findings in last year's survey report and, again, lower than the incidence of check fraud observed in prior years. Checks are the payment method most used by organizations, and so not surprisingly are the most frequent targets of fraudsters. Declining check usage is possibly also contributing to fewer instances of check fraud. (According to the 2019 AFP® *Electronic Payments Survey*, check usage has decreased by nine percentage points from 2016 to 2019.)

But while there has been a general decline in payments fraud via checks over the last several years, incidences of fraud via ACH debits and ACH credits are on the uptick. This finding is evidence of the persistence of fraudsters; they are constantly innovating and devising plans to defraud organizations. Business leaders cannot let their guard down—they have to actively monitor fraud activity, be vigilant and take all precautions in order to outsmart sophisticated criminals.

Every year since 2005, the Association for Financial Professionals® (AFP) has conducted its *Payments Fraud Survey*. The surveys examine the nature of fraud attacks on business-to-business transactions, the payment methods impacted and the strategies organizations are adopting to protect themselves from those committing payments fraud. Continuing this research, AFP conducted the 18th *Annual Payments Fraud and Control Survey* in January 2022. The survey generated 552 responses from corporate practitioners from organizations of varying sizes representing a broad range of industries. Results presented in this report reflect data for 2021. Survey respondent demographics are available at the end of this report.

AFP thanks J.P. Morgan for its continued underwriting support of the *AFP Payments Fraud and Control Survey* series. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibility of AFP's Research Department.

KEY FINDINGS

Percentage of Organizations That Are Victims of Payments Fraud Attacks/Attempts on the Decline

After the record highs of payments fraud recorded in 2018 and 2019, the share of organizations reporting fraud activity in 2020 decreased to 74 percent. This year's survey results are encouraging as there was a further decrease in the incidence of attempted or actual payments fraud in 2021; 71 percent of survey respondents report their organizations were victims of payments fraud attacks in 2021.



Employees Working Remotely Only Partly to Blame for Any Increase in Payments Fraud at their Organizations

Forty-seven percent of respondents do not believe that remote work is to blame for the increase in payments fraud at their organizations. Thirty-two percent of respondents believe any increase in payments fraud at their companies is the result of employees working remotely, while 21 percent are unsure

whether employees working away from the office has had an impact on the incidence of payments fraud.



A Sharp Decrease in Business Email Compromise (BEC)

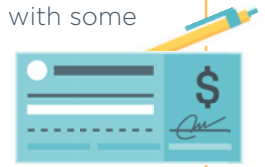
Sixty-eight percent of organizations were targeted by BEC in 2021, eight percentage points lower than in 2020 and the second lowest percentage since AFP began tracking this data in 2015. Wires and ACH credits were both key targets for email scams, with each of these payment methods targeted at 41 percent of organizations in 2021.

Checks and ACH Debits Most Susceptible to Payments Fraud While Wire Fraud Decreases

In 2021, checks and ACH debits were the payment methods most impacted by payments fraud activity (66 percent and 37 percent, respectively). Sixty-six percent of financial professionals report that check fraud activity was unchanged from 2020. Payments fraud via checks had been on the decline since 2010, with some intermittent upticks in between.

The share of respondents reporting payments fraud via ACH debits increased from 34 percent in 2020 to 37 percent in 2021. The share of fraud activity via ACH debits has been increasing gradually—from 33 percent in 2019 to 34 percent in 2020 and to 37 percent in 2021.

Payments fraud via wire transfers decreased from 39 percent in 2020 to 32 percent in 2021. The percentage of organizations that were victims of fraud via wire transfers has been on a steady decline—48 percent in 2017, 45 percent in 2018, 40 percent in 2019, 39 percent in 2020 and 32 percent in 2021.



Accounts Payable Departments Targeted by Email Scammers



Accounts Payable (AP) departments continue to be the department most susceptible to BEC with 58 percent of survey respondents indicating their AP departments were compromised through email scams. While that is slightly less than the 61 percent reported last year, it remains a concern as payments fraud via ACH debit and ACH credit is on the rise.

Majority of Organizations is Validating Payment Beneficiary Information

Two-thirds of organizations are validating payment beneficiary information, either through their vendors/banks (36 percent) or by using an external service (30 percent).





PAYMENTS FRAUD ACTIVITY



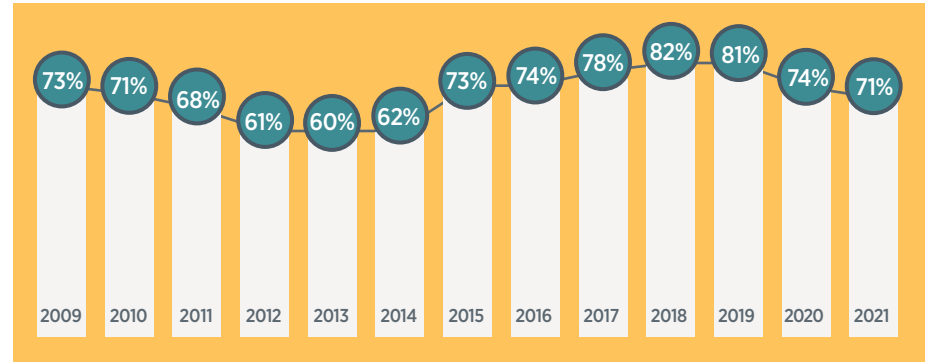
PAYMENTS FRAUD TRENDS

Percentage of Organizations That Are Victims of Payments Fraud Attacks/Attempts on the Decline

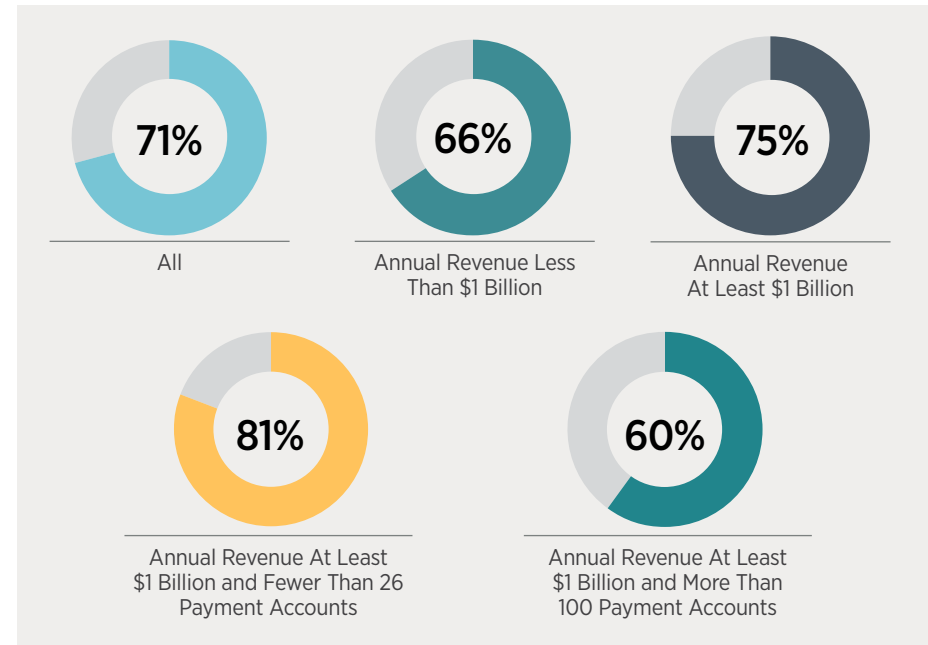
From 2009-2013, the percentage of organizations that experienced attempted or actual payments fraud steadily declined. In 2015, there was an uptick in the share of companies that were victims of payments fraud attempts and attacks: 73 percent of organizations were targets of payments fraud in 2015—a significant 11-percentage-point increase 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, just shy of the previous year's record-setting 82 percent. In 2020 fraud figures decreased to 74 percent. This year's survey results are encouraging, as the occurrence of attempted or actual payments fraud declined again, with 71 percent of organizations having been victims of payments fraud attacks in 2021.

Larger organizations (with annual revenue of at least \$1 billion) are more susceptible to payments fraud attacks than are smaller ones (with annual revenue of less than \$1 billion): 75 percent compared to 66 percent. 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 that their companies experienced payments fraud in 2021 compared with the share of respondents from other organizations.

Percent of Organizations That Are Victims of Payments Fraud Attacks/Attempts



Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud in 2021



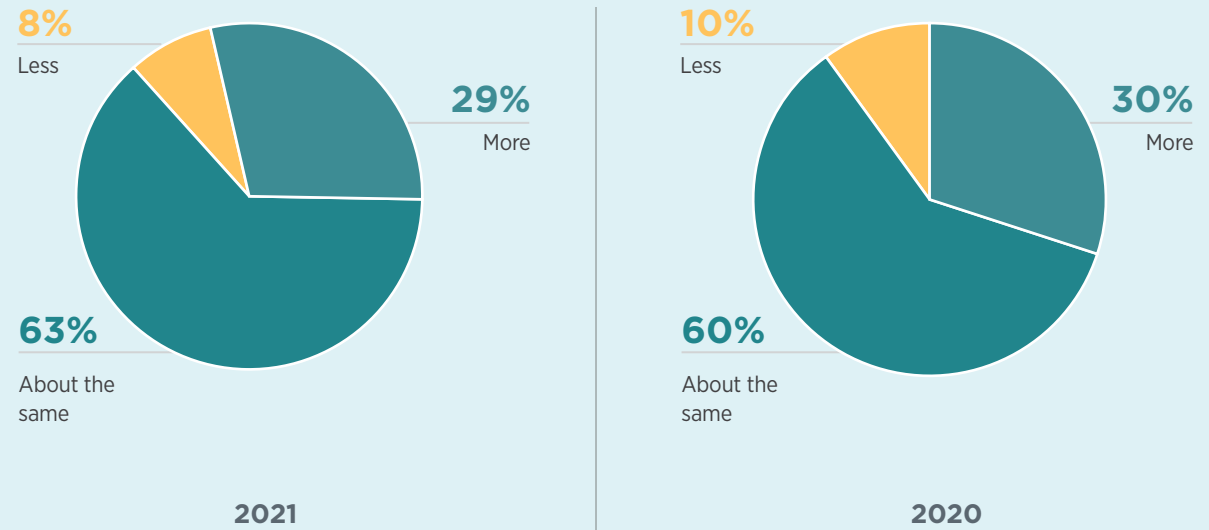


PAYMENTS FRAUD TRENDS

Uptick in Fraud at Nearly 30 Percent of Companies

Sixty-three percent of financial professionals report the incidence of payments fraud in 2021 was unchanged from that in 2020, while 29 percent indicate there *had* been an increase and 8 percent report a decline. The share of financial professionals reporting an increase in payments fraud activity has steadily declined—from 34 percent in 2019 to 30 percent in 2020 and to 29 percent in 2021. A larger percentage of respondents from organizations with annual revenue of at least \$1 billion and more than 100 payment accounts report an increase in payments fraud occurrences at their companies in 2021 compared to those from organizations with annual revenue of at least \$1 billion but fewer payment accounts (50 percent and 30 percent, respectively).

Change in Incidence of Payments Fraud in 2021 Compared to 2020
(Percentage Distribution of Organizations)





IMPACT OF REMOTE WORK ENVIRONMENT ON PAYMENTS FRAUD

Employees Working Remotely Only Partly to Blame for Some of the Fraud Increase

It has been two years since the world was confronted by the COVID-19 pandemic, resulting in social distancing measures and causing companies to require their staff to work remotely. Thirty-two percent of respondents believe that the increase in payments fraud at their companies was the result of employees working remotely, while 21 percent are unsure whether employees working away from the office had any impact on the incidence of payments fraud. Forty-seven percent do not believe that remote work is to blame for the reported increase in payments fraud at their organizations.

Of those who do believe employees working remotely had an effect on payments fraud activity, only 7 percent believe the share of increased fraud due to employees working remotely is greater than 50 percent. Eighteen percent of financial professionals report that one to 25 percent of any increase in fraud activity was likely due to employees working remotely, while 12 percent attribute 26 to 75 percent of any increased fraud instances was due to remote work.

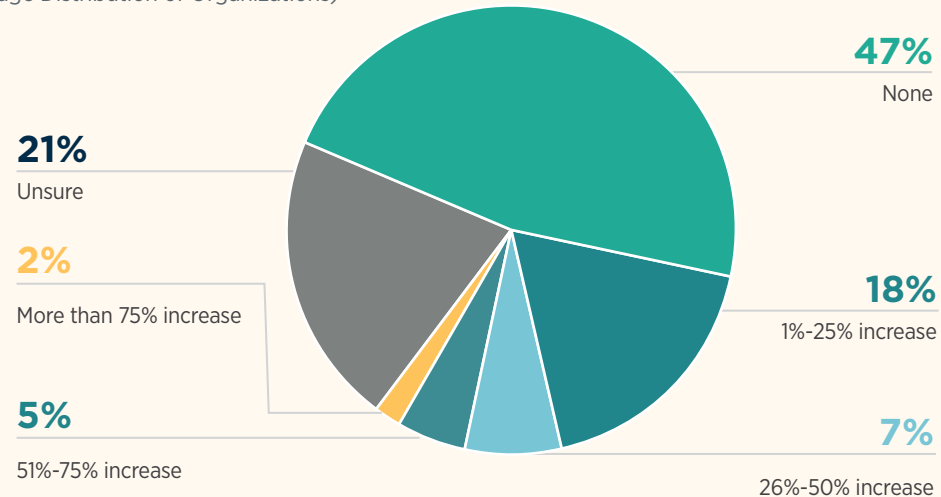
The pandemic provided those organizations whose staff worked working remotely with

a short learning curve to safeguard against payments fraud. Financial professionals resorted to best practices such as providing effective training at detecting fraud, shoring up policies and procedures and minimizing check usage. In addition, utilizing vendors/bank tools further helped to mitigate fraud. Tools such as Positive Pay, Payee Positive Pay, ACH Positive Pay and receiving alerts for possible fraudulent activity are several

examples of how companies have successfully combatted payments fraud.

A greater share of respondents from larger organizations with an annual revenue of more than \$1 billion report that the increase in payments fraud at their organizations was a result of employees working remotely compared to the share of those from smaller organizations with revenue less than \$1 billion (38 percent versus 23 percent).

Share of Increased Fraud due to Employees Working Remotely
(Percentage Distribution of Organizations)





PAYMENT METHODS IMPACTED BY FRAUD

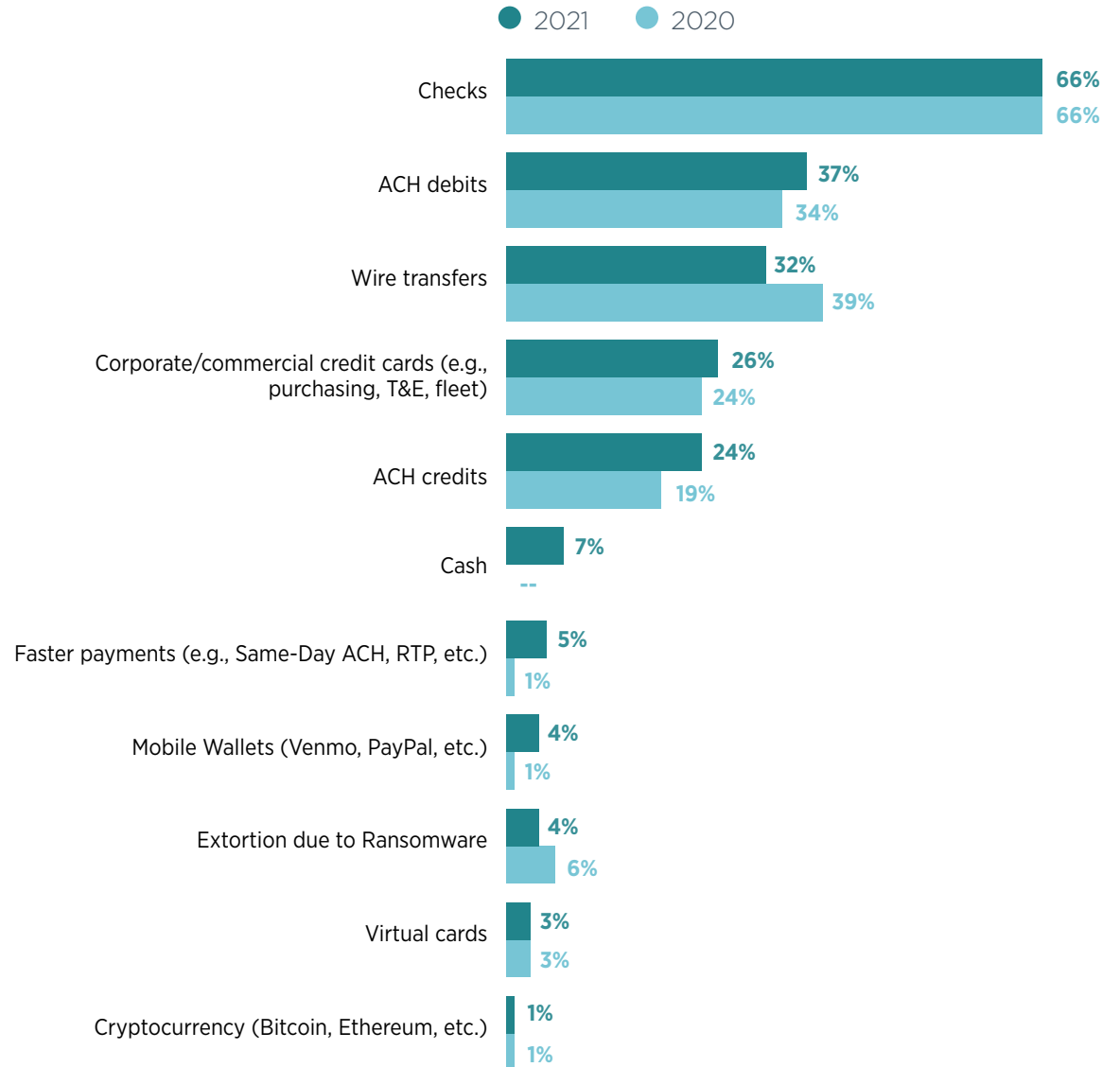
Checks and ACH Debits Most Susceptible to Payments Fraud

In 2021, checks and ACH debits were the payment methods most impacted by fraud activity (66 percent and 37 percent, respectively). Sixty-six percent of financial professionals report check fraud activity was unchanged from 2020 to 2021. Payments fraud via checks had been on the decline since 2010, with some intermittent upticks in between. Seventy percent of financial professionals reported that their organizations' check payments were subject to fraud attempts/attacks in 2018, while 74 percent reported the same for 2019. We then saw a decrease to 66 percent in 2020.

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. As noted in the *2019 AFP® Electronic Payments Survey*, however, check usage declined by nine percentage points from 2016 to 2019, and so likely also contributed to the decrease in check fraud activity. The decline in check fraud can also be due to organizations using fewer checks for business-to-business (B2B) transactions as well as the increased use of electronic payments due to staff working remotely.

Even as the incidence of payments fraud overall decreases, fraudsters are shifting their focus from paper payment methods to digital methods. The share of respondents reporting fraud via ACH debits increased from 34 percent in 2020 to 37 percent in 2021. The percentage of fraud

Payment Methods Subject to Attempted/Actual Payments Fraud
(Percent of Organizations)





PAYMENT METHODS IMPACTED BY FRAUD

activity via ACH debits has been increasing gradually—from 33 percent in 2019 to 34 percent in 2020 and to 37 percent in 2021. The three-percentage-point increase in fraud via ACH debits in 2021 could be a result of one of the following scenarios:

- Companies are shifting checks to digital, and with that shift organizations may also need to make sure the policies and procedures for identifying ACH debits promptly remain in place
- Conducting daily reconciliations rather than monthly
- Utilization of ACH debit filters/debit blocks
- Updating company IDs for filters on a timely basis
- Holding an independent review of the processes done by internal audit

Larger companies are more susceptible to fraud via ACH debits than are other organizations, and are collaborating with internal partners to identify and return ACH debits in a timely manner within the return window to help in preventing fraud.

The incidence of payments fraud via wire transfers decreased from 39 percent in 2020 to 32 percent 2021. The percentage of organizations that were victims of fraud via wire transfer has been on a steady decline—48 percent in 2017, 45 percent in 2018, 40 percent in 2019, 39 percent in 2020 and 32 percent

in 2021. Companies have become better at identifying wire fraud via business email compromise (BEC) scams; the steady decline in such fraud is proof that companies' efforts to combat wire fraud are working.

Apart from wire transfers and checks, the percentages of organizations that were victims of fraud attacks via corporate/commercial credit cards, ACH credits, faster payments and mobile wallets have increased from 2020 to 2021. Fraud attacks via corporate/commercial credit cards increased from 24 percent to 26 percent, fraud attacks via ACH credits increased from 19 percent to 24 percent, fraud attacks via faster payments increased from 1 percent to 5 percent and fraud attacks via mobile wallets increased from 1 percent to 4 percent.

A concern going forward is the rise in ACH credit and ACH debit fraud. With the Same Day ACH limit rising from \$100,000 to \$1 million effective March 18, 2022, companies will need to be extremely vigilant when monitoring their bank accounts for any transactions that appear to be out of the norm, unexpected, or can be simply returned and acted on quickly. NACHA's ACH WEB Debit Account Validation Rule (effective March 19, 2022) should help combat ACH fraud. According to the NACHA Operating Rule Supplement #2-2018: "Originators of WEB debits are required to use a 'commercially reasonable fraudulent transaction detection system'" to screen

WEB debits. The new rule makes explicit that account validation is an inherent part of any commercially reasonable fraudulent transaction detection system. Originators of WEB debits will be required to validate the Receiver's account number for its first use with a WEB debit entry, and for any subsequent changes to the account number, on a going-forward basis beginning on the effective date." According to AFP's 6th Edition of the *Essentials of Treasury Management: Web/Internet* format is used for payments that are not pre-authorized but are initiated by consumers using the internet. WEB entries can be either single payments for one-time purchases or recurring payments" It's worth having a conversation with your banking/vendor ACH partner to inquire on the status of their ACH Format sent as 38 percent of the 2021 ACH Network Volume was in the WEB/Internet Format,¹ which is higher than direct deposit volume and B2B volume.

In this year's survey, we asked respondents for the first time whether they experienced attempted/actual payments fraud via cash. Seven percent of respondents indicate that cash as a payment method was subjected to fraud.

Respondents from organizations with annual revenue of at least \$1 billion are more likely than those from other companies to report checks were subject to attempted or actual payments fraud in 2021 (74 percent compared to 61 percent for organizations with annual revenue less than \$1 billion).

¹2021 ACH Network Volume and Value Infographic (nacha.org)



BUSINESS EMAIL COMPROMISE

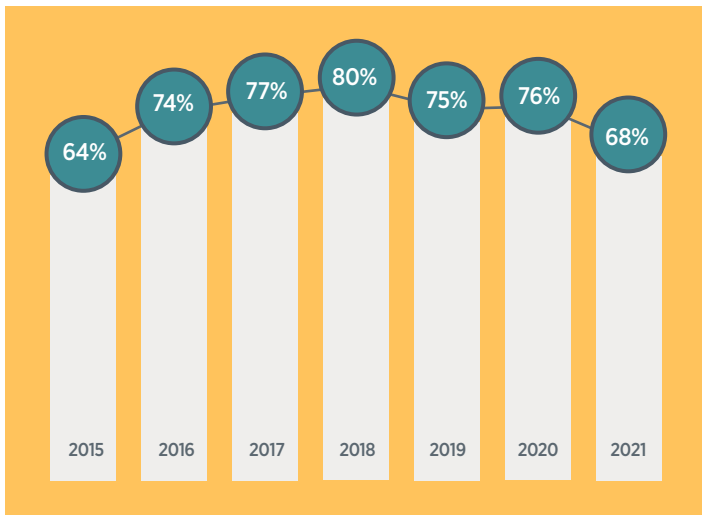


BUSINESS EMAIL COMPROMISE TRENDS

A Sharp Decrease in Business Email Compromise (BEC)

Sixty-eight percent of organizations were targeted by BEC in 2021, eight percentage points lower than in 2020 and the lowest figure reported since 2015. There has been a steady decrease in the past few years since 2018 when 80 percent of organizations experienced fraud via. This year's survey results reflect the most significant decrease in the history of AFP's reporting this data. Companies have become much better at identifying and mitigating this type of risk through better training and policies and procedures.

Percent of Organizations that Experienced Business Email Compromise (BEC), 2015-2021



Organizations Dealing with Fewer than 25 Instances of BEC Fraud in 2021

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

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

Few companies are reporting more than 25 instances of BEC fraud annually. Other types of BEC fraud respondents have experienced include fraud through Linked-In, regular spam emails, emails from personal vendors and malicious spam.

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

	LESS THAN 25 INSTANCES ANNUALLY	26-100 INSTANCES ANNUALLY	101-200 INSTANCES ANNUALLY	200+ INSTANCES ANNUALLY
Emails from fraudsters impersonating as vendors (using vendors' actual but hacked emails addresses) directing transfers based on real invoices to the fraudster's accounts.	86%	12%	1%	1%
Emails from other third parties requesting changes of bank accounts, payments instructions, etc.	85%	11%	1%	3%
Emails from fraudsters pretending to be senior executives using spoofed email domains directing finance personnel to transfer funds to the fraudsters' accounts	82%	15%	2%	1%



DEPARTMENTS MOST SUSCEPTIBLE TO BUSINESS EMAIL COMPROMISE

Accounts Payable Departments Sought After by Email Scamsters

Business email compromise scams continue to take various forms and change as criminals get more creative. While fraudsters might target an entire organization, they generally are more focused on Accounts Payable departments as that is where payments originate. Fifty-eight percent of respondents indicate that their Accounts Payable department was the most vulnerable business unit targeted. This is slightly lower than the 61 percent reported in the *2021 AFP® Payments Fraud and Control Report*. The other department most

susceptible to BEC fraud was the Treasury department (15 percent).

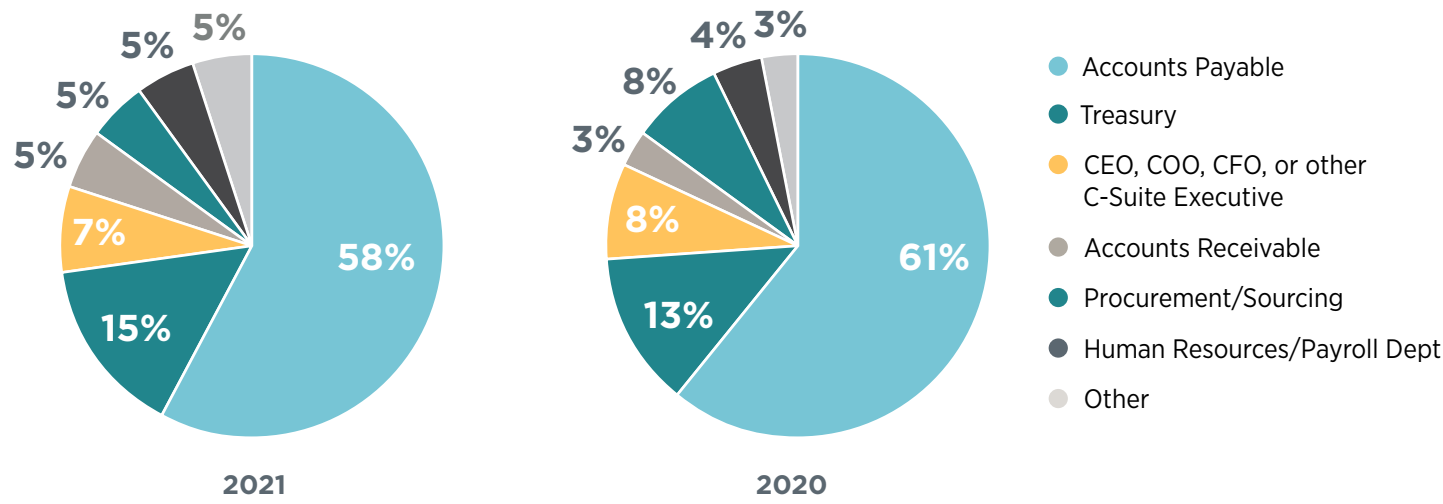
Accounts payable departments at larger organizations (those with annual revenue of more than \$1 billion and those with *both* annual revenue of more than \$1 billion and more than 100 payment accounts) are more vulnerable to BEC fraud (72 percent and 88 percent, respectively) than are other organizations. The larger the organization is, the more opportunity a fraudster has to take advantage of an Accounts Payable (AP) department due to the structure of the organization and the compartmentalized focus the AP group has

in terms of taking direction from its internal clients to make payments. Respondents from those companies with annual revenue of less than \$1 billion indicate that the CEO, COO, CFO or other C-Suite executives were the most targeted group by email scams.

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

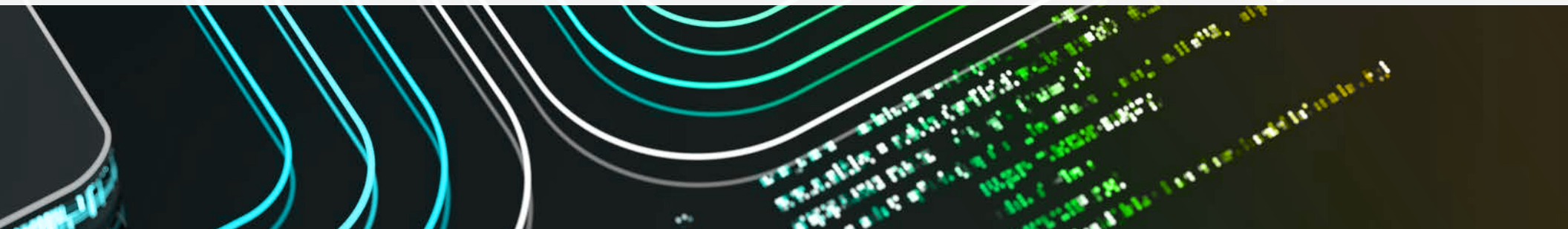
- Operations
- Sales
- Non-Finance professionals
- Customer Service

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





PAYMENTS FRAUD CONTROLS





VALIDATING PAYMENT BENEFICIARY INFORMATION AND SANCTION SCREENING

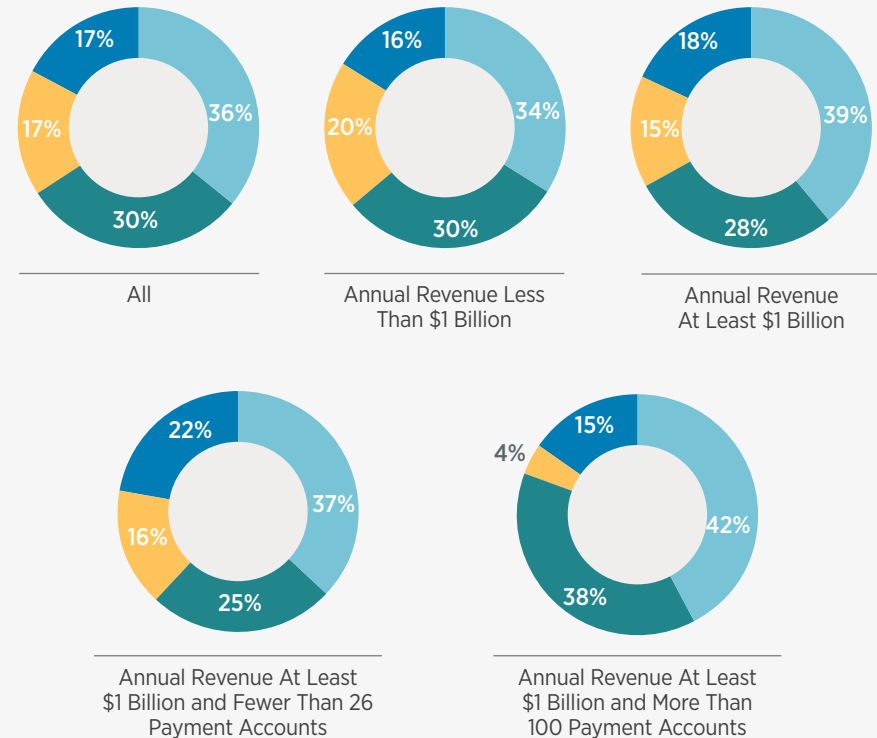
Majority of Organizations are Validating Payment Beneficiary Information

Two-thirds of organizations are validating payment beneficiary information, either through their vendor/bank (36 percent) or by using an external service (30 percent). Seventeen percent are not validating beneficiary payment information. Some respondents mentioned the following regarding how they are validating payment beneficiary information:

- Implementing a verification vendor
- Verbally validate for large transactions
- Payment information is verified for change requests
- Validate internally/staff validates
- Company validates with vendor
- In the process of setting up account validation
- Rely on dual confirmation
- Currently process is insufficient

Validating payment beneficiary information helps to reduce fraud and ensures that the intended beneficiaries receive their proceeds. It also helps from an Office of Foreign Asset Control (OFAC) reporting standpoint as well. If companies issue Web ACH Transactions/Internet ACH transactions, they will also be compliant with the new NACHA regulation which became enforceable as of March 19, 2022. Therefore, if sending WEB ACH transactions either through a bank, from a vendor or inhouse, it is important to utilize a service that is compliant with NACHA's Validation Requirement.

Percentage of Organizations that Validate Beneficiary Payment Information
(Percentage Distribution of Organizations)



- Rely on our financial vendor/bank to validate beneficiary payment information
- Organization uses an external service to validate beneficiary payment information
- Do not validate beneficiary payment information
- Other



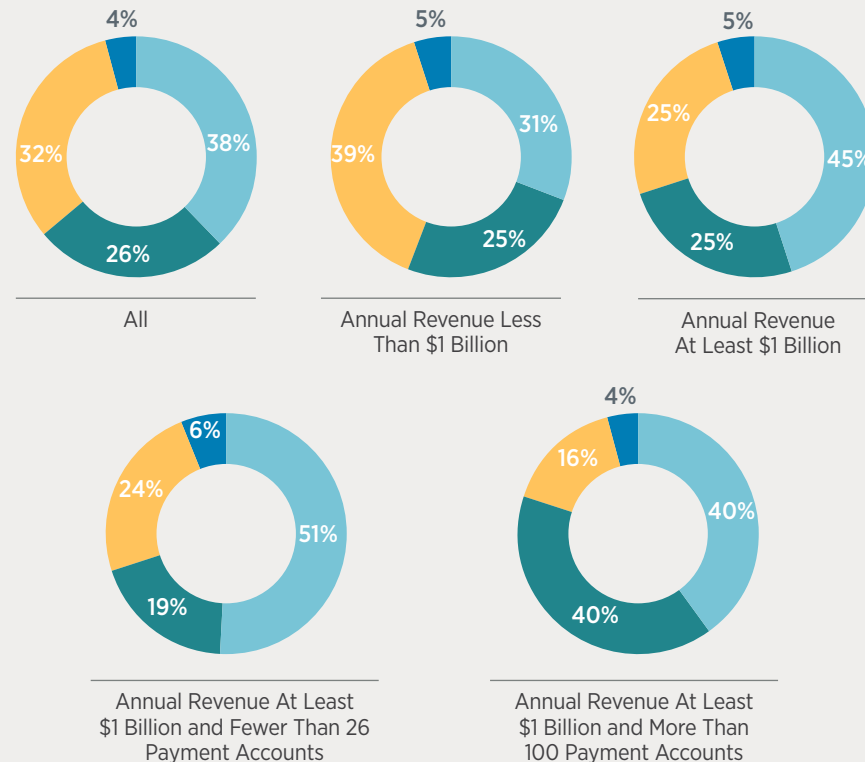
VALIDATING PAYMENT BENEFICIARY INFORMATION AND SANCTION SCREENING

Sanction Screening Primarily via Financial Vendor/Bank

Companies are taking a risk if sending payments to embargoed jurisdictions and/or entities included on various sanctions lists. It can lead to excessive fines, reputational damage and lengthy monitorships from regulators for the financial institutions sending the payments. Cross-border screening is more involved and thus more stringent compared with domestic screening. It is important to inquire regarding the processes that banks and vendors use to screen payments in order to ensure compliance with anti-money laundering regulations (making sure money is not routed to terrorist groups, sanctioned countries or individuals, etc.).

Organizations are conducting sanction screening; 38 percent are doing so via their financial vendor/bank and 26 percent are using an external service to conduct sanction screening. Thirty-two percent are not conducting sanction screening.

Percentage of Organizations that Conduct Sanction Screening
(Percentage Distribution of Organizations)



- Rely on our financial vendor/bank to conduct sanction screening
- Organization uses an external service to conduct sanction screening
- Do not validate sanction screening
- Other

CONCLUSION

After peaking at over 80 percent in 2018 and 2019, there has been a gradual decrease in the percentage of organizations being impacted by a payments fraud attack or attempt. While this is a positive sign, we cannot ignore the fact that over seven out of ten organizations were victims of fraud via payment methods in 2021. Corporate practitioners are well aware that fraud via payment methods is not going away anytime soon. Their efforts in curbing attacks appear to be working and they need to remain focused on staying ahead of the scamsters and remain vigilant as schemes change and evolve. Fraudsters seek to attack targets that lack protection or those with loose controls. Organizations need to equip their staff with the tools necessary to better manage the perils associated with payments fraud activity, making all efforts to implement measures that will impede fraudsters' success.

Technology will likely be used by perpetrators to commit crimes and inflict damage; fraudsters keep up to date with new technology and are constantly finding new schemes to capture funds from their targets. Those planning these attempts will be looking for loopholes and vulnerabilities to infiltrate organizations' payment systems. In turn, business leaders need to use technology to their advantage to ensure they have what is needed to stay ahead of these fraudsters

Similar to overall payments fraud activity, fraud via email is declining too. Senior leaders at organizations have implemented training for



employees to assist them in being cognizant of phishing emails and scams. A majority of respondents believes that educating employees on the threat of BEC and how to identify spear phishing attempts is a crucial element in efforts to control BEC. Organizations

test employee attentiveness by sending out simulated emails; some have introduced aggressive email filtering software and have special messages included on internal emails. In addition to these strategies, companies are implementing policies for providing

appropriate verification of any changes to existing invoices, bank deposit information and contact information and have controls to eliminate payments initiation based on emails or other less secure messaging systems. While it is encouraging to see the downward trend in BEC fraud, it is disconcerting that even today, over 50 percent of organizations are victims of BEC fraud.

Checks continue to be the payment method most targeted by fraud, although the incidence of check fraud activity is similar to that reported in last year's survey. While payments fraud via wires were the second-most targeted payment method by fraudsters in past years, in 2021 ACH debits were the second most popular payment method targeted. This emphasizes how criminals are relentless in their efforts to commit fraud and constantly seeking areas where they can infiltrate their target's payment systems. This needs to be monitored closely as the concern with fraud via ACH debits is on the rise. Utilizing simple banking tools to mitigate this risk such as ACH filters and blocks will help to alleviate the concern. More importantly, having a full suite of proper controls in place by reconciling activity on a regular basis, separation of duties and having a good banking/vendor partner to fully understand best practices in preventing this type of fraud is very helpful.

It is encouraging that payments fraud activity is moving in the right direction, and the decline in overall payments fraud can very well be attributed to vigilant financial professionals who are actively implementing strategies

preventing their organizations from being vulnerable targets for payments fraud. But it is also likely that the pandemic-induced changes in the way operations and processes are being conducted resulted in obstruction of fraud activity. Companies sought to patch up deficiencies in their controls, policies and procedures as well as provide education efforts to equip their staff at being better prepared in detecting risk.

Effectively combating payments fraud requires more than just robust internal controls. Financial professionals need to prioritize payments fraud in their strategies and tactics. Importantly, they must think "outside the box" and keep up to date on new technologies—fraud perpetrators certainly do. Organizations and their finance staff must be prepared to take and invest in the measures necessary to prevent fraudsters from being successful. The more frequently organizations succumb to these attacks, the more encouraged those fraudsters will be.





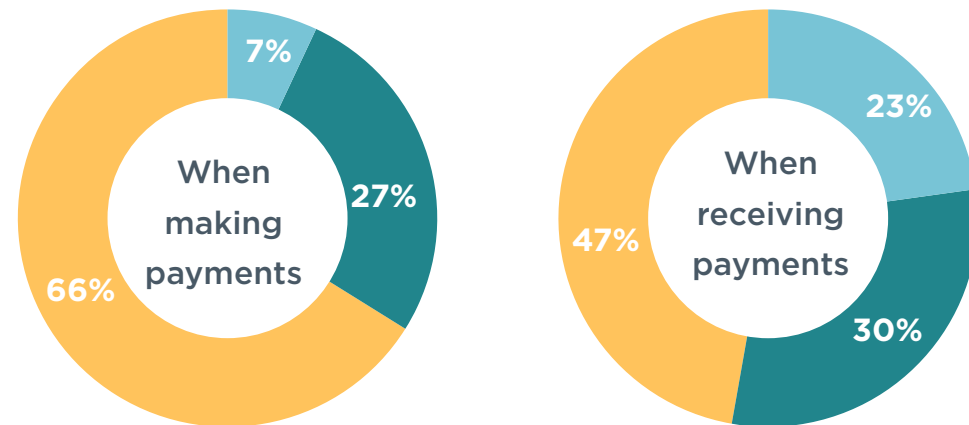
DEMOGRAPHICS

ABOUT RESPONDENTS

In January 2022, the Research Department of the Association for Financial Professionals® (AFP) surveyed its corporate practitioner members and prospects. The survey was sent to corporate practitioners with the following job titles: Vice President of Treasury, Treasurer, Assistant Treasurer, Director of Treasury, Treasury Manager, Director of Treasury and Finance, Senior Treasury Analyst, and Cash Manager. A total of 552 responses were received from practitioners, which form the basis of the report.

AFP thanks J.P. Morgan for Underwriting the *2022 AFP® Payments Fraud and Control Survey*. Both the 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)



● Primarily consumers ● Split between consumers and businesses ● Primarily businesses

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%	30%	14%	26%	--
5-9	18%	20%	16%	31%	--
10-25	20%	18%	23%	43%	--
26-50	9%	8%	10%	--	21%
51-100	9%	6%	13%	--	27%
More than 100	21%	18%	24%	--	52%

ABOUT RESPONDENTS

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%	73%	84%	61%
Decentralized	16%	12%	21%	13%	31%
Other	4%	2%	6%	3%	8%

Accounts that Controls are Applied to

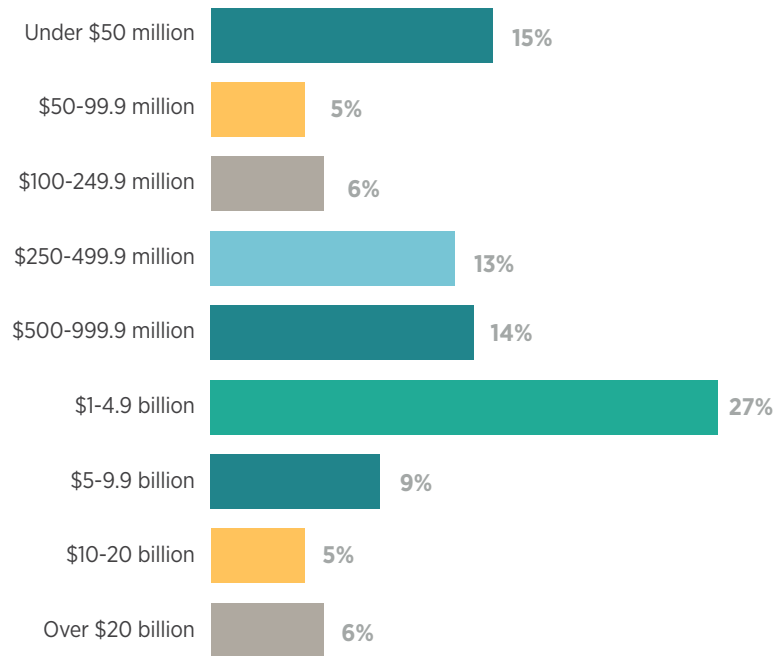
(Percentage Distribution of Organizations)

	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	84%	84%	82%	84%	80%
Applied to all accounts in select areas	9%	10%	10%	9%	12%
Not applied to all accounts	6%	6%	6%	7%	6%
Other	1%	--	2%	--	2%

ABOUT RESPONDENTS

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	36%	19%	57%	52%	61%
Privately held	41%	54%	26%	28%	25%
Nonprofit (not-for-profit)	15%	19%	10%	10%	10%
Government (or government-owned entity)	8%	8%	7%	10%	4%

Industry Classification

(Percentage Distribution of Organizations)

	ALL
Agricultural, Forestry, Fishing & Hunting	1%
Administrative Support/Business services/Consulting	2%
Banking/Financial services	13%
Construction	3%
E-Commerce	2%
Energy	3%
Government	5%
Health Care and Social Assistance	8%
Hospitality/Travel/Food Services	2%
Insurance	5%
Manufacturing	16%
Non-profit	9%
Petroleum	1%
Professional/Scientific/Technical Services	2%
Real estate/Rental/Leasing	5%
Retail Trade	3%
Wholesale Distribution	4%
Software/Technology	4%
Telecommunications/Media	4%
Transportation and Warehousing	4%
Utilities	4%

AFP® 2022 Payments Fraud and Control Report
Copyright © 2022 by the Association for Financial Professionals (AFP).
All Rights Reserved.

This work is intended solely for the personal and noncommercial use of the reader. All other uses of this work, or the information included therein, is strictly prohibited absent prior express written consent of the Association for Financial Professionals. The *AFP® 2022 Payments Fraud and Control Report* the information included therein, may not be reproduced, publicly displayed, or transmitted in any form or by any means, electronic or mechanical, including but not limited to photocopy, recording, dissemination through online networks or through any other information storage or retrieval system known now or in the future, without the express written permission of the Association for Financial Professionals. In addition, this work may not be embedded in or distributed through commercial software or applications without appropriate licensing agreements with the Association for Financial Professionals.

Each violation of this copyright notice or the copyright owner's other rights, may result in legal action by the copyright owner and enforcement of the owner's rights to the full extent permitted by law, which may include financial penalties of up to \$150,000 per violation.

This publication is **not** intended to offer or provide accounting, legal or other professional advice. The Association for Financial Professionals recommends that you seek accounting, legal or other professional advice as may be necessary based on your knowledge of the subject matter.

All inquiries should be addressed to:

Association for Financial Professionals
4520 East West Highway, Suite 800
Bethesda, MD 20814

301.907.2862

AFP@AFPonline.org

www.AFPonline.org



**ASSOCIATION FOR
FINANCIAL
PROFESSIONALS**

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

+1 301.907.2862

www.AFPonline.org

J.P.Morgan



Most companies will experience fraud

Don't be one of them. Be protected.

Learn how our advanced prevention tools
and exclusive resources can help defend
your organization.

[GET EXPERT SOLUTIONS](#)

