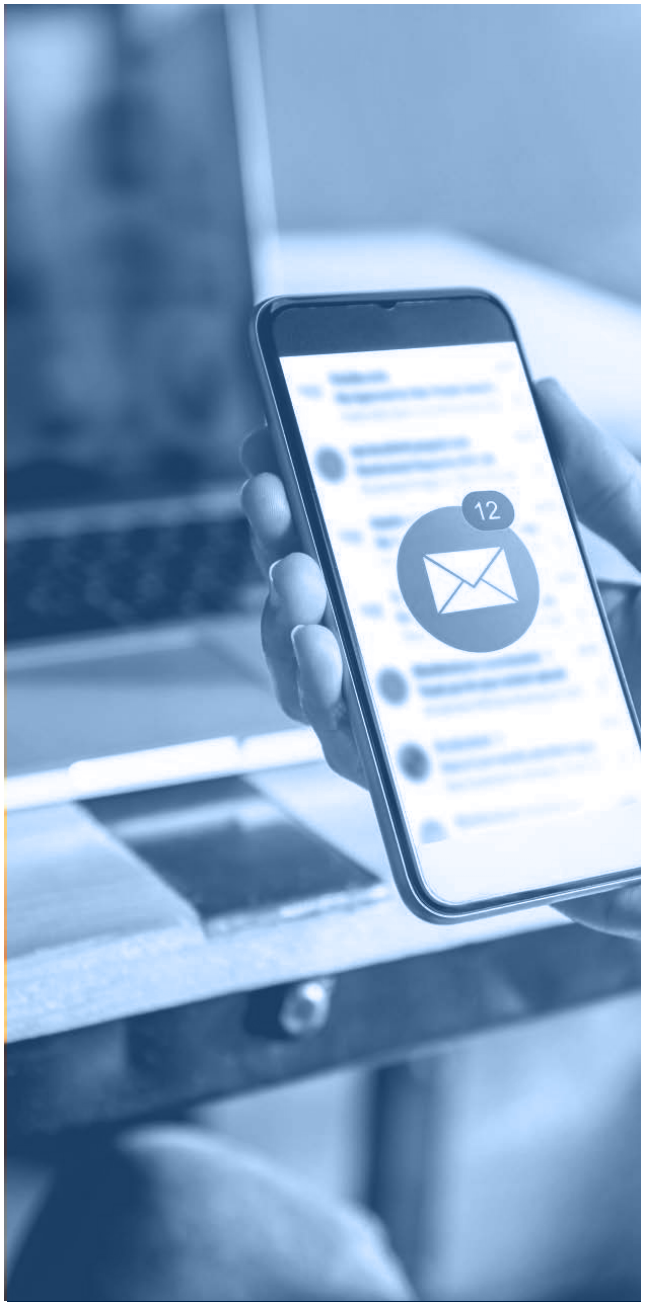
ASSOCIATION FOR FINANCIAL PROFESSIONALS

2018 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Key Highlights

Underwritten by J.P.Morgan



2018 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Key Highlights

April 2018

2018 AFP PAYMENTS FRAUD AND CONTROL SURVEY REPORT
This summary report includes highlights from the comprehensive 2018 AFP Payments Fraud and Control Survey Report. The complete report comprising all findings and detailed analysis is exclusively available to AFP members. **Learn more about AFP membership.**

Underwritten by J.P.Morgan

Topics Covered in the Comprehensive 2018 AFP Payments Fraud and Control Survey Report

J.P.Morgan

J.P. Morgan is proud to sponsor the AFP Payments Fraud and Control Survey for the tenth consecutive year and to provide you with the 2018 report.

The survey shows that 78 percent of companies were targets of payments fraud last year demonstrating the crucial need for cybersecurity protocols and strict control governance. Additionally, the survey reveals that in 2017:

- 77 percent of organizations experienced Business Email Compromise (BEC)
- 54 percent of BEC scams targeted wires, followed by checks at 34 percent
- 77 percent of organizations implemented controls to prevent BEC scams
- 74 percent of organizations experienced check fraud, a slight decrease from 2016
- 28 percent were subject to ACH debit fraud and 13 percent were subject to ACH credit fraud
- 67 percent of payments fraud was discovered by the organization's treasury staff

With these statistics in mind, it is important for all businesses to take preventive measures to protect payments, including educating employees on current payments fraud practices, and implementing the products and processes necessary to protect corporate assets and data from cyber fraud.

J.P. Morgan is one of the world's largest providers of treasury management services and is a leader in electronic payments technology and solutions. We are committed to fraud mitigation and information protection across our entire infrastructure, and we will continue to invest in the technology, educational tools and risk management expertise in the ongoing fight against payments fraud.

We hope this survey serves as such an important tool in understanding the potential cyber risks within the payments industry—they should not be underestimated. We would like to thank the AFP for providing us with this year's valuable insights—they are an important reminder that the best defense is to remain vigilant in fraud detection and cybersecurity protection protocols.

With best regards,

Jessica Lupovici
Managing Director
J.P. Morgan

Bob St Jean
Managing Director
J.P. Morgan

J.P. Morgan is a marketing name for certain businesses segments of JPMorgan Chase & Co. and its subsidiaries worldwide. The material contained herein or in any related presentation or oral briefing do not constitute in any way J.P. Morgan research or a J.P. Morgan report, and should not be treated as such (and may differ from that contained in J.P. Morgan research) and are not intended as an offer or solicitation for the purchase or sale of any financial product or a commitment by J.P. Morgan as to the availability to any person of any such product at any time. All J.P. Morgan products, services, or arrangements are subject to applicable laws and regulations, its policies and procedures and its service terms, and not all such products and services are available in all geographic areas.

Introduction

Payments fraud activity continues to increase, and there are no signs of it abating any time soon. The level of payments fraud activity in 2017 was the highest on record, rising at a greater pace than in 2016. Controlling fraud is top-of-mind for business leaders, and organizations are implementing controls and measures to restrict the occurrence of such activity. Yet, the perpetrators of these attacks continue to succeed in targeting payment methods. Additionally, while advances in and widespread use of technology have increased payments efficiency, they have also provided criminals with more tools to facilitate payments fraud success.

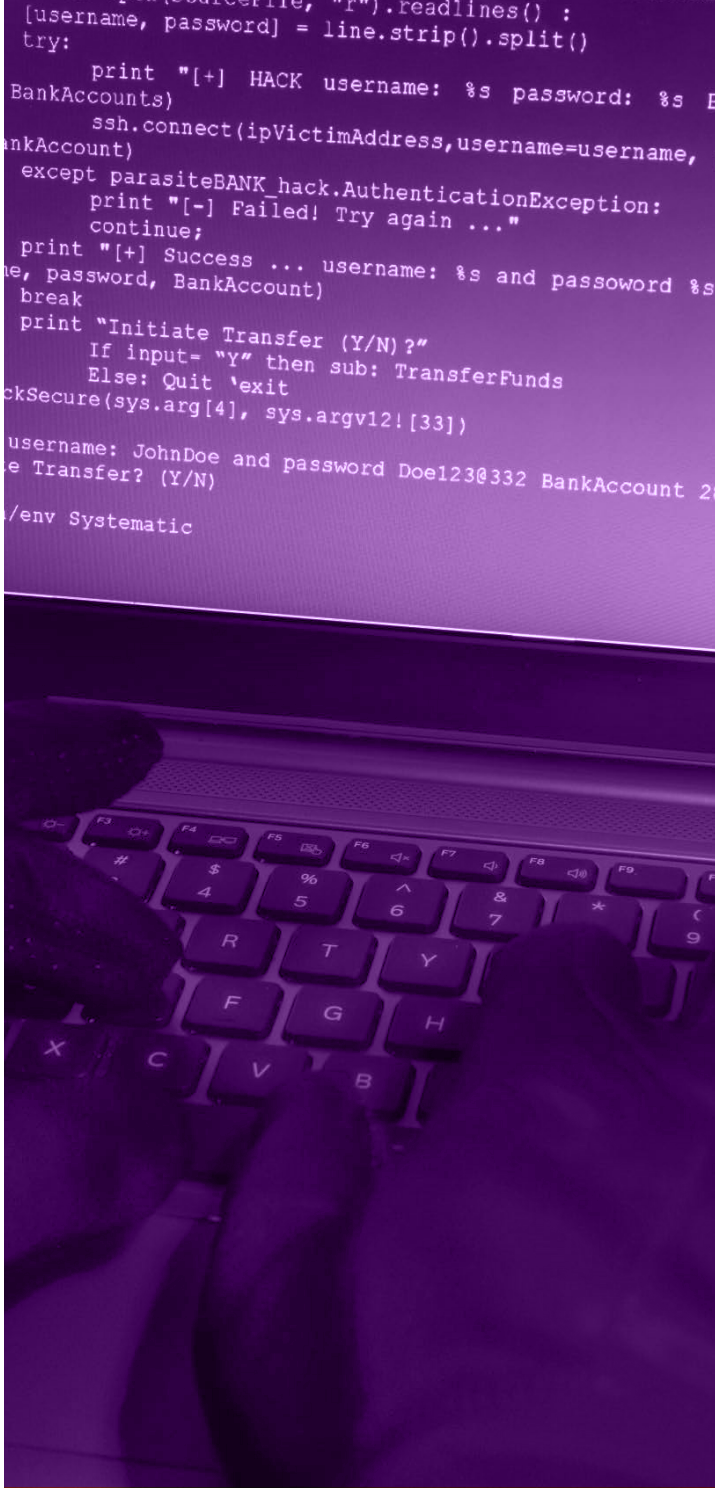
While payments fraud occurs across a variety of payment methods, checks again topped the list of targets in 2017, being subject to more payments fraud than any other payment method. The frequency of fraud via checks had been on the decline until 2016 when it rose from 71 percent (in 2015) to 75 percent. One likely reason for the uptick is a slight increase in the use of checks for business-to-business (B2B) transactions.

An additional concern in the past couple of years has been the increase in wire fraud. Since 2014, the incidence of wire fraud has risen precipitously—more than tripling from 14 percent in 2014 to 48 percent in 2017. This dramatic increase in wire fraud is likely a result of the increasing number of business email compromise (BEC) scams which primarily target wire payments, and contributes to keeping wire fraud at an elevated level. BEC scams continue to evolve and are often associated with more sophisticated fraud attempts (which also increased). This year's survey findings also suggest that checks are becoming more popular targets for BEC. The number of organizations being exposed to BEC has been rising each year, with 77 percent of organizations having experienced at least one instance of fraud activity via BEC during 2017.

Treasury and finance professionals need all the tools and information available in order to outsmart fraudsters. In their efforts to be more efficient in their payments, organizations may also unknowingly expose themselves to attacks. Criminals scamming payment systems are adept at hacking those systems, and evidence suggests that despite the efforts of organizations to alleviate instances of fraud, little is hindering fraudsters' efforts. While financial loss due to payments fraud may not be large, the risk of reputational damage could be far more significant.

Since 2005 the Association for Financial Professionals® (AFP) has conducted its *Annual Payments Fraud Survey.* The surveys examine the nature of fraud attacks on business-to-business transactions, payment methods impacted and strategies organizations are adopting to protect themselves against fraudsters. Continuing this research, AFP conducted the 14th *Annual Payments Fraud and Control Survey* in January 2018. The survey generated 682 responses from corporate practitioners from organizations of varying sizes representing a broad range of industries. Results from the survey presented in this report reflect data for 2017. 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.



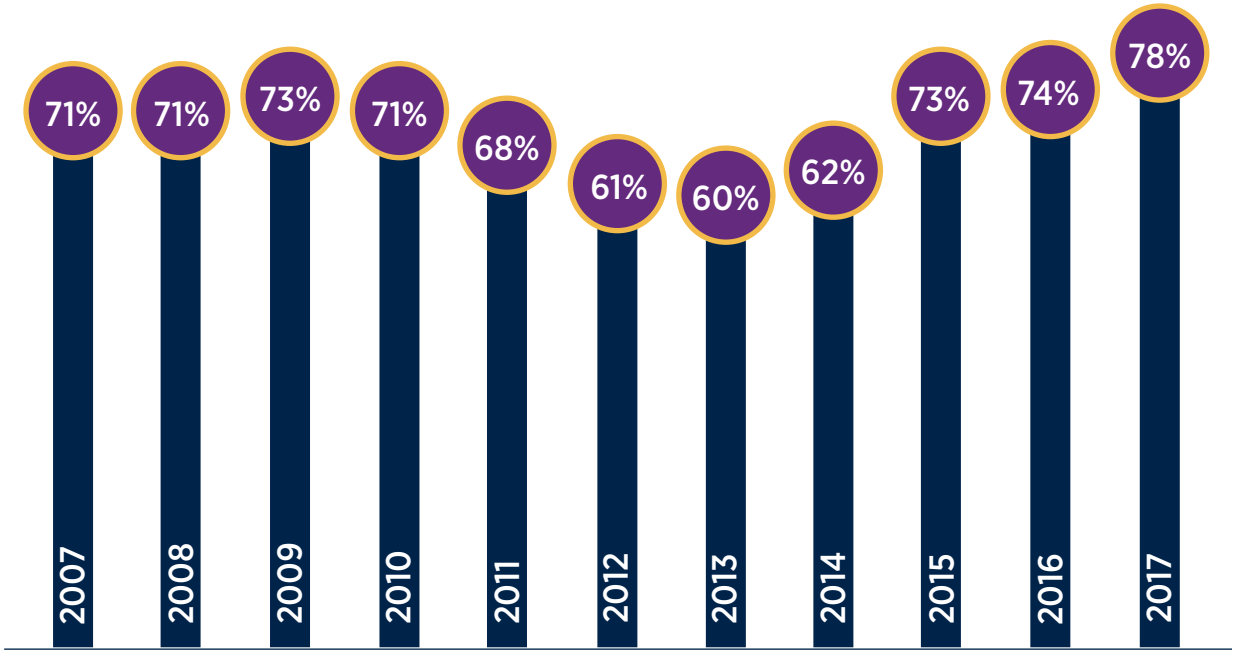
01 PAYMENTS FRAUD

Payments Fraud Continues on the Uptick

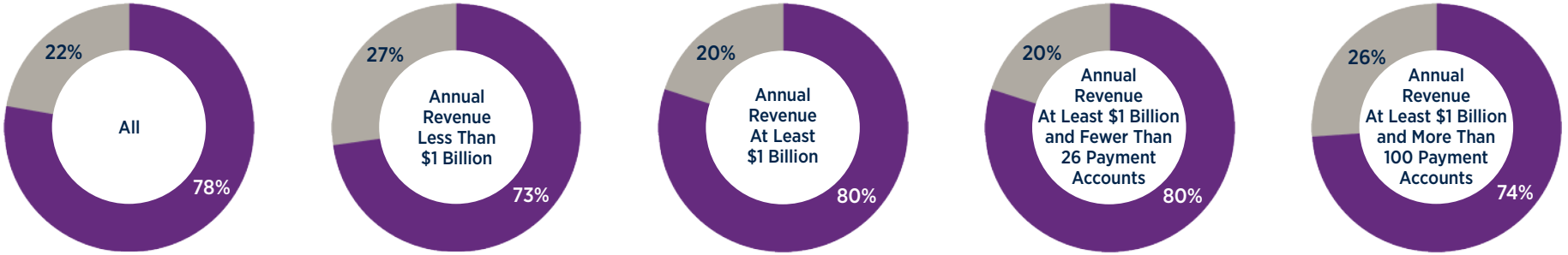
Over the last decade, the incidence of payments fraud has fluctuated significantly. In 2007 and 2008, 71 percent of organizations were targets of either attempted or actual fraud. From 2009 to 2013 there was steady decline in payments fraud activity. But in 2014 that trend reversed; since then organizations have experienced an uptick in payments fraud with a steep increase in 2015 and another increase in 2017. Seventy-eight percent of finance professionals report that their companies experienced attempted/actual payments fraud in 2017—the largest percentage on record.

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—reports payments fraud activity than do respondents from other organizations. In fact, in the last three years, larger organizations with fewer than 26 payment accounts have been more vulnerable to payment fraud attacks than were other companies. At least 80 percent of these organizations have been victims of payments fraud in each of the past three years.

Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud, 2007-2017



Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud in 2017



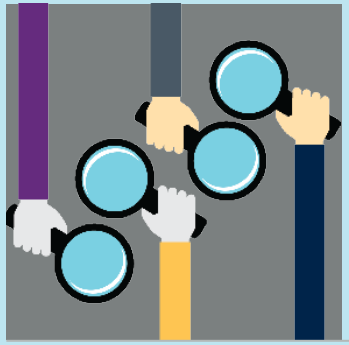
Key Facts about Payments Fraud Activity

65%

54%

Who are these fraudsters?

The majority of payments fraud activity continues to originate from **outside individuals** via forged checks or stolen cards (cited by 65 percent of survey respondents) and **business email compromise** (BEC) (54 percent).



67% of Treasury Staff

Who discovered the payments fraud activity?

At two-thirds of organizations, **treasury staff** discovered the fraud. **Payments and Accounts Payable staff** also played an active role in helping identify instances of payments fraud (41 percent).

AFP Voices

Who discovered the payments fraud activity?

"Customer Service notified by policyholder of stolen identity"

"Positive Pay, Credit Card Provider"

"Bank Reconciliation Staff"

"Discovered through communication between multiple departments regarding a payment request"

47%

21%

How long did it take to discover the fraud?

At nearly half of organizations (47 percent) the fraud was uncovered in **less than a week;** at another 21 percent of companies the fraud was discovered in between one to two weeks.

92% report that it cost their companies **half a percent** of total revenue

How much did payments fraud cost the company?

An overwhelming majority (92 percent) of survey respondents reports that the fraud attacks cost their companies **no more than half a percent of the organization's total revenue**. Another eight percent report the impact of fraud on their organizations' revenue ranged from 0.51 percent to 1.5 percent.

AFP Voices

Instances of payments fraud

"Over 100 cards in our city's Commercial Card Program fell victim to a credit master attack, where fraudsters used sophisticated algorithms to estimate what the account numbers and expiration dates were."

"Recently someone was issuing checks to individuals for work done over the internet. The checks were forged from one of our disbursement accounts. They were all caught with Positive Pay and returned."

"We discovered counterfeit checks and ACH debit fraud on an account that did not have Positive Payee feature or ACH debit block because of the urgency to open account. We added the necessary filters and notified the bank of the fraudulent activities. I cannot stress enough the importance of Positive Payee."

02 BUSINESS EMAIL COMPROMISE

What is Business Email Compromise?

Business Email Compromise (BEC) is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The Email Account Compromise (EAC) component of BEC targets individuals that perform wire transfer payments. The scam is carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices. The scam has evolved to include the compromising of legitimate business email accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees, and may not always be associated with a request for transfer of funds.

Source: The Federal Bureau of Investigation (FBI)

Statistical Data

The following BEC/EAC statistics were reported to the Federal Bureau of Investigation's Internet Crime Compliance Center (IC3) and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between October 2013 and December 2016:

Domestic and international incidents:
40,203

Domestic and international exposed dollar loss:
$5,302,890,448

Source: The Federal Bureau of Investigation (FBI)

To Conclude

As findings from this survey suggest, U.S. businesses are experiencing increased levels of payments fraud activity. A significant 78 percent of organizations were targets of payments fraud in 2017—an increase of four percentage points from 2016 and the highest share on record. Over the past decade, there were some periods during which payments fraud activity declined, but in the past three years fraud activity has been on the rise. The consequences of fraud activity on organizations can be extreme and have far-reaching impacts on companies' bottom lines, employees, consumers—and their reputations. Fraudsters are also looking to steal personally identifiable information and other confidential data which elevates fraud risk for an organization, its suppliers and customers. AFP members report that their companies are incurring high clean-up costs and investing heavily in measures to guard against future attacks.

What is concerning is that despite the actions companies are taking to guard against payments fraud, scammers continue to persist in their efforts to attack payment systems. Even when fraudsters face challenges when planning their attacks on a particular payment method, they likely shift their focus to an alternative payment vehicles, as in the case with business email compromise (BEC). Business leaders need to be vigilant in their efforts to prevent future fraud attempts and to make it more difficult for criminals to hack into payment systems.

Results from the *2018 Payments Fraud and Control Survey* reveal key trends in payments fraud activity. Notable among these are:

The increase in payments fraud activity in general is certainly unsettling, and the amount of the increase is a little surprising given the number of protective measures that are available. Organizations cannot assume they can protect themselves from all payments fraud, but there certainly are ways fraud can be mitigated.

Payments fraud via wires remains elevated, and has increased slightly since 2015. Wires are the most targeted payment method for BEC scams, and these scams unfortunately are still successful. In addition, given that more and more organizations are implementing measures to protect themselves from BEC scams, the elevated level of wire fraud also indicates that BEC scams are evolving into methods and structures, challenges for which organizations may not be prepared.

The more sophisticated kind of payments fraud involving account take-overs and third-party breaches also appears to have increased or remained at an elevated level. This supports the assumption that BEC scams are evolving as these are considered more sophisticated forms of payments fraud and ones that require extensive research and background work by the criminals in order to for the scam to succeed. Organizations are actively taking steps to prevent being victims of BEC fraud, including the training of staff, as well as incorporating other measures, to verify that payment requests are authentic. This is encouraging and probably one reason why the rapid growth in payments fraud via BEC appears to have been restrained in 2017.

It is also notable that checks remain the payment method most often subject to payments fraud. It may not be surprising given the high use of checks for B2B transactions. But with the wide array of protective measures such as positive pay as well as the general decline in the use of checks, the level of check fraud should abate.

Finally, it is also encouraging to see that organizations are being proactive in implementing protective measures against payments fraud. Organizations are now using measures such as positive pay to a much larger extent than before, after its use declined in 2016. Organizations are also installing new internal controls to protect against BEC scams. This is a positive trend, but it is important that organizations remain vigilant in protecting themselves against fraud. Companies need to keep looking "outside the box"—the criminals do.

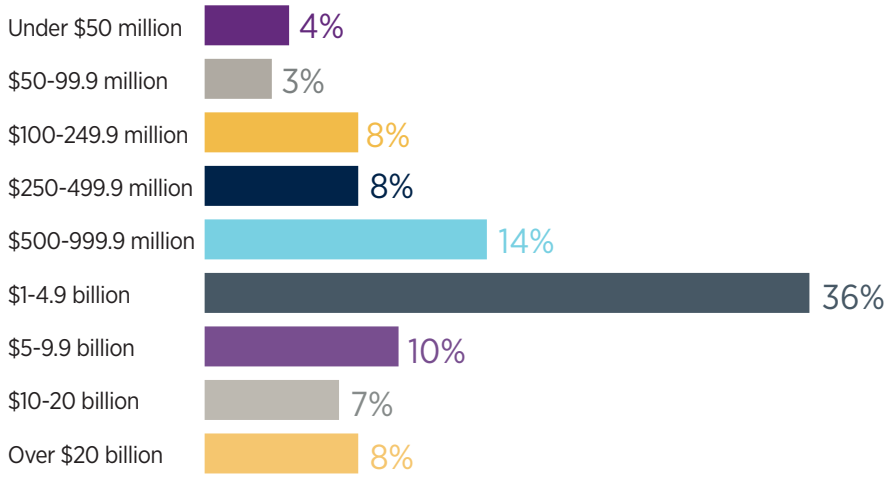
04 ABOUT SURVEY PARTICIPANTS

About the Survey Participants

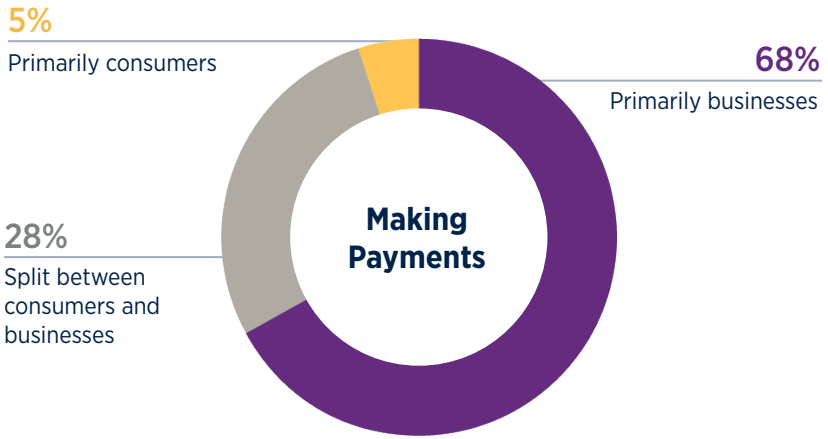
In January 2018, the Research Department of the Association for Financial Professionals® (AFP) surveyed a sample of its corporate practitioner members and prospects. The survey was sent to corporate practitioners with the following job titles: cash manager, treasurer, assistant treasurer, analyst, director, and vice president of treasury. We received 420 responses from members and an additional 262 responses from prospects, generating a total of 682 responses.

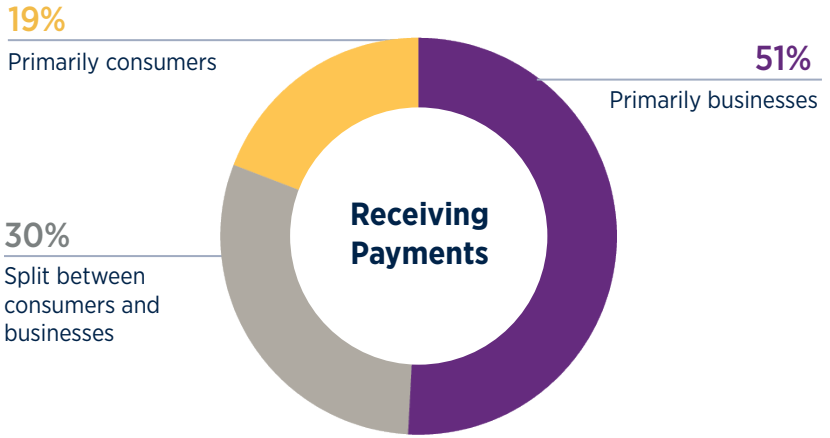
AFP thanks J.P. Morgan for underwriting the *2018 AFP Payments Fraud and Control Survey.* Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibilities of the AFP Research Department. The following tables provide a profile of the survey respondents, including payment types used and accepted.

Annual Revenue (U.S. dollar)
(Percentage Distribution of Organizations)



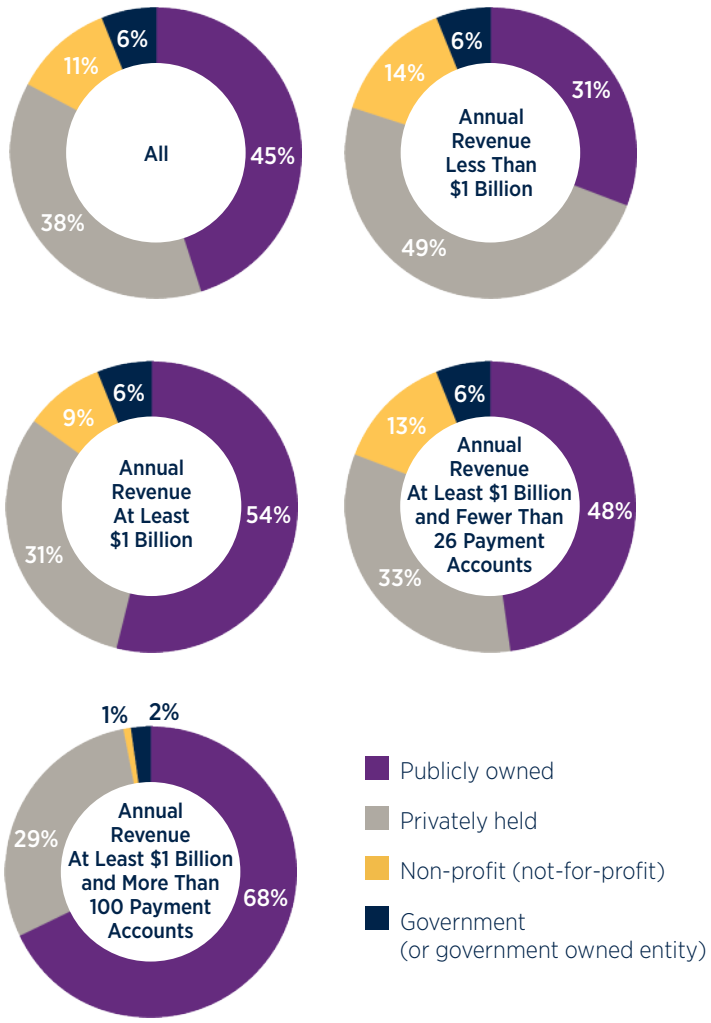
Type of Organization's Payment Transactions
(Percentage Distribution of Organizations Payment Transactions)





About the Survey Participants continued

Organization's Ownership Type
(Percentage Distribution of Organizations)



Payment Accounts Maintained
(Percentage Distribution of Payment Accounts Maintained)

	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	26%	36%	21%	37%	–
5-9	18	23	16	28	–
10-25	20	18	21	36	–
26-50	8	4	11	–	–
51-100	7	7	8	–	–
More than 100	21	13	23	–	100%

Industry
(Percentage Distribution of Organizations)

	ALL
Banking/Financial Services	9%
Business Services/Consulting	4
Construction	3
Energy (including utilities)	9
Government	5
Health Services	8
Hospitality/Travel	2
Insurance	6
Manufacturing	20
Non-profit (including education)	6
Real Estate	4
Retail (including wholesale distribution)	11
Software Technology	5
Telecommunications/Media	3
Transportation	3

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, 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®

The Association for Financial Professionals (AFP) is the professional society committed to advancing the success of its 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 finance. Each year, AFP hosts the largest networking conference worldwide for over 6,500 corporate finance professionals.

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

www.AFPonline.org

Payments Fraud

PROTECT for if, **PREPARE** for when

In 2017 alone, 78 percent of companies were impacted by payments fraud through credit card and business email compromise, among other malicious techniques. Get proactive about cybersecurity, and visit our Fraud Resource Center to learn how to identify fraud and protect your business.

Learn more at jpmorgan.com/cb/fraud-prevention

Commercial Banking Treasury Services

J.P.Morgan

© 2018 JPMorgan Chase & Co. All rights reserved. 424362