ASSOCIATION FOR FINANCIAL PROFESSIONALS

2022 AFP®

Payments Fraud and Control Report

Comprehensive Findings

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

TABLE OF CONTENTS

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.

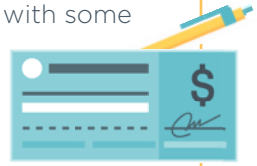
KEY FINDINGS

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.

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.

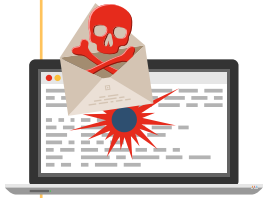
Employees Working Remotely Only Partly to Blame for Any Increase in Payments Fraud at their Organizations

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.

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

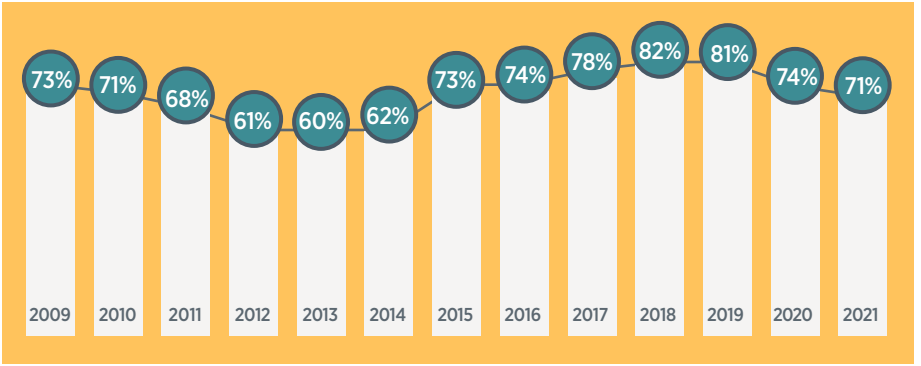
PAYMENTS FRAUD TRENDS

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

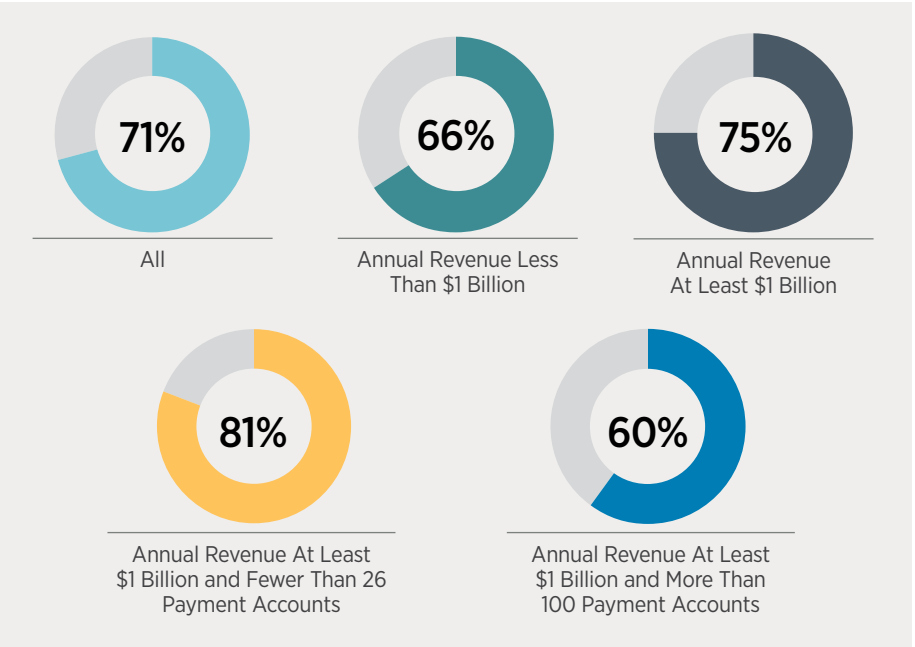
From 2009-2013, the percentage of organizations that experienced attempted or actual payments fraud steadily declined. In 2015, there was an uptick in the share of companies that were victims of payments fraud attempts and attacks: 73 percent of organizations were targets of payments fraud in 2015—a 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

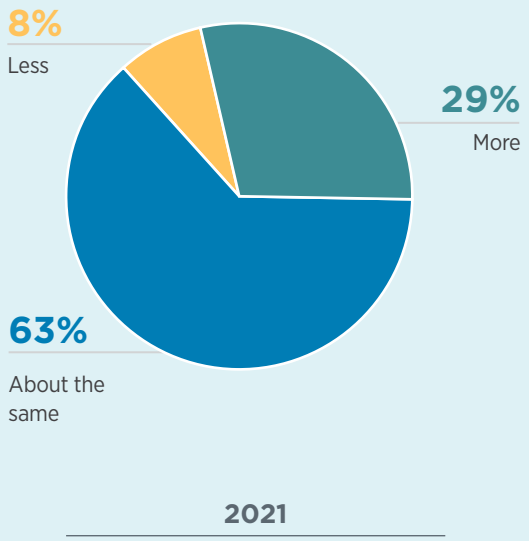


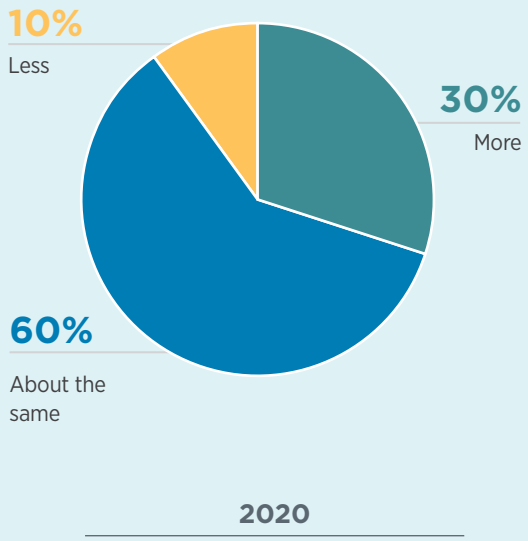
PAYMENTS FRAUD TRENDS

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

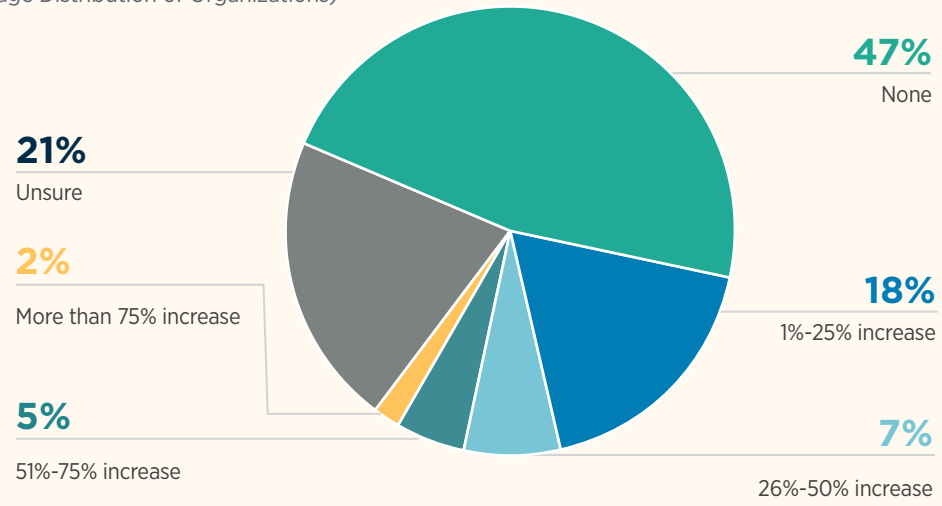
It has been two years since the world was confronted by the COVID-19 pandemic, resulting in social distancing measures and causing companies to require their staff to work remotely. Thirty-two percent of respondents believe that the increase in payments fraud at their companies was the result of employees 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

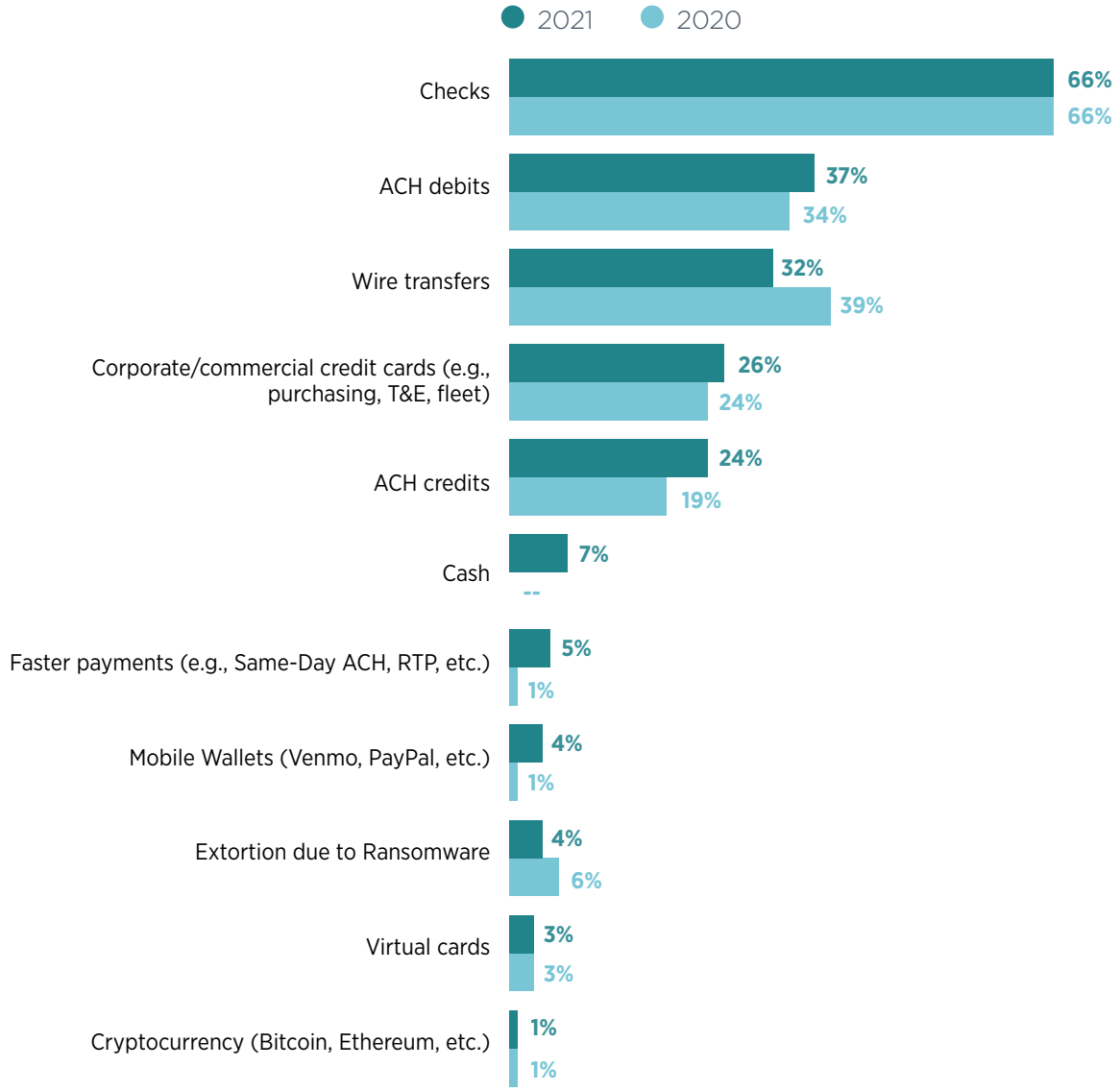
Checks and ACH Debits Most Susceptible to Payments Fraud

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).

[1] 2021 ACH Network Volume and Value Infographic (nacha.org)

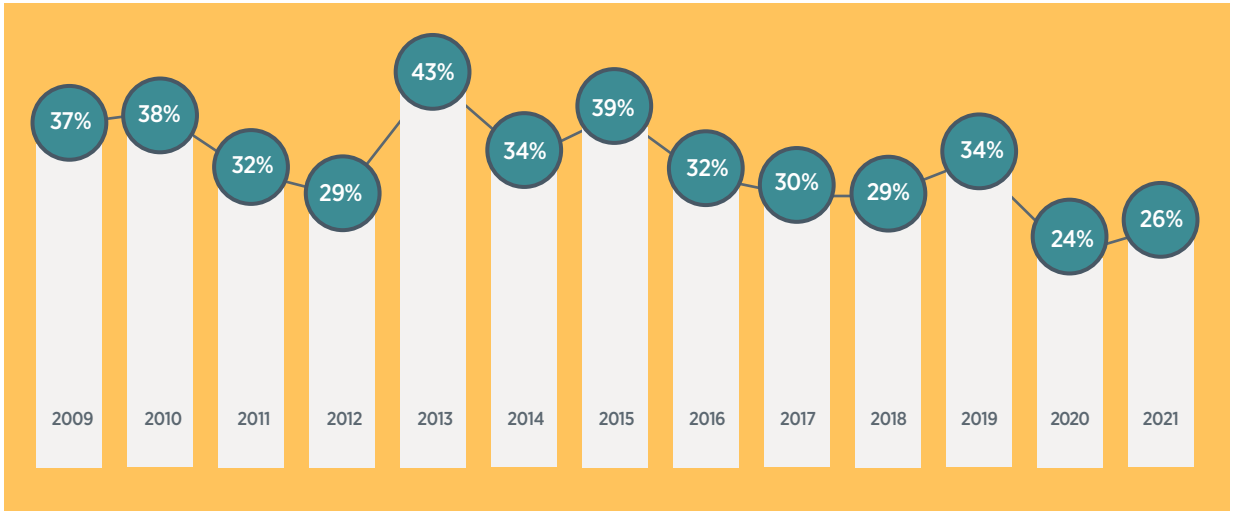
CORPORATE/COMMERCIAL CREDIT CARD FRAUD

Steady Trends for Corporate/ Commercial Credit Card Fraud

Twenty-six percent of financial professionals report that their organizations were subject to corporate/ commercial credit card fraud in 2021. That is a slight increase from the 24 percent reported in 2021, but lower than credit card fraud recorded in prior years.

The types of corporate/commercial cards most prone to payments fraud in 2021 were purchasing cards (49 percent) and travel & entertainment (T&E) cards (44 percent). These figures are significantly lower than those for 2020 (61 percent and 79 percent, respectively). This decrease can be attributed to the travel restrictions imposed by companies due to the COVID-19 pandemic. Employees were using these cards far less frequently than they had in the past.

Percent of Organizations that Experienced Payments Fraud through Corporate/Commercial Credit/ Debit Cards, 2009-2021



CORPORATE/COMMERCIAL CREDIT CARD FRAUD

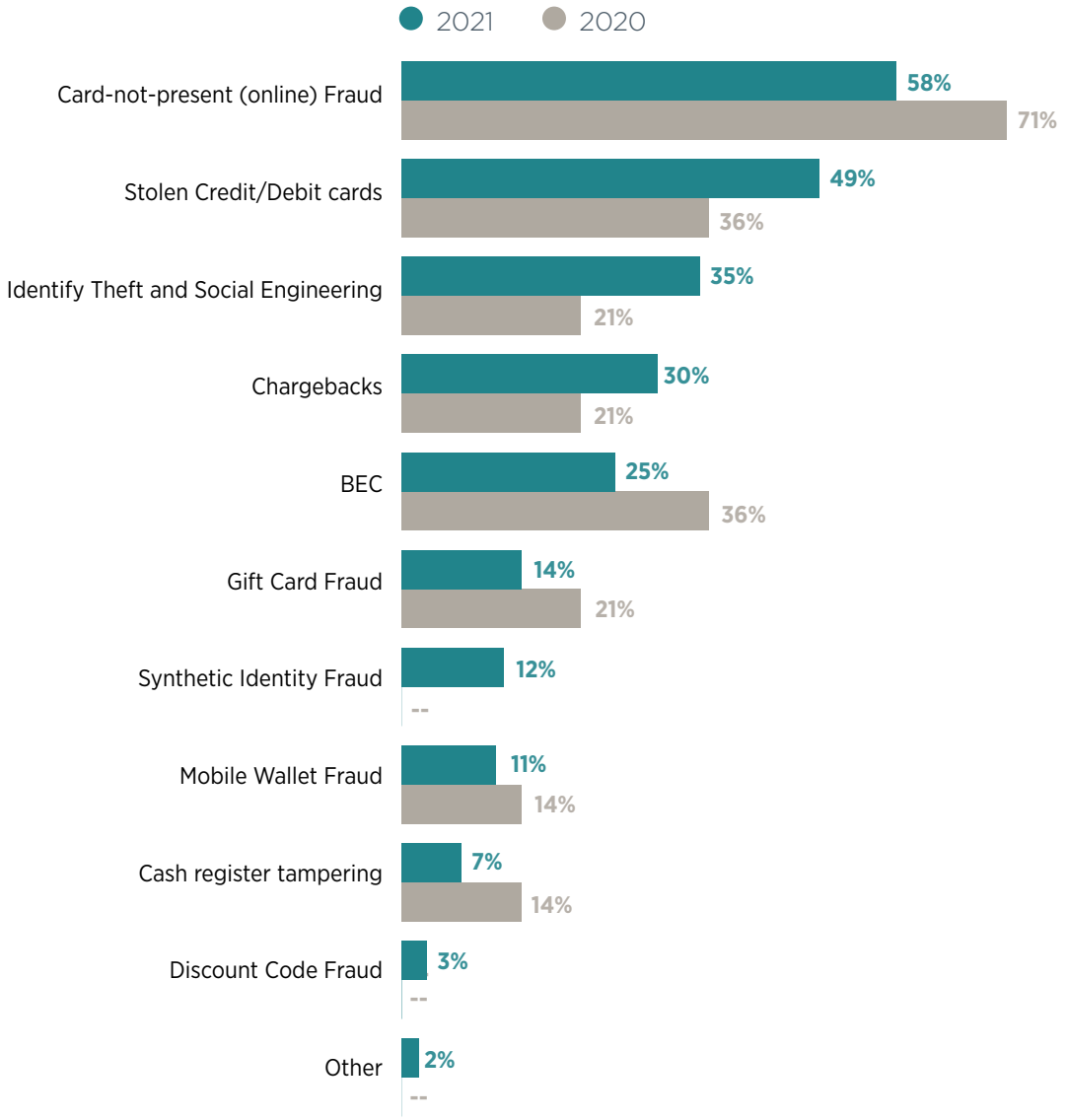
Major concerns among survey respondents regarding card fraud are card-not-present during transactions (cited by 58 percent of respondents), stolen credit/debit cards (49 percent, an increase of 13 percentage points from last year), identity theft and social engineering (35 percent, an increase of 14 percentage points from last year).

Only 14 percent of respondents indicate that their organizations actually suffered a financial loss due to corporate/commercial card fraud. The main reason for the loss suffered by these companies was fraudulent credit card charges made by a third party (78 percent), while 22 percent of respondents report that fraud was initiated by an employee.

Other concerns regarding fraud reported include:

- Lack of dual authorization
- Not relevant to our business
- Email scams and phone calls

Major Concerns Regarding Card Fraud
(Percent of Organizations)

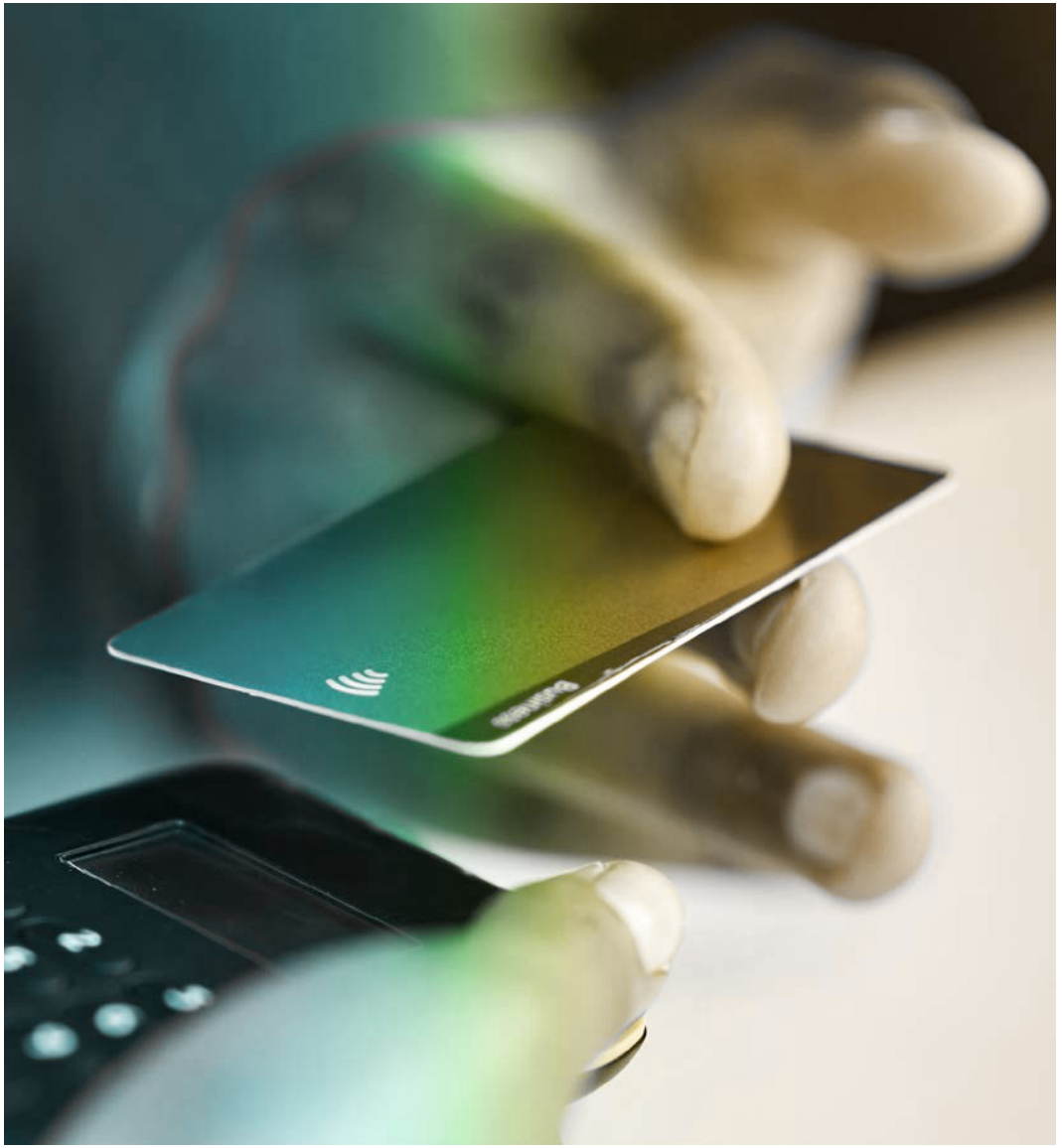


CORPORATE/COMMERCIAL CREDIT CARD FRAUD

Payments fraud via corporate credit cards steadily declined from 2009-2012. Then there was a substantial uptick in fraud via credit cards in 2013. Since then the percentage of organizations experiencing this type of fraud has fluctuated with an increase in some years and in others a decrease.

The concerns and issues surrounding credit card fraud have been fairly consistent over the years. Travel & entertainment cards and purchasing cards are still the most vulnerable to fraud. At a majority of companies, the primary cause of card fraud is fraudulent charges made by a third party, again similar to past years. Financial professionals are continuing to grapple with card fraud and have not, as yet, had much success in preventing instances of such fraud.

Unauthorized online charges frequently appear on our corporate credit cards. When this happens, the fraud is reported to our card provider and they have always been very helpful with crediting back the fraudulent charges and issuing replacement cards.



LOSSES INCURRED DUE TO PAYMENTS FRAUD ATTACKS/ATTEMPTS

Estimated Total Dollar Amount of Actual Financial Loss and Costs to Manage Fraud

Historically, actual financial losses from payments fraud attacks are not extensive, and that continued to be the case in 2021. Fifty-five percent of respondents report that their organizations faced potential financial losses totaling less than $50,000 (or no loss) as a result of payments fraud activity in 2021. Twenty-one percent of financial professionals indicate there were no potential losses at their companies, while seven percent indicate that over $2 million may have been lost. Loss of confidential and personnel information, however, while not a direct impact on the bottom line, required extensive efforts to resolve.

Potential Financial Loss from Attempted and/or Actual Payments Fraud in 2021

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

TOTAL DOLLAR AMOUNT	
ZERO	21%
UP TO $24,999	24%
$25,000-49,999	10%
$50,000-99,999	9%
$100,000-249,999	13%
$250,000-499,999	7%
$500,000-999,999	5%
$1,000,000-1,999,999	4%
$2,000,000 OR MORE	7%

Actual direct financial losses were less than *potential* losses. Sixty percent of financial professionals report that their organizations did not incur an actual financial loss as a result of fraud activity, while 20 percent report an actual financial loss of less than $25,000.

Actual Direct Financial Loss from Payments Fraud in 2021

(Percentage Distribution of Organizations that Experienced Payments Actual Payments Fraud)

TOTAL DOLLAR AMOUNT	
ZERO	60%
UP TO $24,999	20%
$25,000-49,999	6%
$50,000-99,999	5%
$100,000-249,999	6%
$250,000-499,999	1%
$500,000-999,999	2%
$1,000,000-1,999,999	--
$2,000,000 OR MORE	--

Costs to manage, defend and/or clean up from fraud attacks were relatively low for most organizations that experienced such attacks. Forty-four percent of companies did not incur any expenses due to a fraud attempt and 35 percent spent less than $25,000 to defend against or clean up the fraud.

Costs to Manage/Defend/Cleanup from Attempted and/or Actual Payments Fraud in 2021

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

TOTAL DOLLAR AMOUNT	
ZERO	44%
UP TO $24,999	35%
$25,000-49,999	7%
$50,000-99,999	6%
$100,000-249,999	6%
$250,000-499,999	1%
$500,000-999,999	1%
$1,000,000-1,999,999	--
$2,000,000 OR MORE	--

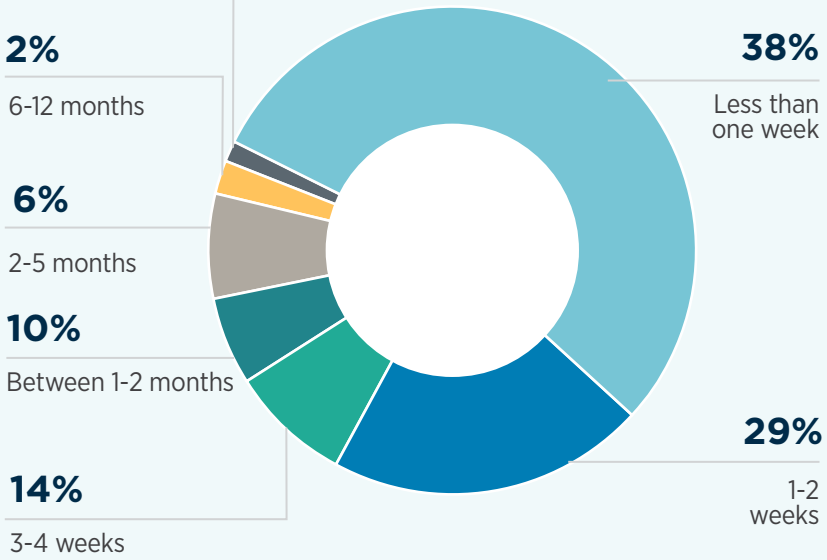
DETECTING FRAUD ACTIVITY

Time Taken to Uncover Fraud

Of those organizations that were victims of payments fraud attacks in 2021, 38 percent detected the fraudulent activity in less than one week. Forty-three percent uncovered the fraud attack within one to four weeks; a mere one percent took one to two years before realizing they had been targeted. Over 80 percent of respondents identified fraud within a month—the typical timeframe within which bank reconcilements are done. With the move to larger Same Day ACH Windows and the rise in fraud via ACH debit and ACH credit, there is room for improvement in organizations' ability to detect occurrences of fraud promptly. If fraud is not detected within the first few days, the chances of a recovery from the fraud are slim.

A fraudster with the CEO's email address with one character changed, sent AP an urgent wire transfer request. This was very out of the ordinary and AP followed up with the CEO via phone call to discover it was a fraudulent attempt.

Time Taken to Discover Fraud
(Percentage Distribution of Organizations)



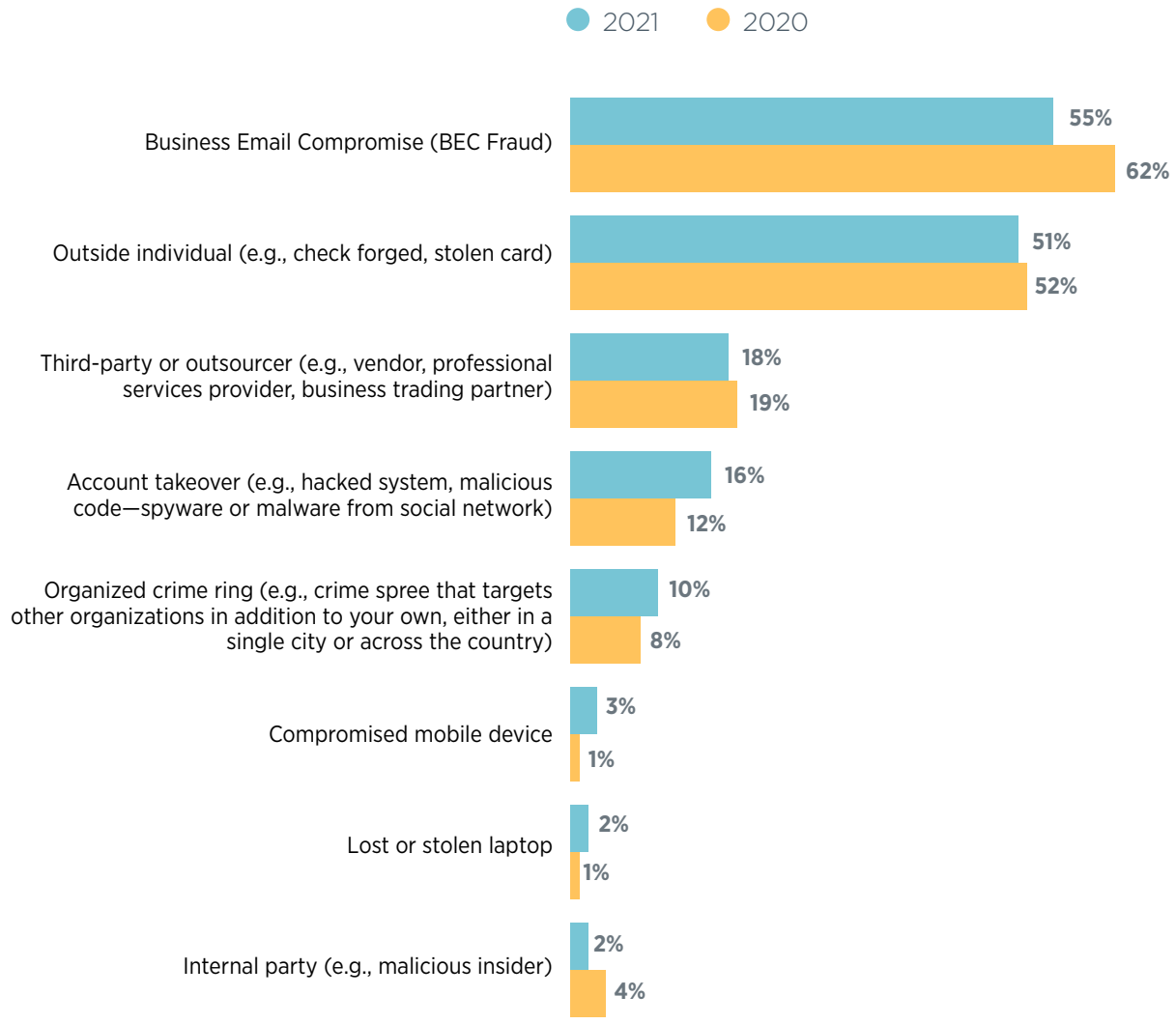
PRIMARY SOURCES OF ATTEMPTED/ACTUAL PAYMENTS FRAUD

Majority of Payments Fraud Continues to Originate from Business Email Compromise (BEC)

In 2021, the majority of payments fraud attempts/attacks originated from Business email compromise (BEC). Fifty-five percent of companies that experienced attempted or actual payments fraud in 2021 did so as a result of BEC. 2019 was the first year that BEC topped the list of "sources" of fraud attempts and it continues be the dominant source of payments fraud. In 2019, 61 percent of respondents cited BEC as a source of fraud; in 2020 the share inched up to 62 percent. In 2021, although BEC continued to be the chief reason organizations were experiencing fraud, the share of organizations (55 percent) that cited BEC as a reason for payments fraud at their companies decreased from past years.

The second most-common source of payments fraud in 2021 was an external source or individual (e.g., forged check, stolen card); 51 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 18 percent of organizations). Account takeovers (e.g., hacked system, phishing, spyware or malware) are reported by 16 percent of respondents from companies that experienced attempted/actual payments fraud.

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



PRIMARY SOURCES OF ATTEMPTED/ACTUAL PAYMENTS FRAUD

It is encouraging to see a further decline in the percentage of companies experiencing fraud due to BEC, suggesting that the controls and measures being implemented to curb BEC are having some success. A larger share of respondents from companies with annual revenue of at least $1 billion and fewer than 26 payment accounts were targets of BEC fraud (62 percent) in 2021, similar to the 61 percent reported in last year's survey. Organizations continue to be targeted by outside individuals (51 percent) and to a similar extent as in past years. While it is challenging to anticipate these types of attacks, financial professionals cannot let their guard down; implementing controls that safeguard against these fraudsters' attacks might need to be a focus going forward. 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.

BUSINESS EMAIL COMPROMISE

ABOUT BUSINESS EMAIL COMPROMISE

Business Email Compromise[2]

Business email compromise (BEC)—also known as email account compromise (EAC)—is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business—both personal and professional.

In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request, like in these examples:

- A vendor your company regularly deals with sends an invoice with an updated mailing address.
- A company CEO asks her assistant to purchase dozens of gift cards to send out as employee rewards. She asks for the serial numbers so she can email them out right away.
- A homebuyer receives a message from his title company with instructions on how to wire his downpayment.

Versions of these scenarios happened to real victims. All the messages were fake. In each case, thousands—or even hundreds of thousands—of dollars were sent to criminals instead.

How Criminals Carry Out BEC Scams[3]

A scammer might:

- **Unauthorized use of Online Meeting Platform. "**An individual compromises legitimate business email accounts through social engineering to conduct unauthorized transfers of funds using a still picture of the CEO or CFO and utilize "Deep Fake" audio and claim their video/audio is not properly working. They then direct a transfer of funds via the chat function or a follow up email."
- **Spoof an email account or website.** Slight variations on legitimate addresses (john.kelly@examplecompany.com vs. john.kelley@examplecompany.com) fool victims into thinking fake accounts are authentic.
- **Send spear phishing emails.** These messages look like they're from a trusted sender to trick victims into revealing confidential information. That information lets criminals access company accounts, calendars and data that give them the details they need to carry out the BEC schemes. According to data sources (KnowBe4),[4] 91 percent of all data breaches start with a spear phishing attack.
- **Use a compromised email account.** Criminals will sometimes use compromised email accounts to send fraudulent change of payment instructions to potential victims.
- **Use malware.** Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages, so accountants or financial officers don't question payment requests. Malware also lets criminals gain undetected access to a victim's data, including passwords and financial account information.

An email from an executive in an external entity asking to process an invoice urgently. We did a call back to a known number for the executive and found out it was not them.

[2] Source: Internet Crime Complaint Center (IC3) | Business Email Compromise: Virtual Meeting Platforms

[3] Source: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

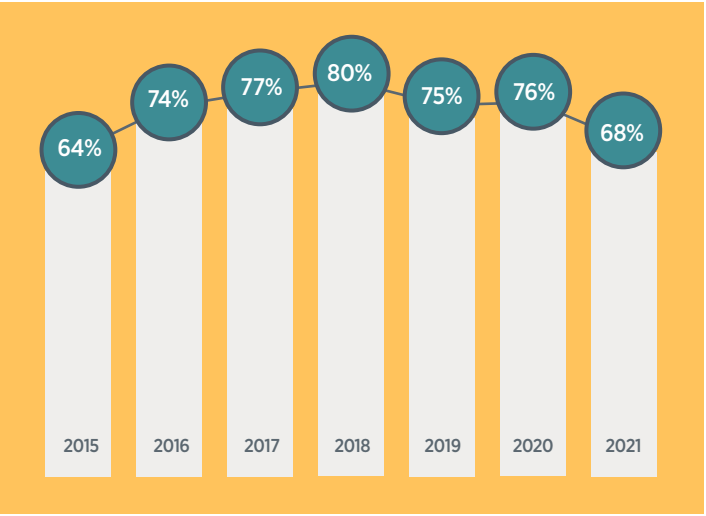
[4] Source: http://www.Knowbe4.com

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%

FINANCIAL IMPACT OF BUSINESS EMAIL COMPROMISE

Financial Impact of Business Email Compromise Remains Unchanged

Although the percentage of organizations falling victim to BEC fraud has decreased in the last year, the percentage of financial professionals reporting that their companies suffered a financial loss due to BEC is unchanged. Companies have attempted to mitigate BEC fraud by providing employee education and training, using verification methods and call-back features to confirm payment requests, and implementing company policies on handling changes to existing bank accounts. The sharp decrease of fraud in the past year is evidence that these the measures are working.

Thirty-five percent of companies experienced a financial loss because of these email scams in 2021—similar to the 34 percent reported for 2020. Both figures are the lowest reported in recent years. In 2019, over half of companies (54 percent) were impacted by a financial loss because of BEC and 46 percent of organizations experienced a loss due to BEC in 2018. The steady decrease in the incidence of financial loss as a result of email scams can be attributed to organizations providing extensive training to their employees as well as being proactive in implementing controls.

While the majority of respondents that *does* report their companies incurred a loss indicate that the loss experienced was less than $50,000, a higher percentage of respondents report incurring a loss of between $50,000 and $499,999 in 2021 compared to 2020 (15 percent versus 11 percent). Nineteen percent of organizations with annual revenue of at least $1 billion suffered a loss of between $50,000 and $499,999, which suggests that perpetrators are targeting larger organizations to steal larger amounts of money.

Of course, non-financial losses can result from BEC as well. For example, if a fraud attack exposes personal or confidential information, the damages can be severe and difficult to quantify.

Estimated Total Dollar Loss to Organizations from BEC in 2021
(Percentage Distribution of Organizations)

	2021	2020
No Loss	65%	66%
Up to $24,999	13%	14%
$25,000-49,999	5%	7%
$50,000-99,999	6%	4%
$100,000-249,999	6%	4%
$250,000-499,999	3%	3%
$500,000-$999,999	2%	2%
$1,000,000-1,999,999	--	--
Over $2,000,000	--	--

Someone tried to take over a participant 401k account and withdraw the funds. It was luckily stopped by a coincidental issue and we discovered it was not the participant who requested the withdrawal. Stronger controls and adding some verification is planned.

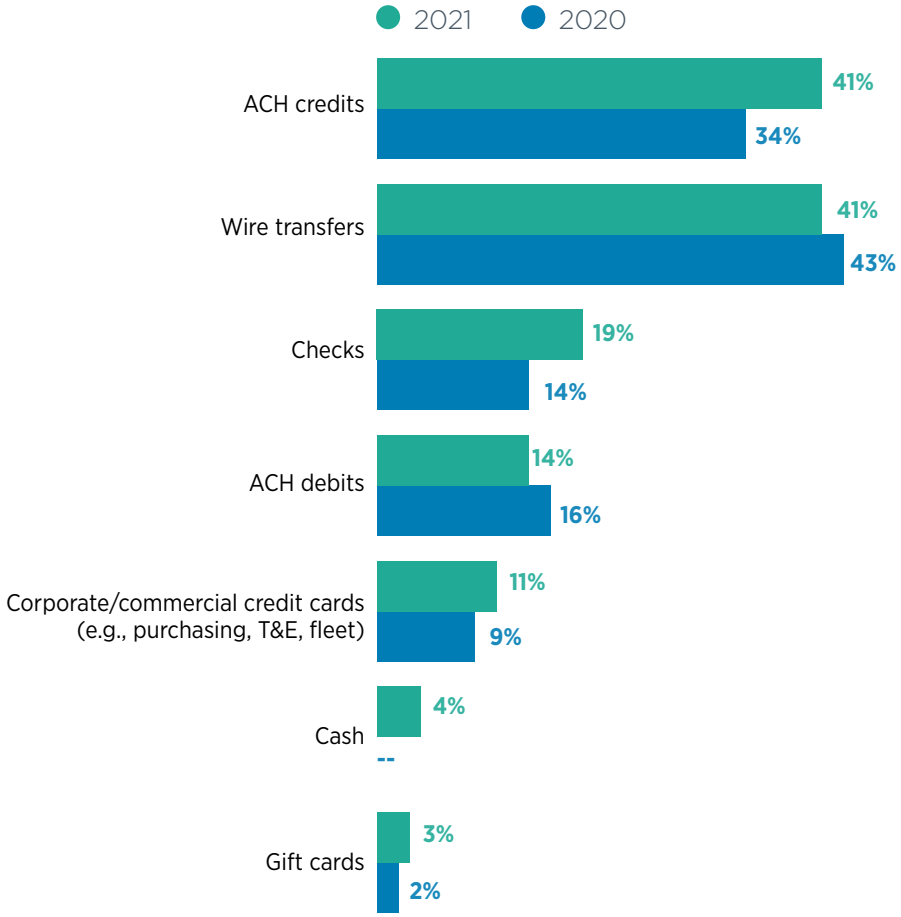
TARGETS OF BUSINESS EMAIL COMPROMISE SCAMS

ACH Credits and Wire Transfers Continue to be Prime Targets for Business Email Compromise Scams

Forty-one percent of financial professionals report that wire transfers were impacted by BEC, a slight decrease from 43 percent in last year's report and the 42 percent reported in 2020. While in past years wire transfers were the most popular payment method targeted for BEC scams, in 2021 they tied with ACH credits as the most often targeted method. Forty-one percent of respondents report that ACH credits at their organizations were impacted by email fraud in 2021—higher than the 34 percent in 2020 and the 37 percent in 2019.

The share of practitioners reporting that ACH debits were impacted by BEC decreased from 21 percent in 2020 to 16 percent in 2021. The percentage of financial professionals reporting that BEC compromised their organizations' check payments decreased five percentage points—from 19 percent in 2020 to 14 percent in 2021. The shift to targeting ACH transactions via BEC is likely because ACH is an easier touchpoint for those attempting to commit fraud, while checks (as noted earlier) are being used less frequently. Another reason fraudsters target ACH when using BEC is because they are aware that businesses pay their bills using ACH. Wires are expensive; therefore, organizations use ACH instead and perpetrators of these attacks are using this information and targeting ACH using emails.

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



DEPARTMENTS MOST SUSCEPTIBLE TO BUSINESS EMAIL COMPROMISE

Accounts Payable Departments Sought After by Email Scamsters

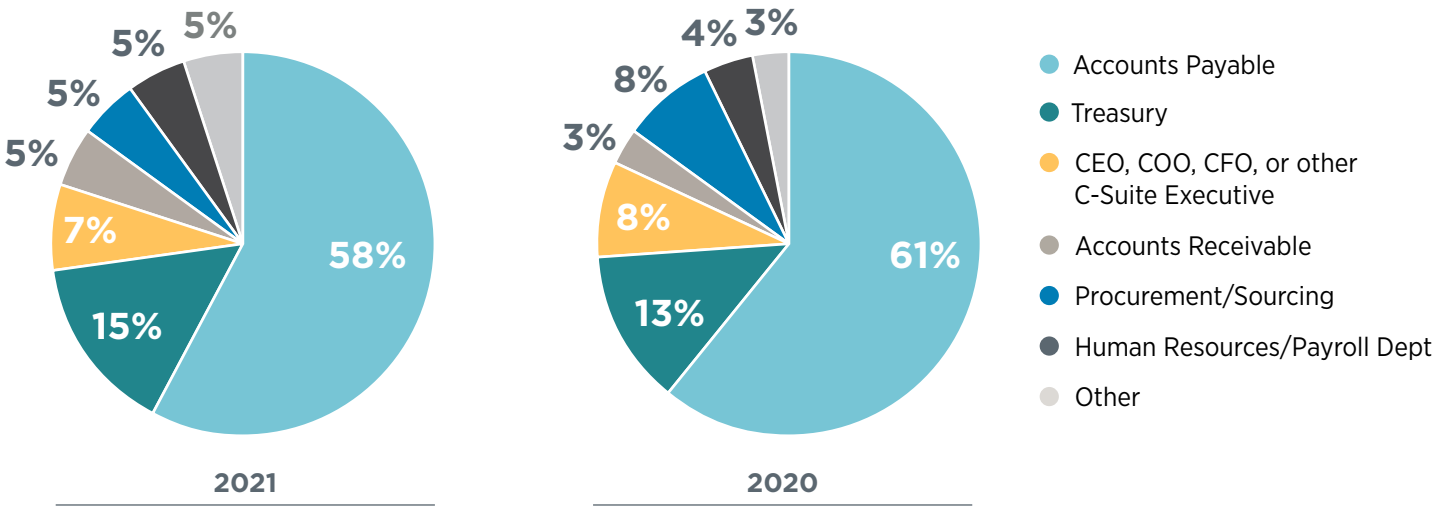
Business email compromise scams continue to take various forms and change as criminals get more creative. While fraudsters might target an entire organization, they generally are more focused on Accounts Payable departments as that is where payments originate. Fifty-eight percent of respondents indicate 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

BUSINESS EMPLOYEE COMPROMISE (BEC) CONTROLS

Employee Training Will Protect Against Email Scams

Business email compromise continues to be 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 compromised. Nearly three-fourths of respondents believe that educating employees on the threat of BEC and how to identify spear phishing attempts crucial elements in efforts to mitigate BEC. Providing education to combat BEC Fraud has been an effective solution. Companies will need to make sure all their payment methods are protected in the same manner—i.e., checks are as protected as are wires, ACH payments, Real-Time payments, etc.

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

End-user education and training on the BEC threat and how to identify spear phishing attempts — **74%**	Implemented company policies for providing appropriate verification of any changes to existing invoices, bank deposit information and contact information — **68%**	Stronger Internal Controls prohibiting payments initiation based on emails or other less secure messaging systems — **61%**	Confirm requests for transfer of funds by executing a call back to a verified and authorized contact at the payee organization using a phone number from a system of record (not numbers listed in an email or attachment) — **61%**
Adopted at least a two-factor authentication or other added layers of security for access to company network and payments initiation — **60%**	Require authorized signoff of senior management for transactions over a certain threshold — **53%**	Color-coded emails with colored banners or other methods of distinction etc. indicating they are external — **35%**	Flag emails where the "reply" email address is different than the "from" email address shown — **31%**
Intrusion detecting system that flags emails with extensions that are similar to company email (example: where "rn" could be in the place of an "m" etc.) — **27%**	Prohibit, or quickly detect, inbox email forwarding rules that redirect all or some emails to external email addresses. — **19%**	Using passcodes known only to both parties in a proposed wire transaction (not contained in an email) — **12%**	Penalties for employees who frequently open attachments or click links in phishing emails — **12%**

BUSINESS EMPLOYEE COMPROMISE (BEC) CONTROLS

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 68 percent of respondents)
- Stronger internal controls prohibiting payments initiation based on emails or other less secure messaging systems (61 percent)
- 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 or attachment) (61 percent)
- Adopting at least a two-factor authentication or other added layers of security for access to company network and payments initiation (60 percent)

Other revisions implemented or considering implementing:

- Aggressive email filtering software
- Practice phishing emails to employees
- Advanced warning services
- Special messaging when the email is internal
- Bank token

An individual had successfully infiltrated the server of a 3rd party that communicates with us. They intercepted emails and asked us to pay a new bank account. We called a known number to confirm the request, confirmed it was fraudulent, and the 3rd party began their process to resolve the infiltration.

BUSINESS EMPLOYEE COMPROMISE (BEC) CONTROLS

Validating Fraud Controls to Mitigate BEC Fraud

Six-out-of-ten organizations are validating fraud controls to mitigate BEC fraud. This is definitely a more frequent practice among larger organizations with revenue at least $1 billion as well as those with more than 100 payment accounts. Those companies who are validating fraud controls to prevent BEC fraud are doing so using various methods:

- Annual internal audits of controls
- Working closely with IT and cybersecurity departments
- Employees are trained and frequently reminded of fraud and phishing attempts
- Testing to ensure employees are mindful of phishing attempts
- Implemented account validation service through the bank
- Have policies and procedures in place to validate payment methods

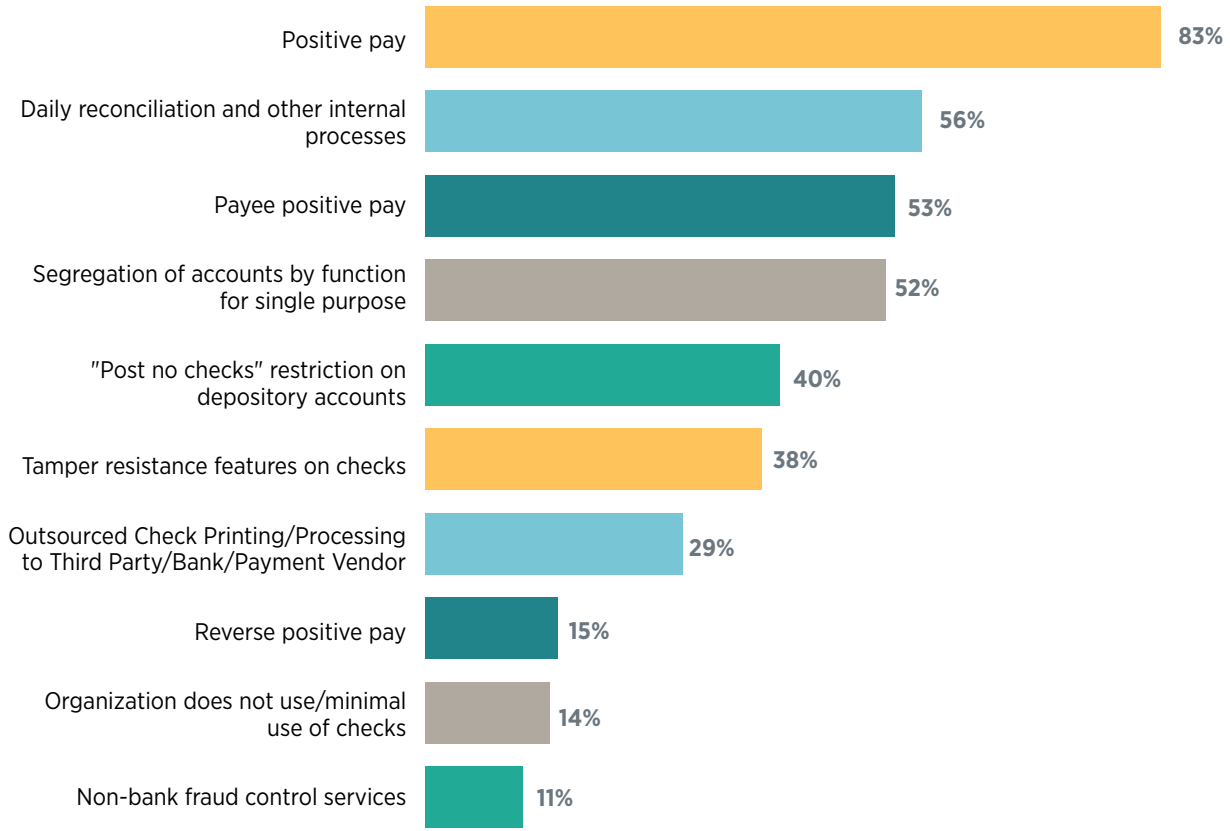
Percentage of Organizations who Validate Fraud Controls Implemented to Mitigate BEC Fraud
(Percentage Distribution of Organizations)

CHECK FRAUD CONTROLS

Positive Pay Most Popular in Protecting Against Check Fraud

Positive pay continues to be the method most often used by organizations to guard against check fraud. This approach is used by 83 percent of organizations—slightly lower than the 85 percent reported in 2021. Protective measures such as positive pay are not generally included in the payment offering options from organizations' financial institution partners; positive pay is, rather an added service for which the bank charges an extra fee. Other methods often used include daily reconciliations and other internal processes (cited by 56 percent of respondents), payee positive pay (53 percent), segregation of accounts (52 percent).

Fraud Control Procedures and Services used to Protect Against Check Fraud
(Percent of Organizations)



ACH FRAUD CONTROLS

Various Controls Implemented to Safeguard Against ACH Fraud

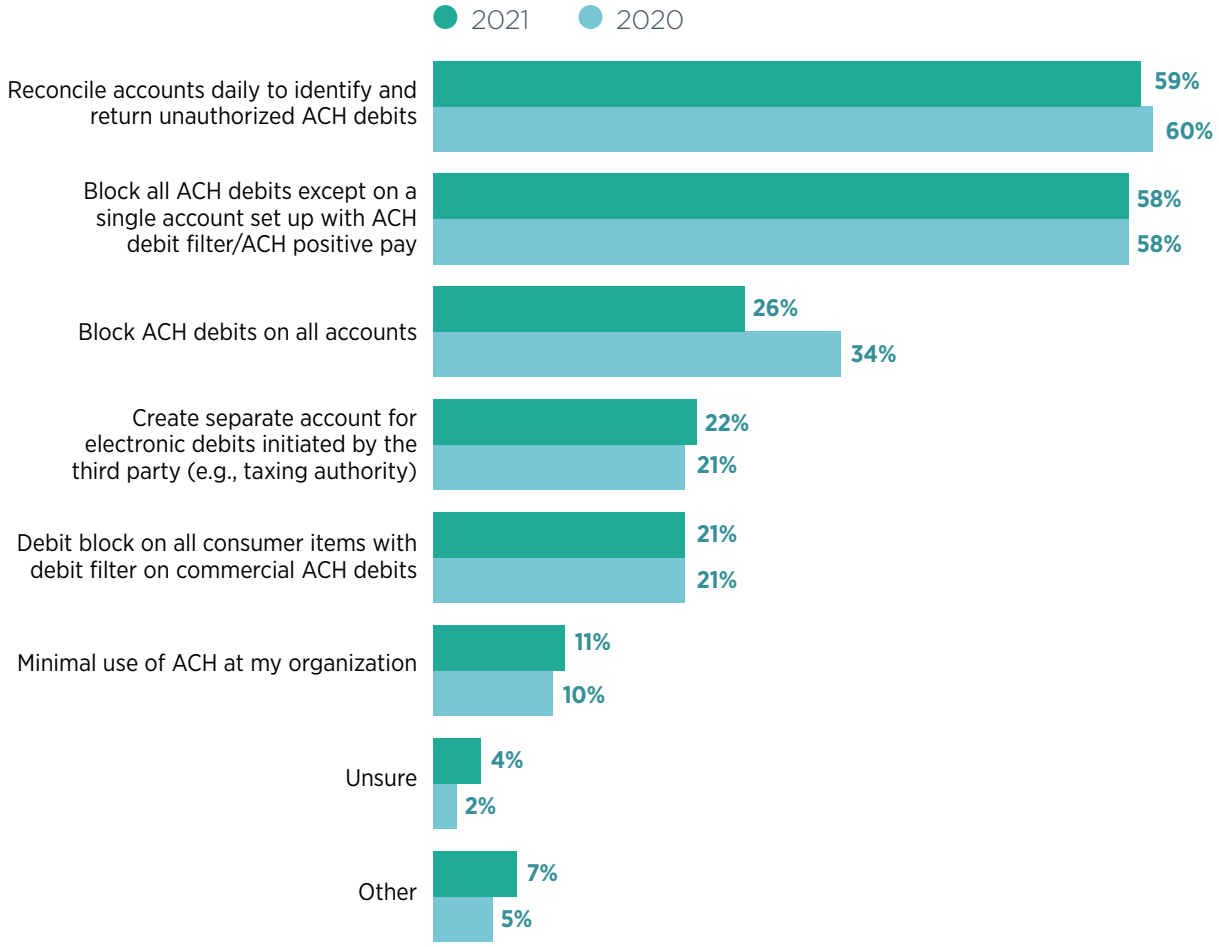
In 2021, 37 percent of organizations were victims of ACH debit fraud and 24 percent experienced ACH credit fraud. To safeguard against being impacted by ACH fraud, organizations are implementing the following measures:

- Reconcile accounts daily to identify and return unauthorized ACH debits, cited by 59 percent of respondents for 2021—a slight decrease from 60 percent in 2020
- Block all ACH debits except on a single account set up with ACH debit filter/ ACH positive pay (58 percent)—exactly the same as reported in 2020
- Block ACH debits on all accounts (26 percent)—a significant decrease from 34 percent in 2020

Other Includes:

- ACH positive pay
- Fraud review
- Account validation service
- Dual authorization
- Block ACH debit

Fraud Control Procedures or Services used to Prevent ACH Debit Fraud
(Percent of Organizations)



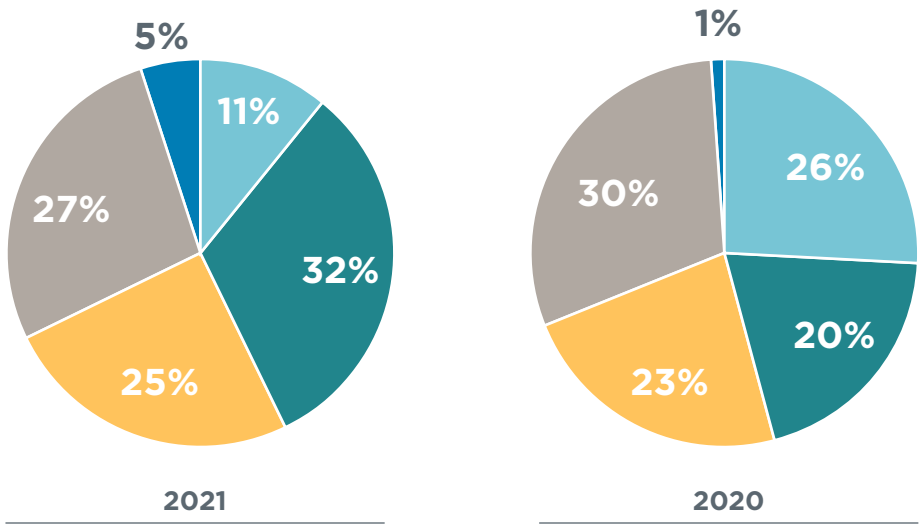
ACH FRAUD CONTROLS

Organization's Preparedness to Mitigate Additional Risks is Mixed

While Same-Day ACH is operational for both credit and debit transactions, only 11 percent of organizations have implemented plans to mitigate potential additional risks. This is significantly less than the 26 percent in last year's survey. Over 30 percent of companies have not yet implemented any plans to safeguard against and mitigate potential risks but are in the process of doing so (32 percent). Twenty-five percent of organizations are not taking any steps to prepare for and mitigate potential additional risks that might occur, and 27 percent are unsure as their banking partners have not extended any advice. As ACH usage becomes more widespread, the lack of planning for additional risks is an area of concern, especially as the Same Day ACH limit was raised to $1 million effective March 18, 2022.

Those who have implemented plans to mitigate additional risks have done so by continued training and focusing on call backs, implementing ACH debit blocks, introducing a second form of verification, positive pay or added an IT security guard.

Organizations Preparedness to Mitigate Potential Additional Risks with Same-Day ACH Operational for Both Credit and Debit Transactions
(Percentage Distribution of Organizations)



Other includes:

- Currently not using faster payment options or same day ACH
- Two-person authorization for any ACH payments
- Allow ACH debits to only a small number of vendors
- Looking at bank services in the near future

VALIDATING PAYMENT BENEFICIARY INFORMATION AND SANCTION SCREENING

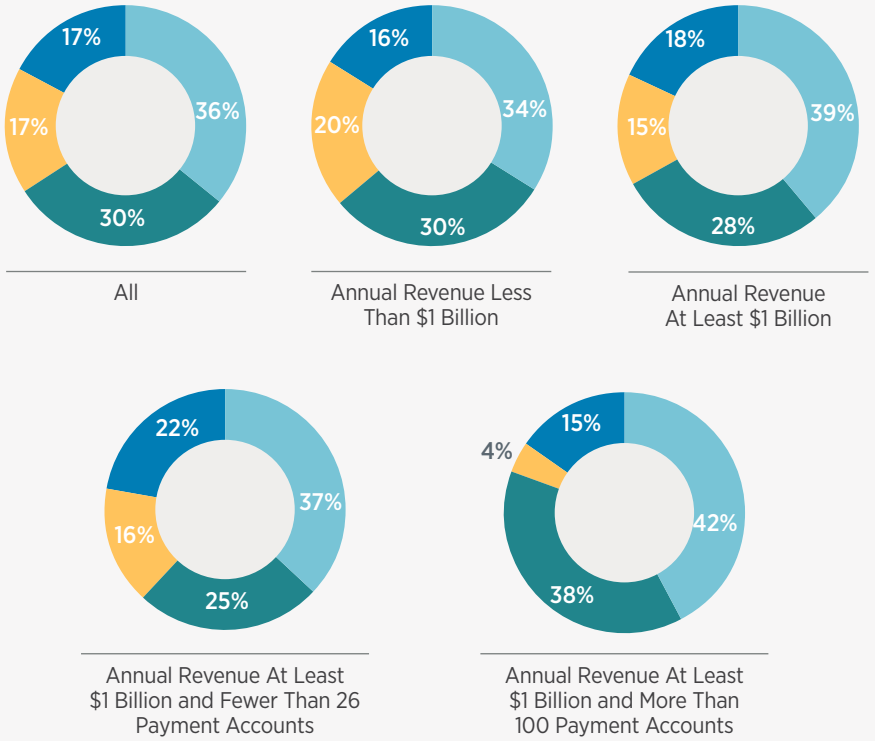
Majority of Organizations are Validating Payment Beneficiary Information

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)



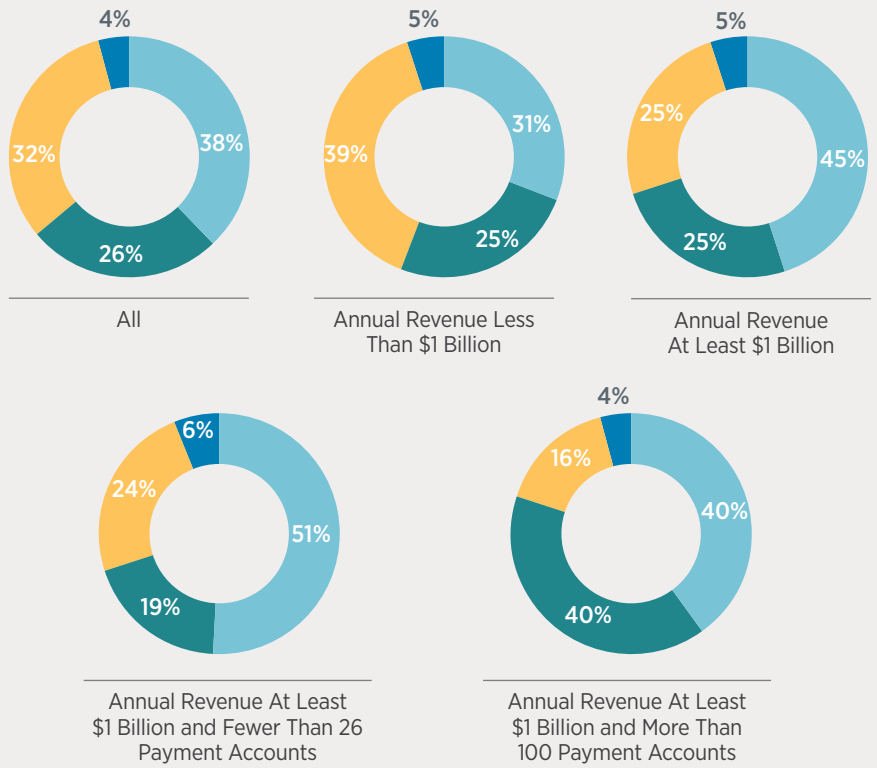
VALIDATING PAYMENT BENEFICIARY INFORMATION AND SANCTION SCREENING

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)



CURRENT MEASURES IMPLEMENTED TO IMPROVE CONTROLS AND MEASURES WISHED FOR IN 2022

Measures Implemented in 2021 to Improve Controls

Respondents implemented various measures in 2021 to improve controls and these included the following:

- Implementing call-back verifications
- Finance approval needed for banking information change
- Restrict access to who can add vendors
- Additional validation screening
- Payments requests are required to be approved via Payscan invoice workflow,
- Developed a vendor onboarding portal that requires a login and 2-factor authentication to access
- Conducted additional end-user training with a minimum pass rate required
- Daily verification of checking account debits and checks
- Dynamic overhaul of cloud security
- Formalized policy to independently validate change in wire instructions
- Updated email software to filter out spam and other malicious emails. Automating processes to eliminate the human error side of fraud
- Use of multifactor authentication for payment systems and use of account validation tools to validate account/payee ownership
- Added additional measures when a vendor requests a change to their banking information/remit address. We have implemented a multi-faceted comprehensive solution for mitigating the risks of payments fraud
- Further employee training
- Added the red banner on emails indicating external emails.
- Implemented stronger controls over account verification for vendor setup/ changes
- Purchased cyber-security insurance.

Wishlist for Measures to Improve Controls in 2022

- The measures they would like to see improved or changed in 2022
- Using an external source to validate beneficiary validation services
- Would like the ability to verify beneficiary information via the bank's website
- Automating internal processes is a goal for 2022
- Adding account validation services in 2022
- Implement recovery plan in case company or banks are compromised
- In 2022, I would like to see our company move to outsourcing checks as well as using external company to validate payment information
- More emphasis on educating users how to spot malicious activity
- Revised wire authorization form, improve wire instruction verification process, added more positive pay (checks/ACH) services to all of our bank accounts, limit user access to the account information

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.

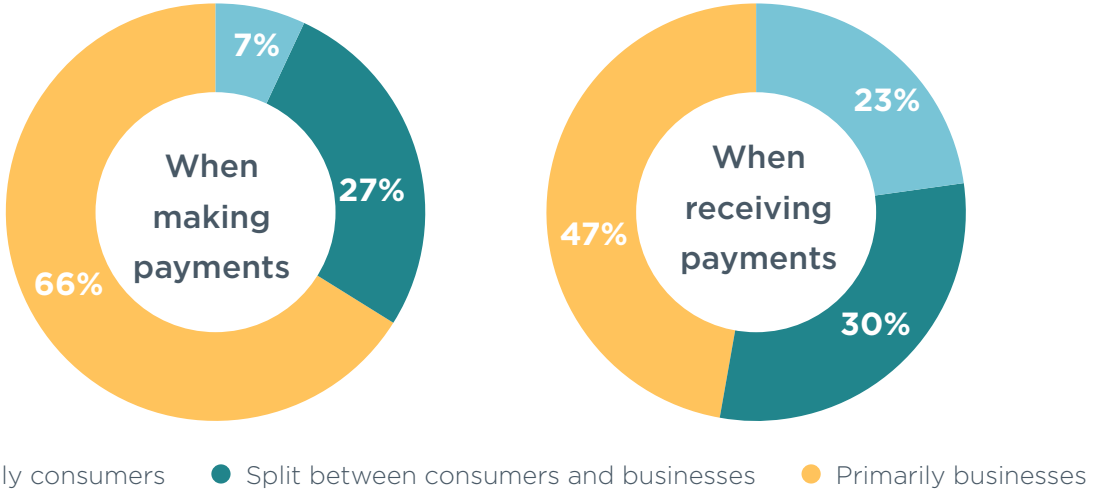
DEMOGRAPHICS

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)



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)

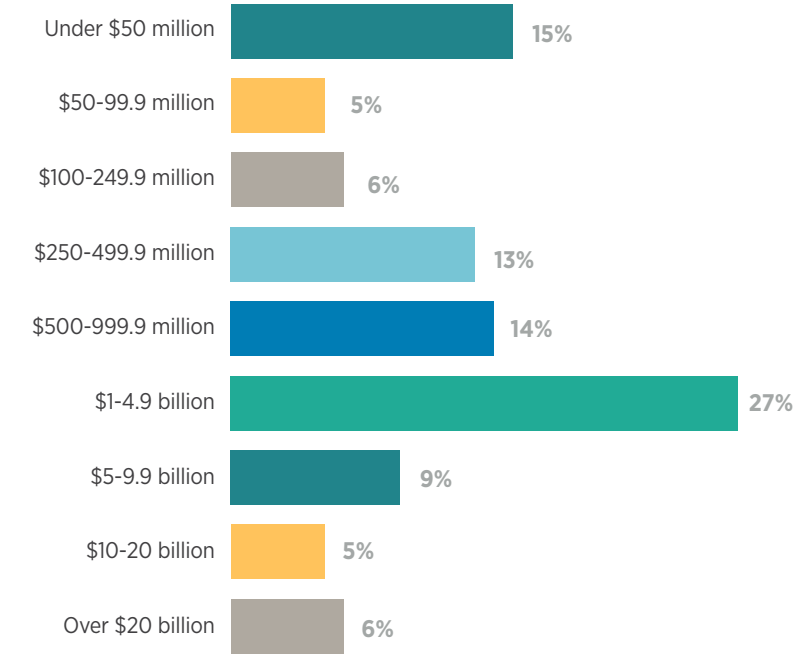
	ALL	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS
Centralized	80%	86%	73%	84%	61%
Decentralized	16%	12%	21%	13%	31%
Other	4%	2%	6%	3%	8%

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%

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

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